Arbeitsübersetzung (maßgeblich ist der englische Text vom 22 April 2016)

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development
Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

22. April 2016

Deutsch - Or. Englisch

ENVIRONMENT DIRECTORATE
UMWELTDIREKTORAT
JOINT MEETING OF THE CHEMICALS COMMITTEE AND
JOINT MEETING DES CHEMIKALIENAUSSCHUSSES UND
THE WORKING PARTY ON CHEMICALS, PESTICIDES AND BIOTECHNOLOGY
DER ARBEITSGRUPPE CHEMIKALIEN, PFLANZENSCHUTZMITTEL UND BIOTECHNOLOGIE

ENV/JM/MONO(2016)13
Nicht klassifiziert

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING
OECD-SCHRIFTENREIHE ÜBER DIE GRUNDSÄTZE DER GUTEN LABORPRAXIS UND DIE ÜBERWACHUNG IHRER EINHALTUNG
Nummer 17

Advisory Document of the Working Group on Good Laboratory Practice
Beratungsdokument der Arbeitsgruppe Gute Laborpraxis

Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme

Die Übersetzung wurde nicht von der OECD erstellt und ist keine offizielle OECD Übersetzung.
Die OECD ist nicht haftbar für den Inhalt oder Fehler in der Übersetzung

JT03394591

Das vollständige Dokument finden Sie im Originalformat im Informationsdienst OLIS.
Das vorliegende Dokument und alle darin enthaltenen Landkarten werden unbeschadet des Status oder der Souveränität eines Territoriums sowie ungeachtet geltender internationaler Staats- und Ländergrenzen und ungeachtet der Namen von Territorien, Städten bzw. Gebieten verwendet.

Deutsch - Or. Englisch

OECD Environment, Health and Safety Publications
OECD-Veröffentlichungen zur Umweltsicherheit und -hygiene

Series on Principles of Good Laboratory Practice and Compliance Monitoring
Schriftenreihe über die Grundsätze der Guten Laborpraxis und die Überwachung ihrer Einhaltung

Nr. 17

Advisory Document of the Working Group on Good Laboratory Practice
Beratungsdokument der Arbeitsgruppe Gute Laborpraxis

Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme

Environment Directorate
Umweltdirektorat

ORGANISATION FÜR WIRTSCHAFTLICHE ZUSAMMENARBEIT UND ENTWICKLUNG

Paris 2016

EBENFALLS IN DER OECD-SCHRIFTENREIHE ÜBER DIE GRUNDSÄTZE DER GUTEN LABORPRAXIS UND DIE ÜBERWACHUNG IHRER EINHALTUNG VERÖFFENTLICHT:

- *No. 1, OECD Principles of Good Laboratory Practice (as revised in 1997)*
  Nr. 1, OECD-Grundsätze der Guten Laborpraxis (Neufassung aus 1997)

- *No. 2, Revised Guides for Compliance Monitoring Procedures for Good Laboratory Practice (1995)*
  Nr. 2, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 3, Revised Guidance for the Conduct of Laboratory Inspections and Study Audits (1995)*
  Nr.3, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 4, Quality Assurance and GLP (as revised in 1999)*
  Nr. 4, Qualitätssicherung und Gute Laborpraxis (Neufassung aus 1999)

- *No. 5, Compliance of Laboratory Suppliers with GLP Principles (as revised in 1999)*
  Nr. 5, Einhaltung der GLP-Grundsätze durch Lieferanten (Neufassung aus 1999)

- *No. 6, The Application of the GLP Principles to Field Studies (as revised in 1999)*
  Nr. 6, Die Anwendung der GLP-Grundsätze auf Freilandprüfungen (Neufassung aus 1999)

- *No. 7, The Application of the GLP Principles to Short-term Studies (as revised in 1999)*
  Nr. 7, Die Anwendung der GLP-Grundsätze auf Kurzzeit-Prüfungen (Neufassung aus 1999)

- *No. 8, The Role and Responsibilities of the Study Director in GLP Studies (as revised in 1999)*
  Nr. 8, Die Rolle und Verantwortlichkeiten des Prüfleiters bei GLP-Prüfungen (Neufassung aus 1999)

- *No. 9, Guidance for the Preparation of GLP Inspection Reports (1995)*
  Nr. 9, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 10, The Application of the Principles of GLP to Computerised Systems (1995)*
  Nr. 10, Die Anwendung der GLP-Grundsätze auf computergestützte Systeme (1995)

- *No. 11, The Role and Responsibilities of the Sponsor in the Application of the principles of GLP (1998)*
  Nr. 11, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 12, Requesting and Carrying Out Inspections and Study Audits in Another Country (2000)*
  Nr. 12, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

- *No. 13, The Application of the OECD Principles of GLP to the Organisation and Management of Multi-Site Studies (2002)*
  Nr. 13, Die Anwendung der OECD GLP-Grundsätze auf Organisation und Management von Multi-Site-Prüfungen (2002)

- *No. 14, The Application of the Principles of GLP to in vitro studies (2004)*
  Nr. 14, Die Anwendung der OECD GLP-Grundsätze auf in vitro Prüfungen (2004)

- *No. 15, Establishment and Control of Archives that Operate in Compliance with the Principles of GLP (2007)*
  Nr. 15, Einrichtung und Betrieb von Archiven in Übereinstimmung mit den Grundsätzen der Guten Laborpraxis (2007)

- *No. 16, Guidance on the GLP Requirements for Peer Review of Histopathology (2014)*
  Nr. 16, Zur Zeit noch keine deutsche Übersetzung veröffentlicht

ÜBER DIE OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist eine internationale Organisation, in der die Regierungsvertreter von 34 Industrienationen aus Nord- und Südamerika, Europa und der Region Asien und Pazifik sowie Vertreter der Europäischen Kommission zusammentreffen, um ihre Politik zu koordinieren und zu harmonisieren, Themen von gemeinsamem Interesse zu erörtern, und mit dem Ziel zusammenarbeiten, Lösungen für internationale Probleme zu finden. Der überwiegende Teil der Arbeit der OECD wird von mehr als 200 Fachausschüssen und sonstigen Gremien geleistet, die sich aus den Delegierten der Mitgliedsländer zusammensetzen. Beobachter aus mehreren Ländern, die bei der OECD einen Sonderstatus haben, und Vertreter interessierter internationaler Organisationen nehmen an zahlreichen OECD-Workshops und anderen Tagungen teil. Die Ausschüsse und sonstigen Gremien werden vom OECD-Sekretariat in Paris unterstützt, welches sich in Direktorate und Abteilungen untergliedert.

Die Abteilung Umweltsicherheit und -hygiene (EHS) veröffentlicht 11 unterschiedliche Reihen von kostenlos erhältlichen Dokumenten: **Testing and Assessment; Good Laboratory Practice and Compliance Monitoring; Pesticides; Risk Management; Harmonisation of Regulatory Oversight in Biotechnology; Safety of Novel Foods and Feeds; Chemical Accidents; Pollutant Release and Transfer Registers; Emission Scenario Documents sowie Safety of Manufactured Nanomaterials.** Weitere Informationen über das Programm Umweltsicherheit und -hygiene und die EHS-Veröffentlichungen sind über die World Wide Web-Site der OECD (www.oecd.org/ehs/) verfügbar.

Die vorliegende Veröffentlichung wurde im Rahmen des Inter-Organization Programme for the Sound Management of Chemicals (IOMC) erstellt. Inhaltlich spiegelt die Veröffentlichung nicht unbedingt die Ansichten oder erklärten Strategien einzelner Teilnehmerorganisationen des IOMC wider.

Das Inter-Organisation Programme for the Sound Management of Chemicals (IOMC) wurde 1995 gemäß den Empfehlungen der UN-Konferenz über Umwelt und Entwicklung von 1992 eingerichtet, um die Zusammenarbeit zu stärken und die internationale Koordinierung im Bereich der Sicherheit von Chemikalien zu verbessern. Die Teilnehmerorganisationen sind FAO, ILO, UNDP, UNEP, UNIDO, UNITAR, WHO, World Bank und OECD. Ziel der IOMC ist es, die Koordinierung der von den Teilnehmerorganisationen gemeinsam oder einzeln verfolgten Politik und Aktivitäten zu fördern, um zu einem im Hinblick auf die menschliche Gesundheit und die Umwelt sachgemäßen Umgang mit Chemikalien beizutragen.

Diese Veröffentlichung kann kostenlos in elektronischer Form abgerufen werden.

Diese sowie zahlreiche weitere Veröffentlichungen zum Thema Umwelt Gesundheit und Sicherheit sind über die Webseite (www.oecd.org/ehs/) der OECD

verfügbar bzw. können direkt angefordert

werden bei:

OECD Environment Directorate,
Environment, Health and Safety Division
2 rue André-Pascal
75775 Paris Cedex 16
Frankreich

Fax: +33 1 44 30 61 80

E-Mail: ehscont@oecd.org

Die Originalversion wurde von der OECD in Englisch veröffentlicht unter dem Titel: OECD (2016), Advisory Document of the Working Group on Good Laboratory Practice, ***OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No.17*****, (ENV/JM/MONO(2016)13),**
http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=env/jm/mono%282016%2913&doclanguage=en
© 2018 German Quality Management Association e.V. für diese deutsche Übersetzung

VORWORT

Die Arbeitsgruppe Gute Laborpraxis der OECD hat auf ihrer 26. Tagung im Jahre 2012 eine Redaktionsgruppe unter der Leitung des österreichischen Bundesamtes für Sicherheit im Gesundheitswesen (Red. Ronald BAUER) eingesetzt, um das OECD GLP-Konsensdokument Nr. 10 „Die Anwendung der GLP-Grundsätze auf computergestützte Systeme“ (1995) zu aktualisieren. Die Redaktionsgruppe bestand aus Vertretern Österreichs, Belgiens, Irlands, Italiens, der Schweiz, dem Vereinigten Königreich und der US-amerikanischen Umweltschutzbehörde EPA.

Das nachfolgende Advisory-Dokument ersetzt das Konsensus-Dokument aus dem Jahre 1995. In die Arbeitsunterlage übernommen wurde der gesamte wichtige Text aus dem ursprünglichen Konsensdokument Nr. 10, jedoch wurden neue Textpassagen eingefügt, um den aktuellen Sachstand auf diesem Gebiet zum widerzuspiegeln. Dieses Advisory-Dokument wurde im Entwurf am 17. September 2014 auf der öffentlichen GLP-Website online gestellt, und die Öffentlichkeit wurde aufgerufen, bis zum 14. November 2014 ihre Kommentare dazu abzugeben. Die abgegebenen Kommentare kommen in vorliegendem Dokument zum Ausdruck.

Das vorliegende Dokument wird unter der Verantwortung des Joint Meeting des Chemikalienausschusses und der Arbeitsgruppe Chemikalien, Pflanzenschutzmittel und Biotechnologie der OECD veröffentlicht.

INHALTSVERZEICHNIS

1. EINLEITUNG 12
1.1. Anwendungsbereich und Begriffsbestimmungen 12
1.1.1. Computergestütztes System 12
1.1.2. Validierung 12
1.1.3. Qualifizierung 13
1.1.4. Lebenszyklus 14
1.2. Risikomanagement 14
1.3. Personal, Rollen und Verantwortlichkeiten 15
1.3.1. Leitung der Prüfeinrichtung 15
1.3.2. Prüfleiter 16
1.3.3. Qualitätssicherung 16
1.4. Einrichtungen 17
1.5. Inventar 17
1.6. Lieferant 17
1.7. Handelsübliche Standardprodukte (COTS) 18
1.8. Änderungs-und Konfigurationskontrolle 19
1.9. Anforderungen an die Dokumentation 19
2. PROJEKTPHASE 21
2.1. Validierung 21
2.2. Änderungskontrolle während der Validierungsphase 21
2.3. Systembeschreibung 21
2.4. Benutzeranforderungsspezifikationen 22
2.5. Qualitätsmanagementsystem und unterstützende Verfahren 22
2.6. Kundenspezifische Systeme 22
2.7. Prüfungen 23
2.8. Datenmigration 23
2.9. Datenaustausch 24
3. BETRIEBSPHASE 25
3.1. Genauigkeitskontrollen 25
3.2 Daten und Datenspeicherung 25
3.3. Ausdrucke 26
3.4. Audit-Trails 26
3.5. Änderungs- und Konfigurationsmanagement 27
3.6. Regelmäßige Überprüfung 28
3.7. Physische, logische Datensicherheit und Datenintegrität 29

3.8. Störfallmanagement 30
3.9. Elektronische Unterschrift 30
3.10. Datenfreigabe 32
3.11. Archivierung 32
3.12 Desaster Recovery (Wiederherstellung nach Systemausfällen) 33
4. STILLLEGUNGSPHASE 34
5. REFERENZEN 35
Anlage 1: Rollen und Verantwortlichkeiten 36
Anlage 2: Glossar 37

1. EINLEITUNG

1. Gegenstand des vorliegenden Dokumentes ist die Einführung eines Lebenszyklusansatzes für die Validierung und den Betrieb computergestützter Systeme. Dabei steht die Risikobeurteilung als zentrales Element eines skalierbaren, ökonomischen und effektiven Validierungsprozesses mit Fokus auf Datenintegrität im Mittelpunkt. Mit dem vorliegenden Dokument soll eine Orientierungshilfe und Anleitung gegeben werden, die es Prüfeinrichtungen ermöglicht, eine geeignete Strategie für die Validierung und den Betrieb jeglicher Art von computergestützten Systemen in einer GLP-Umgebung zu entwickeln, ungeachtet ihrer Komplexität.

1.1. Anwendungsbereich und Begriffsbestimmungen

2. Die jeweiligen Begriffe sind im Glossar in Anlage 2 definiert.

1.1.1. Computergestütztes System

3. Diese Leitlinien gelten für alle Arten von computergestützten Systemen, die in GLP-geregelten Maßnahmen zum Einsatz kommen, ungeachtet ihrer Komplexität (sie reichen von einfachen Geräten, wie Waagen, bis hin zu komplexeren Geräten, wie Einzelplatz-PCs, die laborbasierte Geräte und komplexe Systeme, wie z. B. Laborinformations- und Managementsysteme, steuern). Das computergestützte System besteht aus Hardware, Software und Schnittstellen zu dessen Betriebsumgebung. Die Hardware besteht aus den physischen Komponenten des computergestützten Systems. Sie umfasst die Computereinheit als solche sowie deren periphere Komponenten. Die Software ist das Programm/sind die Programme, das/die den Betrieb des computergestützten Systems steuert/steuern. Alle GLP-Grundsätze, die für Ausrüstungen gelten, gelten daher sowohl für Hardware als auch für Software. Während der Planung, Durchführung, Berichterstattung und Archivierung von Prüfungen werden verschiedene computergestützte Systeme für eine Reihe unterschiedlicher Zwecke verwendet. Diese sind beispielsweise die direkte oder indirekte Datenerfassung durch automatisierte Geräte, der Betrieb/die Steuerung automatisierter Geräte und die Verarbeitung und Speicherung der Daten sowie die Berichterstattung. Dafür müssen entsprechende Abläufe für die Kontrolle, Wartung und für den Betrieb von computergestützten Systemen installiert sein.

1.1.2. Validierung

4. Der Nachweis, dass ein computergestütztes System während seines Lebenszyklus für seinen vorgesehenen Zweck geeignet ist, ist von grundlegender Bedeutung und wird als Validierung von computergestützten Systemen bezeichnet. Alle computergestützten Systeme, die zur Erzeugung, Messung, Kalkulation, Auswertung, Übertragung, Verarbeitung, Speicherung oder Archivierung von Daten eingesetzt werden, die nach entsprechenden nationalen Vorschriften einer Bewertungsbehörde im Rahmen eines Zulassungs-, Erlaubnis-, Registrierungs-, Anmelde- oder Mitteilungsverfahrens oder zur Unterstützung von Zulassungsentscheidungen vorzulegen sind, müssen in Übereinstimmung mit den GLP-Grundsätzen validiert, betrieben und gewartet werden. Die gleichen Anforderungen gelten auch für

computergestützte Systeme, die für die Erzeugung anderer GLP-relevanter Daten genutzt werden, wie zum Beispiel von Rohdatensätzen, Umweltbedingungen, Personal- und Schulungsprotokollen, Instandhaltungsdokumentationen usw. Der Prozess, den ein computergestütztes System durchführt, muss zuverlässig und zweckmäßig sein. Der Validierungsprozess muss ein hohes Maß an Sicherheit dahingehend garantieren, dass ein computergestütztes System seine vorab definierten Spezifikationen erfüllt. Die Validierung muss mithilfe eines formalen Validierungsplans erfolgen und vor der Verwendung im Regelbetrieb durchgeführt werden.

5. Die Validierung neu eingerichteter computergestützter Systeme muss prospektiv durchgeführt werden. In Abhängigkeit von Größe, Kritikalität und Neuheit des Systems muss das Testen möglichst in einer bestimmten Validierungsumgebung stattfinden, bevor der Übergang in die Laborumgebung erfolgt. Es muss gewährleistet sein, dass die Validierungsumgebung äquivalent zur Laborumgebung ist, damit eine Simulation in geeigneter Art und Weise erfolgt. Es muss eine entsprechende Änderungskontrolle im Verlauf des Lebenszyklus des Systems einschließlich seiner Stilllegung vorhanden sein.

6. Eine retrospektive Validierung ist erst dann zulässig, wenn der Nutzungsumfang sich verändert hat oder wenn ein vorhandenes System GLP-relevant geworden ist (z. B. wenn die Notwendigkeit der Einhaltung der GLP-Grundsätze nicht vorgesehen oder spezifiziert war). Wo dies auftritt, muss vor Verwendung des Systems in einer GLP-Studie eine dokumentierte Begründung abgegeben werden. Dies muss eine retrospektive Evaluierung zur Bewertung der Eignung beinhalten, die mit der Zusammenstellung relevanter historischer Daten über das computergestützte System beginnt. Diese Aufzeichnungen müssen überprüft und eine schriftliche Zusammenfassung angefertigt werden. Diese retrospektive Zusammenfassung muss Angaben darüber enthalten, welche Nachweise verfügbar sind und welche zusätzlichen Anforderungen noch im Rahmen formaler Akzeptanztests zu prüfen sind, um einen validierten Status zu erreichen.

1.1.3. Qualifizierung

7. Für kommerzielle Standardsysteme (COTS), automatische Ausrüstungen mit geringer Komplexität oder kleine Systeme kann eine formale Qualifizierung anstatt einer Validierung zulässig sein. Aufgrund ihrer extensiven Verwendung kann die Validität der verwendeten Software in den Fällen als gegeben angenommen werden, wo keine Anpassung vorgenommen wurde. Es wird auf die entsprechenden Leitlinien aus dem Bereich Good Manufacturing Practice (Gute Fertigungspraxis, GMP), wie z. B. Anhang 15 zur EU-Richtlinie *Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use*, betreffend „Qualification and Validation" verwiesen.

8. Beispiele für COTS mit geringer Komplexität, automatische Ausrüstungen oder kleinere Systeme können sein: analytische Geräte, wie elektronische Pipetten, Waagen, Photometer und Geräte zu Lagerungszwecken, wie z. B. Kühlschränke, Gefrierschränke usw.

9. Die Leitung der Prüfeinrichtung muss über Kriterien entscheiden und festlegen, wann die Validierungs- und/oder Qualifizierungsansätze für ein computergestütztes System anzuwenden sind. Bei der Festlegung kritischer Prozessparameter sowie von Maßnahmen, die zur Überwachung eines jeden Prozesses zum Einsatz kommen, muss ein risikobasierter Ansatz angewendet werden, um zu gewährleisten, dass das computergestützte System während seines Lebenszyklus sich in einem kontrollierten Zustand befindet. Es wird daher erwartet, dass neben der Verwendung von internen Referenzen bzw. Standards mit klaren vordefinierten Spezifikationen konsequente Kalibrierungs- und Wartungsmaßnahmen zum Einsatz kommen. Es wird die Anwendung von Tools für die statistische Prozesskontrolle (z. B. Qualitätsregelkarten) empfohlen, zudem wird eine langfristige Nachverfolgbarkeit der Überwachungsergebnisse erwartet. Es wird erwartet, dass an den Stellen, an denen Schnittstellen zu anderen Systemen eingerichtet wurden, ein besonderes Augenmerk auf die Kontrolle des Datenflusses gelegt wird und dieser besonders überwacht wird. Es müssen Standardverfahren gelten, die festgelegte Verfahrens- und Kontrollschritte eindeutig beschreiben.

10. In vorab festgelegten Zeiträumen müssen Re-Qualifizierungsmaßnahmen auf Basis identifizierter Risiken durchgeführt werden. Der Qualifizierungsansatz muss detailliert in Verfahrensanweisungen ausgeführt sein.

11. Falls es innerhalb der Prüfeinrichtung zur Anwendung mehrerer gleicher Geräte kommt, können vorhandene Qualifizierungspläne und -berichte als Referenz benutzt werden.

1.1.4. Lebenszyklus

12. Der Validierungsansatz muss risikobasiert sein, und der Leitung der Prüfeinrichtung ist es freigestellt, ein geeignetes Lebenszyklusmodell zu wählen. Es muss sicherstellen, dass die Validierungsmaßnahmen festgelegt sind und auf systematische Weise realisiert werden, angefangen von der Konzeption, dem Verständnis der Anforderungen, über die Entwicklung, Freigabe, operative Nutzung, bis zur Stilllegung des Systems. Alle relevanten Lebenszyklusphasen müssen dokumentiert und festgelegt sein. Dies kann Kauf, Spezifikation, Design, Entwicklung und Prüfung, Implementierung, Betrieb und Stilllegung computergestützte Systeme umfassen. Lebenszyklusaktivitäten müssen, basierend auf einer dokumentierten Risikobeurteilung, skaliert sein. Maßnahmen geringen Umfangs können für einfache Prozesse ausreichend sein, wie zum Beispiel das Wiegen auf einer Einzelplatzwaage. Umfangreichere Maßnahmen können für komplexere Systeme erforderlich sein, wie zum Beispiel für die über Schnittstellen angeschlossenen Laborinformations- und Managementsysteme.

1.2. Risikomanagement

13. Ein Risikomanagement muss über den gesamten Lebenszyklus eines computergestützten Systems hinweg zum Einsatz kommen, um die Sicherung der Datenintegrität und der Qualität der Prüfergebnisse zu gewährleisten. Das Risikomanagement besteht aus Risikoerfassung, Risikobeurteilung, Risikominimierung und Risikokontrolle. Entscheidungen zum Umfang der Validierung und der Kontrollen zur Datenintegrität müssen auf Basis einer dokumentierten Begründung und einer dokumentierten Risikobeurteilung erfolgen. Das Risikomanagement muss mit anderen wichtigen Verfahren verknüpft sein (z. B. mit dem Konfigurations- und Änderungsmanagement, mit Datenhandlingsprozessen, Geschäftsrisiken usw.)

14. Eine Risikoabschätzung muss zur Entwicklung einer adäquaten Validierungsstrategie und zur Skalierung der Validierungsbemühungen genutzt werden. Der Validierungsaufwand muss am Verwendungszweck des Systems und an den potentiellen Risiken für die Datenqualität und Datenintegrität ausgerichtet sein. Das Ergebnis des Risikobeurteilungsprozesses muss in der Konzeption von geeigneten Validierungsmaßnahmen für computergestützte Systeme bzw. für Funktionen von computergestützten Systemen resultieren. Für einen effektiven und effizienten Validierungsansatz ist der angemessene Einsatz einer Risikobeurteilung von Bedeutung. Werden Ergebnisse der Risikobeurteilung in angemessener Weise genutzt, geben diese der Leitung der Prüfeinrichtung eine geeignete Methodik an die Hand, mit der sowohl einfache Laborsysteme als auch komplexe Labordaten-Managementsysteme validiert werden können.

15. Eine Risikobeurteilung von computergestützten Systemen, die sowohl für GLP-Prüfungen als auch non-GLP-Prüfungen genutzt werden, muss auch die möglichen Auswirkungen von non-GLP-Aktivitäten auf GLP-konforme Prüfungen untersuchen. Für solche Systeme bestehen die gleichen Anforderungen bezüglich der Validierung für computergestützte Systeme, die ausschließlich in GLP-Prüfungen eingesetzt werden. Es muss eine klare Unterscheidung zwischen GLP- und non-GLP-Daten vorgenommen werden.

1.3. Personal, Rollen und Verantwortlichkeiten

16. Die GLP-Grundsätze fordern, dass eine Prüfeinrichtung über angemessen qualifiziertes und erfahrenes Personal verfügt und dass dokumentierte aufgabenspezifische Aus- und Fortbildungsprogramme existieren, die die Bereiche der berufsbegleitenden Aus- und Fortbildung und, wo angebracht, die Teilnahme an externen Kursen umfassen. Nachweise dieser Ausbildungen sind aufzubewahren. Diese Bestimmungen sind auch auf Personal anzuwenden, das mit computergestützten Systemen arbeitet. Es müssen die Aufgaben und Verantwortlichkeiten des Personals, der Leitung der Prüfeinrichtung, der Qualitätssicherung, des Prüfleiters und des Prüfpersonals, das computergestützte Systeme benutzt oder wartet, festgelegt und beschrieben werden.

17. Um ein System zu validieren und ein validiertes System zu betreiben, muss es eine enge Zusammenarbeit zwischen der Leitung der Prüfeinrichtung, dem Prüfleiter, dem Qualitätssicherungspersonal, dem IT-Personal und dem Validierungspersonal geben. Das gesamte Personal muss angemessen qualifiziert sein, über den entsprechenden Level an Zugangsberechtigungen und definierten Verantwortlichkeiten verfügen, damit es in der Lage ist, die ihm zugeteilten Aufgaben zu erfüllen.

18. Personal, das computergestützte Systeme validiert, betreibt und wartet, ist dafür verantwortlich, seine Arbeiten in Übereinstimmung mit den GLP-Grundsätzen und den Best Practice-Leitlinien und -Standards durchzuführen (siehe „Quellenangaben“ in Kapitel 5 des vorliegenden Dokuments).

19. Während der Validierung computergestützter Systeme und der Durchführung von GLP-Prüfungen müssen Rollen und Verantwortlichkeiten über Systemzugriffsrechte, Aus- und Fortbildung und allgemeine GLP-Vorgaben definiert und kontrolliert werden. Schulungsprotokolle und Systemzugriffsberechtigungen der Nutzern müssen vorhanden sein und belegen, dass das Personal über ausreichende Kenntnisse und Zugriffsrechte verfügt, so dass es seine jeweiligen Rollen in einer GLP-konformen Weise ausüben wahrnehmen kann.

20. Entsprechende Verträge bzw. Service Level Agreements müssen die GLP-Schulungsanforderungen für IT-Teams auf globaler oder Unternehmensebene oder für externe und interne IT-Dienstleister beinhalten, die möglicherweise nach anderen Qualitätsmanagementsystemen als GLP arbeiten.

21. *Rollen und Verantwortlichkeiten* sind in Anlage 1 beschrieben.

1.3.1. Leitung der Prüfeinrichtung

22. Die Leitung der Prüfeinrichtung trägt die Gesamtverantwortung dafür sicherzustellen, dass Einrichtungen, Ausrüstung, Personal und Verfahren vorhanden sind, um validierte computergestützte Systeme zu erhalten.

23. Dies schließt ein:

a) die Verantwortung zur Ausarbeitung von Verfahren, die gewährleisten, dass computergestützte Systeme zweckmäßig sind und in Übereinstimmung mit den GLP-Grundsätzen betrieben und gewartet werden,
b) die Benennung und effektive Organisation einer ausreichenden Anzahl entsprechend qualifizierten und erfahrenen Personals und
c) die Verpflichtung zur Sicherstellung eines angemessenen Standards für Räumlichkeiten, Ausrüstung und Verfahren für die Datenverarbeitung.

24. Die Leitung der Prüfeinrichtung muss gewährleisten, dass die Verfahren, die zur Erreichung und Aufrechterhaltung des validierten Status der computergestützten Systeme erforderlich sind, verstanden und befolgt werden und dass ihre Einhaltung wirksam überwacht wird.

25. Die Leitung hat Personal zu benennen, bei dem die spezielle Verantwortung für die Entwicklung, Validierung, den Betrieb und die Wartung computergestützter Systeme liegt. Dieses Personal muss angemessen qualifiziert sein und über einschlägige Erfahrung und Ausbildung verfügen, um seine Aufgaben in Übereinstimmung mit den GLP-Grundsätzen zu erfüllen.

26. Die Leitung der lokalen Prüfeinrichtung trägt die Gesamtverantwortung dafür, dass computergestützte Systeme, die in einem größeren Unternehmen bereitgestellt werden, vor Ort in Übereinstimmung mit den GLP-Grundsätzen betrieben und gewartet werden. Schriftliche Vereinbarungen zwischen lokaler Leitung der Prüfeinrichtung und der Mutterorganisation müssen die Verantwortlichkeiten für die Validierung und für den Erhalt des validierten Status sowie für den GLP-konformen Betrieb von computergestützten Systemen eindeutig zuordnen. Die Leitung der Prüfeinrichtung kann Verantwortlichkeiten ganz oder teilweise auf Einzel- oder Gesamt-Systemebene an ausreichend geschultes Personal delegieren (z. B. Übergabe der Gesamtverantwortung für die GLP-Compliance der computergestützten Systeme an einen Systemeigner oder für ein spezielles computergestütztes System an einen Validierungsleiter).

27. Die Leitung der Prüfeinrichtung muss Rollen und Verantwortlichkeiten sowohl für die Validierungsmaßnahmen als auch für den Routinebetrieb eines jeden computergestützten Systems definieren, unabhängig davon, wie komplex das System ist. Potentielle Interessenkonflikte, die im Zusammenhang mit den Rollen und Verantwortlichkeiten entstehen, sind zu berücksichtigen, um Risiken für die Datenintegrität zu vermeiden (z. B. darf Analysepersonal keine Kontrolle über die Audit-Trail-Einstellungen des Systems, mit dem es arbeitet, haben.)

1.3.2. Prüfleiter

28. Der Prüfleiter ist für die Gesamtleitung und die GLP-Compliance der Prüfungen verantwortlich. Der Prüfleiter trägt die Verantwortung dafür, sicherzustellen, dass alle bei den Prüfungen zum Einsatz kommenden computergestützten Systeme validiert sind und bestimmungsgemäß verwendet werden. Die Verantwortlichkeit des Prüfleiters für elektronisch und auf Papier aufgezeichnete Daten ist die gleiche. (Die Daten müssen zuordenbar, lesbar, aktuell, original, fehlerfrei, vollständig, konsistent, dauerhaft und verfügbar sein.) Vor Initiierung einer GLP-Prüfung muss der Prüfleiter den Validierungsstatus aller zum Einsatz kommenden computergestützten Systeme verifizieren.

1.3.3. Qualitätssicherung

29. Das Qualitätssicherungspersonal muss alle GLP-relevanten computergestützten Systeme, die in seiner Prüfeinrichtung bzw. an seinem Prüfstandort eingesetzt werden, kennen. Die Verantwortlichkeiten der Qualitätssicherung für computergestützte Systeme sind von der Leitung der Prüfeinrichtung zu definieren und in Verfahrensanweisungen schriftlich niederzulegen. Die Qualitätssicherung muss in der Lage sein, die valide Verwendung von computergestützten Systemen zu verifizieren. Das Qualitätssicherungsprogramm muss Anweisungen und Anleitungen beinhalten, die sicherstellen, dass eingeführte Standards in allen Lebenszyklusphasen eines Systems eingehalten werden. Aufgaben zur Verifizierung der Standards in den Bereichen Validierung, Betrieb und Wartung von computergestützten Systemen können an Fachleute oder spezialisierte Auditoren (z. B. Systemadministratoren, Systemeigner, externe Fachleute usw.) delegiert werden. Das Qualitätssicherungspersonal muss über ein entsprechendes Aus- und Fortbildungsniveau sowie über entsprechende Zugangsberechtigungen verfügen, die es ihm ermöglicht, wenn nötig, spezielle Computerprozesse zu überprüfen (Überprüfung des Audit Trails, Methoden zur Datenanalyse usw.). Während der Inspektion von Prüfungen muss das

Qualitätssicherungspersonal, falls die Daten nur in einem computergestützten System verfügbar sind, direkten Lesezugriff auf die Daten haben.

30. Prüfleiter und Qualitätssicherungspersonal müssen ausreichend geschult sein, um die relevanten Verfahren für die angemessene Verwendung GLP-relevanter, computergestützter Systeme zu verstehen.

1.4. Einrichtungen

31. Die Standorte für Computerhardware, periphere Komponenten, Kommunikationsausrüstung und elektronische Speichermedien sind mit besonderer Sorgfalt zu wählen. Extreme Temperatur- und Luftfeuchtigkeitswerte, Staub, elektromagnetische Störungen und die Nähe zu Hochspannungskabeln sind zu vermeiden, wenn die Ausrüstung nicht speziell zum Einsatz unter solchen Bedingungen geeignet ist.

32. Die Stromversorgung für Computeranlagen und, wenn deren plötzlicher Ausfall die Ergebnisse der Prüfung beeinträchtigen kann, die Notwendigkeit einer doppelt ausgelegten oder unterbrechungsfreien Stromversorgung für computergestützte Systeme ist ebenfalls zu beachten. Es müssen geeignete Einrichtungen für die sichere Aufbewahrung elektronischer Speichermedien vorhanden sein.

1.5. Inventar

33. Eine aktuelle Aufstellung (Inventarliste) sämtlicher GLP-relevanten computergestützten Systeme und ihrer Funktionen ist vorzuhalten und zu pflegen. Die Liste muss alle GLP-relevanten computergestützten Systeme umfassen, unabhängig von deren Komplexität. In GLP-Prüfungen zum Einsatz kommende computergestützte Systeme müssen rückverfolgbar sein, vom Prüfplan bzw. von der relevanten Prüfmethode bis zur Inventarliste. Die Inventarliste muss den Validierungsstatus, das Fabrikat, Modell bzw. die Version, soweit zutreffend, enthalten, ebenso den Geschäftsprozess- und IT-Systemeigner (Personen, die Verantwortung für das System haben oder für dieses in Haftung genommen werden können).

1.6. Lieferant

34. Wenn Lieferanten (z. B. Dritte, Anbieter, interne IT-Abteilungen, Dienstleister einschließlich Anbieter von Hosting-Diensten) für die Bereitstellung, Installation, Konfiguration, Einbindung, Validierung, Wartung, Modifizierung, Außerbetriebsetzung oder Stilllegung eines computergestützten Systems in Anspruch genommen werden oder mit Dienstleistungen, wie etwa der Datenverarbeitung, Datenspeicherung, Archivierung oder der Erbringung von Cloud-Diensten beauftragt werden, müssen Vereinbarungen (Verträge) zwischen Prüfeinrichtung und Lieferant in Schriftform vorliegen. Diese Vereinbarungen müssen eindeutige Aussagen enthalten, die die Verantwortlichkeiten des Lieferanten darlegen. Zudem müssen diese Vereinbarungen eindeutige Formulierungen zum Dateneigentum beinhalten.

35. Seitens der Leitung der Prüfeinrichtung sind Kompetenz und Zuverlässigkeit des Lieferanten zu überprüfen. Bedarf an und Umfang einer Lieferantenbeurteilung muss auf einer Risikobeurteilung basieren, wobei die Komplexität des computergestützten Systems und die Kritikalität des vom computergestützten System unterstützten Geschäftsprozesses zu berücksichtigen sind. Der Bedarf an der Durchführung eines Audits muss auf einer dokumentierten Risikobeurteilung basieren. Es liegt im Verantwortungsbereich der Leitung der Prüfeinrichtung zu begründen, dass, basierend auf dem bestehenden Risiko, ein Audit erforderlich ist und welcher Art der Audit sein muss.

36. Umfasst der Auswerteumfang einen technischen und auch einen Compliance-Fokus, muss die Hinzuziehung von technischem Fachpersonal sowie von Qualitätssicherungspersonal erwogen werden. Die Leitung der Prüfeinrichtung muss in der Lage sein, die Inspektoren mit Informationen über die Qualitätssysteme der Lieferanten zu versorgen, in Abhängigkeit von den Leistungen, die sie anbieten.

Lieferanten müssen die Konformität zu den GLP-Richtlinien nicht gewährleisten, jedoch müssen sie nach einem dokumentierten Qualitätssystem arbeiten, das von der Leitung der Prüfeinrichtung unter Beteiligung der Abteilung Qualitätssicherung (QA) als akzeptabel verifiziert wurde.

37. Für durch einen Anbieter gelieferte Systeme ist es wahrscheinlich, dass ein Großteil der Dokumentation, die in der Entwicklungsphase erstellt wurde, am Standort des Anbieters vorgehalten wird. In diesem Fall muss die Leitung der Prüfeinrichtung gewährleisten, dass diese sicher aufbewahrt werden. Dies kann einen formalen Vertrag zwischen dem Anbieter und der Prüfeinrichtung erforderlich machen. In diesem Fall muss in der Prüfeinrichtung der Nachweis vorhanden sein, dass eine formelle Bewertung und/oder Lieferantenaudits durchgeführt wurden. Die Prüfeinrichtung muss formale Akzeptanztests der vom Lieferanten gelieferten Systeme durchführen.

38. Die Leitung der Prüfeinrichtung hat in schriftlichen Vereinbarungen festzulegen, wo es Schnittstellen zwischen den Validierungsanweisungen der Prüfeinrichtung und den von einem Lieferanten durchgeführten Aktivitäten gibt. Diese Schnittstellen sind auf die Validierungsphase und auf die Betriebsphase anzuwenden. So müssen zum Beispiel sämtliche von einem Lieferanten durchgeführten Prüfaktivitäten von der Leitung der Prüfeinrichtung evaluiert werden.

39. Gehostete Dienstleistungen (z. B. Plattform-, Software-, Datenspeicherungs-, Backup- oder Prozessdienstleistungen) sind wie jeder andere Lieferantendienst zu behandeln und erfordern schriftliche Vereinbarungen, die die Rollen und Verantwortlichkeiten jeder Seite festlegen. Es liegt im Verantwortungsbereich der Leitung der Prüfeinrichtung, die jeweiligen Services zu evaluieren und einzuschätzen, welches Risiko für die Datenintegrität und die Datenverfügbarkeit besteht. Die Leitung der Prüfeinrichtung muss sich über potentielle Risiken im Klaren sein, die aus der unkontrollierten Nutzung von gehosteten Diensten resultieren.

40. Eine Prüfeinrichtung kann die IT-Abteilung des Unternehmens als Bestandteil der unternehmenseigenen GLP-Einrichtung einbinden. In solchen Fällen muss es eine Berichtslinie zur Leitung der Prüfeinrichtung geben.

1.7. Handelsübliche Standardprodukte (COTS)

41. Ein computergestütztes System kann komplett oder teilweise auf COTS-Produkten basieren. COTS-Produkte können ohne Modifikationen, mit beschränkten oder umfangreichen Konfigurationsänderungen oder sogar mit kundenspezifischer Programmierung verwendet werden. Wie bei jeder anderen Art von Software fordert der Einsatz von COTS-Produkten eine entsprechende Validierung, in Abhängigkeit vom Risiko und der Komplexität der jeweiligen kundenspezifischen Anpassung. Wenn eine Anwendung (z. B. ein Tabellenkalkulationsprogramm) nicht komplex ist, kann es ausreichend sein, die Funktionen im Vergleich zu den Anforderungen zu verifizieren.

42. Benutzeranforderungen sind für alle Anwendungen, die auf einem COTS-Produkt basieren, schriftlich niederzulegen. Dokumentationen, die mit einem handelsüblichen Standardprodukt (COTS) geliefert werden, sind seitens der Leitung der Prüfeinrichtung zu überprüfen, um zu gewährleisten, dass das Standardprodukt die Benutzeranforderungen erfüllen kann.

43. Vorlagen von Tabellenkalkulationen für Berechnungen, die vordefinierte Formeln, selbst geschriebene Gleichungen oder Makros verwenden, sind als selbstentwickelte Anwendungen zu betrachten. Die Validierungsanforderungen für diese Anwendungen sind in den Abschnitten 2 und 3 beschrieben und hängen vom Risiko und der Komplexität ab. Das zugrunde liegende COTS-Produkt erfordert eine entsprechend geeignete Form der Qualifizierung und Dokumentation. Die Qualifizierung des zugrunde liegenden COTS-Produkts allein ist nicht ausreichend.

1.8. Änderungs-und Konfigurationskontrolle

44. Jede Änderung an einem computergestützten System ist in einer kontrollierten Weise sowie in Übereinstimmung mit den schriftlichen Verfahrensweisen für die Änderungskontrollprozeduren durchzuführen. Die Verfahrensweisen für die Änderungskontrolle müssen die Validierungsphase, die Betriebsphase (einschließlich Archivierung) und die Stilllegungsphase des Systems abdecken. Die Leitung der Prüfeinrichtung hat die Rollen und Verantwortlichkeiten derjenigen Personen festzulegen, die in Aktivitäten im Rahmen der Änderungskontrolle involviert sind. Entscheidungen zu Anforderungen an die Änderungskontrolle müssen risikobasiert sein und hängen von der Komplexität und Kritikalität im Hinblick auf die Datenintegrität oder der vom computergestützten System unterstützten Geschäftsprozesse ab. Die bei der Änderungskontrolle angewendete Risikobeurteilung kann eine Softwarekategorisierung nutzen, wie sie in der aktuellen Anleitung ISPE[1] GAMP[2] beschrieben ist.

45. Die Änderungskontrolle hat alle Punkte abzudecken, die eine Revision, Genehmigung und Prüfung durchlaufen und die für eine definierte Konfiguration eines computergestützten Systems relevant sind. Es ist sicherzustellen, dass die Konfiguration eines Systems zu jeder Zeit genauestens beschrieben und dokumentiert ist. Prüfungsspezifische Maßnahmen (z. B. Datenerfassung, Datenkalkulation usw.) müssen bis zu einer bestimmten Konfiguration des computergestützten Systems rückverfolgbar sein, wenn die Konfiguration für die Ergebnisse relevant ist. Die Änderungskontrolle muss Schnittstellen mit der Risikobeurteilung, der Prüfung, der Freigabe sowie mit geeigneten Dokumentationsverfahren aufweisen.

1.9. Anforderungen an die Dokumentation

46. Anforderungen an die Dokumentation in Bezug auf computergestützte Systeme müssen Bestandteil des Qualitätsmanagementsystems sein und sämtliche GLP-relevanten computergestützten Systeme umfassen. Der erforderliche Dokumentationsumfang hängt von der Komplexität und Validierungsstrategie des computergestützten Systems ab. Es muss für jedes computergestützte System eine Dokumentation vorhanden sein, die in der Regel Folgendes umfasst:

a) den Namen und die Version der Software des computergestützten Systems oder eine Software-Identifikationsnummer sowie eine detaillierte und verständliche Beschreibung des Einsatzzwecks des computergestützten Systems;
b) die Hardware, auf der die Software läuft;
c) das in Verbindung mit dem computergestützten System zum Einsatz kommende Betriebssystem und sonstige Systemsoftware (z. B. Tools);
d) die Programmiersprache(n) des computergestützten Systems und/oder Datenbanktools, die nur bei Bedarf zum Einsatz kommen;
e) die wichtigsten vom computergestützten System ausgeführten Funktionen;
f) Eine Übersicht über die in Verbindung mit dem computergestützten System vorkommenden Datentypen und Datenflüsse;

g) Dateistrukturen, Fehler-und Warnmeldungen, die in Verbindung mit der Benutzung des computergestützten Systems auftreten
h) Die Softwarekomponenten des computergestützten Systems, einschließlich Versionsnummern; und
i) Konfigurations- und Kommunikationsverbindungen zwischen Modulen des computergestützten Systems und zu Geräten und anderen Systemen.

---

[1] ISPE - International Society for Pharmaceutical Engineering
[2] GAMP - Good Automated Manufacturing Practice

47. Die Verwendung von computergestützten Systemen ist angemessen zu dokumentieren. Eine derartige Dokumentation umfasst typischerweise unter anderem Folgendes:

a) Verfahren für den Betrieb von computergestützten Systemen (Hardware und Software) und die Verantwortlichkeiten des beteiligten Personals;
b) Verfahren in Bezug auf Sicherheitsmaßnahmen, mit dem Ziel, unbefugte Zugriffe oder unbefugtes Ändern von Daten zu erkennen und zu verhindern;
c) Änderungskontrollverfahren, die die Prozesse zur Autorisierung, Prüfung und Dokumentation von Änderungen an Ausrüstungen (Hardware und Software) beschreiben;
d) Verfahren zur regelmäßigen Überprüfung der fehlerfreien Funktion des gesamten Systems bzw. seiner Komponenten sowie Verfahren zur Aufzeichnung dieser Tests;
e) Verfahren, die die routinemäßige vorbeugende Wartung und Mängelbeseitigung umfassen (diese Verfahren müssen eindeutig und detailliert die Rollen und Verantwortlichkeiten des involvierten Personals darlegen, bei COTS-Systeme ist die Verwendung der Richtlinien und Verfahrensanweisungen des Anbieters zur Durchführung der Arbeiten gegebenenfalls zulässig. Dies ist in einem Service Level Agreement detailliert schriftlich festzuhalten);
f) Verfahren zur Softwareentwicklung, für Akzeptanztests und andere relevante Prüfungen sowie die Dokumentation aller Prüfungen;
g) Verfahren zur Datensicherung und Betriebskontinuität;
h) Verfahren zur Archivierung und zum „Abruf“ aller elektronischen Daten, Softwareversionen und Dokumentationen über die Computerkonfiguration sowie Nachweis aller durchgeführten Maßnahmen;
i) Verfahren zur Überwachung und Auditierung von computergestützten Systemen sowie Nachweis aller durchgeführten Aktivitäten; und
j) Verfahren und Genehmigung für die System-Stilllegung.

48. Falls relevant, sind weitere Leitungs- und Validierungsverfahren zu beschreiben. Diese können unter anderem umfassen: Akquisition, Risikomanagement, Servicemanagement, Validierungsplanung, Anforderungsspezifikation, Designspezifikation, Installation, Systemfreigabe, Rückverfolgbarkeit, Störfallmanagement, Konfigurationsmanagement, Aufzeichnungsmanagement, Personalausstattung, Rollen und Verantwortlichkeiten des Personals und Dokumentenmanagement.

49. Aufzeichnungen und Verfahren müssen vorhanden sein, die die Validierung und Nutzung des computergestützten Systems ausreichend detailliert beschreiben. Diese Aufzeichnungen können unter anderem umfassen: Risikobewertung, Lieferantenbewertung, Service-Level-Vereinbarungen, Anforderungsspezifikationen, Durchführung von Prüfungen, Freigabe, Personal- und Benutzerschulungen, Beschreibung von Störfällen und Änderungen, Konfiguration und Systembetrieb.

50. Die vollständige Dokumentation zu Validierung und Betrieb eines computergestützten Systems ist solange verfügbar zu halten, wie die mit dem System erzeugten Prüfdaten gemäß den geltenden Vorschriften archiviert werden müssen.

2. PROJEKTPHASE

2.1. Validierung

51. Computergestützte Systeme sind so zu konzipieren, dass sie nachweislich für ihren Einsatz in einer GLP-Umgebung geeignet sind. Ihre Einführung muss in einer im Voraus geplanten Art und Weise erfolgen. Die Validierung eines computergestützten Systems, seine Dokumentation sowie die zugehörigen Protokolle müssen die relevanten Schritte des Lebenszyklus umfassen, wie sie durch die Leitung der Prüfeinrichtung definiert sind, basierend auf der Komplexität und dem vorgesehenen Verwendungszweck eines Systems. Der Validierungsaufwand kann skaliert werden und an die Art des Systems angepasst sein, begründet durch die dokumentierte Risikobeurteilung. Bei der Skalierung der Validierungsbemühungen kann die Leitung der Prüfeinrichtung auf Best Practice-Leitlinien zurückgreifen. Die Leitung der Prüfeinrichtung muss in der Lage sein, den Lebenszyklus, die Strategie, die Validierungsstandards, die Protokolle, die Abnahmekriterien, die Verfahrensweisen, die Aufzeichnungen und die dazugehörigen Arbeitsergebnisse basierend auf einer Risikobeurteilung zu begründen. Die Validierungsergebnisse seitens der Leitung der Prüfeinrichtung können auf die Benutzeranforderungsspezifikationen, einen Validierungsplan, die Durchführung von Benutzerakzeptanztests und einen Validierungsbericht beschränkt werden, wenn dies durch die Risikobewertung begründet werden kann.

52. Es muss der Nachweis vorliegen, dass das System in der Prüfeinrichtung entsprechend auf Einhaltung der Abnahmekriterien geprüft worden ist, bevor der Routinebetrieb des Systems aufgenommen wurde. Der formale Akzeptanztest erfordert die Durchführung von Prüfungen nach einem vorab festgelegten Plan sowie die Aufbewahrung dokumentierter Nachweise über alle Prüfverfahren, Prüfdaten, Prüfergebnisse, die formelle Zusammenfassung des Prüfungsablaufs und ein Protokoll über die formelle Akzeptanz.

2.2. Änderungskontrolle während der Validierungsphase

53. Mit dem Beginn des Validierungsprozesses muss ein Änderungskontroll- und Abweichungsmanagement-Prozess vorhanden sein. Falls Aufzeichnungen zum Änderungskontroll- und Abweichungsmanagement als nicht relevant eingestuft werden, ist dies durch die Leitung der Prüfeinrichtung basierend auf einer Risikobeurteilung zu begründen (z. B. ein vereinfachter Validierungsansatz eines weniger komplexen [d. h. einfach konzipierten] Systems).

54. Die Änderungskontrolle während der Entwicklung und Validierung eines Systems muss klar von der Änderungskontrolle während des Systembetriebs unterschieden werden. Die Validierungsdokumentation muss Protokolle zur Änderungskontrolle (wenn zutreffend) und Berichte zu allen im Verlauf des Validierungsprozesses beobachteten Abweichungen enthalten.

2.3. Systembeschreibung

55. Eine Systembeschreibung, die Details zur physischen und logischen Anordnung, zu Datenflüssen und Schnittstellen mit anderen Systemen oder Prozessen, zu Hardware- und Softwarevorgaben sowie zu Sicherheitsmaßnahmen enthält, muss verfügbar sein. Eine aktualisierte Systembeschreibung wie in Kapitel 1.9 beschrieben ist während des gesamten Lebenszyklus des Systems aufzubewahren. Für einfache Systeme mit geringer Komplexität eine weniger ausführliche Beschreibung zulässig.

2.4. Benutzeranforderungsspezifikationen

56. Benutzeranforderungsspezifikationen sind für alle Validierungsmaßnahmen von herausragender Bedeutung und müssen für alle GLP-relevanten computergestützten Systeme unabhängig von der Komplexität des Systems erstellt werden. Benutzeranforderungsspezifikationen müssen die Funktionen eines System beschreiben und auf einem dokumentierten Geschäftsprozess für das System basierend auf den geltenden behördlichen Vorschriften. Eine Risikobeurteilung für die Erstvalidierung muss auf einem Verständnis der Geschäftsprozesse, Benutzeranforderungsspezifikationen und behördlichen Vorschriften basieren.

57. Benutzeranforderungsspezifikationen müssen alle GLP-relevanten Funktionen eines Systems umfassen und müssen in der Risikoabschätzung verwendet werden, um wichtige Funktionen und entsprechende Prüfungsaktivitäten festzulegen. Abhängig von der Komplexität eines Systems müssen Benutzeranforderungsspezifikationen gegebenenfalls auf weitere Spezifikationsdokumente und auf die im Laufe des Lebenszyklus erstellte Prüfdokumentation zurückgeführt werden können.

58. Wenn ein bereitgestelltes System (gekauft oder von einem Lieferanten gehostet) eine größere Anzahl an Funktionen enthält, als benötigt werden, müssen nur die GLP-relevanten Funktionen geprüft werden. Die Validierung muss auch die Funktionen umfassen, die in non-GLP-Prüfungen genutzt werden können und die gegebenenfalls die Verwendung des computergestützten Systems in GLP-Prüfungen beeinträchtigen könnten. Die anderen, außerhalb des Anwendungsbereichs liegenden Funktionen und/oder Funktionalitäten (d. h. für die keine Verwendungsabsicht besteht) sind zu identifizieren, müssen aber nicht geprüft werden.

2.5. Qualitätsmanagementsystem und unterstützende Verfahren

59. Sowohl die Entwicklung eines computergestützten Systems als auch der Validierungsprozess müssen durch ein Qualitätsmanagementsystem geregelt sein. Es muss eine entsprechende Dokumentation darüber vorhanden sein, dass ein System in einer kontrollierten Art und Weise und vorzugsweise gemäß anerkannten Qualitäts- und technische Standards (zum Beispiel ISO 9001) entwickelt wurde. Wenn ein System durch einen Anbieter entwickelt wird, ist die Leitung der Prüfeinrichtung dafür verantwortlich, das Qualitätsmanagementsystem für die Systementwicklung beim Anbieter zu bewerten. Die Leitung der Prüfeinrichtung muss bei der Festlegung der Bewertungsstrategie auf die Risikobeurteilung zurückgreifen.

2.6. Kundenspezifische Systeme[3]

60. Kundenspezifische Systeme werden für einen speziellen Einsatzzweck in einer bestimmten Prüfeinrichtung entwickelt (zum Beispiel spezielle Datenerfassungssysteme für GLP-Prüfungen, Vorlagen für Tabellenkalkulationsprogramme mit Formeln oder Makros, Abfragen, statistische Anwendungen oder Datenauswertungssysteme usw.) Solche computergestützten Systeme können auch speziell für eine oder mehrere GLP-Prüfungen konfiguriert oder entwickelt werden. Kundenspezifische Systeme weisen das höchste intrinsische Risiko auf, wenn keine Erfahrungen aus früheren oder parallelen Einsätzen verfügbar sind. Es muss ein Prozess für die Validierung von kundenspezifischen computergestützten Systemen vorhanden sein, der die formelle Beurteilung und Berichterstattung von Qualitäts- und Leistungsmaßnahmen für alle Lebenszyklusstufen des Systems sicherstellt.

---

[3] Der Quellcode kundenspezifischer Systeme (bzw. der gesamten Software des computergestützten Systems) in einigen OECD-Mitgliedsländern muss für die Leitung der Prüfeinrichtung abrufbar sein, damit sie der Überwachungsbehörde Zugriff auf den Software-Code gewähren kann. Dies kann durch Archivierung einer digitalen Kopie des Quellcodes, durch Treuhandvereinbarungen oder durch schriftliche Vereinbarungen erfolgen.

61. Eine schriftliche Vereinbarung zwischen dem Lieferanten des kundenspezifischen Systems und der Leitung der Prüfeinrichtung ist erforderlich. Darin werden die Rollen und Verantwortlichkeiten in Bezug auf das System sowie seine Validierung beschrieben. Die Validierungsaufwand der Leitung der Prüfeinrichtung muss alle qualitätsrelevanten Maßnahmen des Lieferanten berücksichtigen, auch die am Geschäftssitz des Lieferanten durchgeführten Maßnahmen. Alle ausgelagerten oder internen Aktivitäten des Lieferanten müssen Bestandteil des Lebenszyklus des computergestützten Systems sein.

62. Wenn eine gehostete Anwendung eine kundenspezifisch entwickelte oder konfigurierte Anwendung ist, muss das System sowohl als kundenspezifisches als auch von einem Anbieter geliefertes System bezeichnet werden.

2.7. Prüfungen

63. Es müssen Prüfungen (z. B. Installationsprüfungen, Benutzerakzeptanztests) durchgeführt werden, um zu gewährleisten, dass das System die vordefinierten Anforderungen erfüllt. Es liegt im Verantwortungsbereich der Leitung der Prüfeinrichtung, die Notwendigkeit der Durchführung der Prüfungen zu verstehen und sicherzustellen, dass die Prüfungen sowie die Prüfungsdokumentation vollständig sind. Die Prüfungen müssen auf der Kenntnis über die Geschäftsprozesse und über den Verwendungszweck des Systems basieren. Verfahrensanweisungen müssen beschreiben, wie die Prüfungen durchgeführt werden. Weiterhin müssen die Rollen und Verantwortlichkeiten sowie die Anforderungen an die Dokumentation eindeutig festgelegt sein. Es liegt in der Verantwortung der Leitung der Prüfeinrichtung, orientiert an einer Risikobeurteilung über die Intensität und Umfang der Prüfungen zu entscheiden. Die Leitung der Prüfeinrichtung muss sicherstellen, dass alle Systeme, auch COTS-Systeme, getestet und bewertet werden. Bei ihren Validierungsbemühungen kann die Leitung der Prüfeinrichtung durch die Prüfaktivitäten und Dokumentationsarbeiten des Lieferanten unterstützt werden und können Prüfungen seitens der Prüfeinrichtung ergänzen bzw. ersetzen. Die Leitung der Prüfeinrichtung muss Nachweise über durchgeführte Prüfungen aufbewahren, unabhängig davon, ob diese Prüfungen durch die Prüfeinrichtung oder durch einen Lieferanten durchgeführt worden sind. Durch diese Nachweise kann demonstriert werden, dass geeignete Prüfverfahren und -szenarien angewendet wurden. Insbesondere sind Grenzwerte für System(prozess)parameter, Datenlimits und die Fehlerbehandlung zu berücksichtigen.

64. Die Leitung der Prüfeinrichtung muss prüfverfahrensspezifische Benutzerakzeptanztests in Betracht ziehen, um nachzuweisen, dass das System zur Durchführung einer speziellen GLP-Prüfung geeignet ist (z. B. um die Eignung eines Systems zur Durchführung einer typischen analytischen Bestimmung einschließlich Kalibrierung, Messung, Berechnung und Datenübertragung zu einem Laborinformations- und Managementsystem [LIMS] nachzuweisen.)

65. Es muss eine Schnittstelle zum Änderungskontrollverfahren vorhanden sein. Falls die Prüfungen zu Systemänderungen führen müssen, sind diese über die Änderungskontrolle gemanagt werden. Der Nachweis über die Durchführung angemessener Prüfungen kann über die Aufbewahrung von Aufzeichnungen zu internen Prüfergebnissen oder mit Aufzeichnungen zu Lieferantenaudits erbracht werden.

2.8. Datenmigration

66. Datenmigration kann im Verlaufe einer GLP-Prüfung oder nach Abschluss einer Prüfung auftreten. Datenmigration muss Bestandteil des Validierungsumfangs der Prüfeinrichtung sein, wenn GLP-relevante Daten betroffen sind, unabhängig vom Status einer GLP-Prüfung. Datenmigration kann relevant werden, wenn Prüfungsaufzeichnungen in einem elektronischen System archiviert werden.

67. Werden elektronische Daten von einem System in ein anderes übertragen, so muss der Prozess dokumentiert werden. Es liegt im Verantwortungsbereich der Leitung der Prüfeinrichtung sicherzustellen und nachzuweisen, dass Daten während des Migrationsvorgangs nicht geändert werden. Die Umwandlung

von Daten in ein anderes Format ist als Daten Migration zu bezeichnen (zum Beispiel die Umwandlung aus einem proprietären Datenformat in PDF). Wenn Daten auf ein anderes Medium übertragen werden, ist zu verifizieren, dass es sich um eine exakte Kopie der Daten handelt, bevor die Originaldaten gelöscht werden.

68. Datenmigrationsaufwände können große Unterschiede in Bezug auf Komplexität und Risiken aufweisen. Beispiele sind:

a) Versions-Upgrades;
b) Datenkonvertierung (von einer Datenbank in eine andere; in ein anderes Datenformat; Formatänderung in Zusammenhang mit einem Software Upgrade);
c) Migration im gleichen System (Verschieben von Anwendungen; Datentransfer von einem Server auf einen anderen); und
d) Migration von einem Quell- zu einem Zielsystem.

69. Migrierte Daten müssen verwendbar bleiben und ihren Inhalt sowie ihre Bedeutung beibehalten. Bei einem Migrationsvorgang müssen der Wert und/oder die Bedeutung von und der Link zwischen dem System-Audit-Trail und den elektronischen Signaturen gewährleistet bleiben. Es liegt in der Verantwortung der Leitung der Prüfeinrichtung sicherzustellen, dass der Link zwischen dem lesbaren Audit-Trail bzw. zwischen elektronischen Unterschriften und den auditierten Daten bestehen bleibt.

2.9. Datenaustausch

70. Die Kommunikation zwischen computergestützten Systemen wird grob in zwei Kategorien eingeteilt: Kommunikationen zwischen Computern oder zwischen Computern und peripheren Komponenten. GLP-relevante Daten können automatisch, in einer Richtung oder in beiden Richtungen von einem System zu einem anderen transportiert werden (zum Beispiel von einem externen Datenerfassungssystem zu einer zentralen Datenbank, von einem Spreadsheet zu einem LIMS, von einem Chromatographie-Datenmanagementsystem zu einem LIMS oder von einem Spreadsheet zu einer Statistikanwendung). Alle Kommunikationsverbindungen sind potentielle Fehlerquellen und können zum Datenverlust oder zur Verfälschung von Daten führen. Während der Entwicklung, Validierung, dem Betrieb und der Wartung müssen geeignete Kontrollen der Schnittstellen in Bezug auf die Sicherheit und Systemintegrität durchgeführt werden. Der Austausch elektronischer Daten zwischen Systemen muss geeignete integrierte Kontrollen hinsichtlich der korrekten und sicheren Eingabe und Verarbeitung von Daten beinhalten. Die Netzwerkinfrastruktur muss qualifiziert sein. Diese Vorgabe erfordert jedoch nicht die Validierung einer Standard-Kommunikationsinfrastruktur und deren Verfahren (zum Beispiel die Basis-Kommunikationssprache des Internets TCP/IP [Transmission Control Protocol / Internet Protocol]).

3. BETRIEBSPHASE

71. Alle computergestützten Systeme sind in einer Weise zu betreiben und zu warten, die das Fortbestehen des validierten Zustands gewährleistet.

3.1. Genauigkeitskontrollen

72. Die Leitung der Prüfeinrichtung muss sämtliche GLP-relevanten Daten, die manuell in elektronische Systeme eingegeben wurden, kennen. Die Leitung der Prüfeinrichtung ist dafür verantwortlich, dass alle elektronischen Dateneingabesysteme unabhängig von der Komplexität des jeweiligen Systems entsprechend kontrolliert werden. Zur Identifizierung fehlerhafter Dateneingaben und zur Evaluierung der Kritikalität und der Folgen von falsch und fehlerhaft eingegebenen Daten ist eine Risikobeurteilung anzuwenden. Es sind Strategien zur Risikominimierung zu beschreiben und zu implementieren. Dies könnte dazu führen, dass zusätzliche manuelle und/oder elektronische Kontrollen der Genauigkeit der eingegebenen Daten durch einen zweiten Eingeber oder ein elektronischen Systems erforderlich sind. Wenn automatisierte Kontrollen zur Dateneingabe verwendet werden, müssen sie in die Validierung eines computergestützten Systems einbezogen werden (z. B. automatisch angewendete Validierungsskripts während der manuellen Dateneingabe). Der Umfang des Validierungsaufwands kann basierend auf einer Risikobeurteilung skaliert werden. Die Verwendung nicht validierter Dateneingabesystems ist auszuschließen (z. B. unkontrollierte Verwendung von Tabellenkalkulationen). Wenn für die manuelle Dateneingabe manuelle Kontrollverfahren zur Anwendung kommen, muss das Verfahren durch eine geeignete Dokumentation abgesichert sein, die die Rekonstruktion der Aktivitäten ermöglicht.

3.2 Daten und Datenspeicherung

73. Wenn Daten (Rohdaten, abgeleitete Daten oder Metadaten) elektronisch gespeichert werden, müssen Vorgaben für Datensicherungs- und Archivierungszwecke festgelegt sein. Für alle relevanten Daten muss eine Datensicherung durchgeführt werden, um eine Wiederherstellung nach einem die Systemintegrität gefährdenden Fehlers zu ermöglichen.

74. Gespeicherte Daten müssen sowohl physisch als auch elektronisch gegen Verlust, Beschädigung und/oder Änderung gesichert werden. Gespeicherte Daten müssen auf ihre Wiederherstellbarkeit, Zugänglichkeit, Lesbarkeit und Genauigkeit verifiziert werden. Verifizierungsverfahren von gespeicherten Daten müssen risikobasiert sein. Der Zugriff auf gespeicherte Daten muss während der Aufbewahrungsfrist sichergestellt sein.

75. Hard- und softwareseitige Systemänderungen müssen einen durchgängigen Zugriff zu den Daten sowie eine ständige Aufbewahrung der Daten ermöglichen, ohne dass Risiken bezüglich der Datenintegrität bestehen. Erfolgt ein System- oder Softwareupdate, muss es möglich sein, Daten zu lesen, die von der Vorgängerversion gespeichert wurden oder es müssen andere Methoden zum Lesen alter Daten vorhanden sein. Erläuternde Informationen (zum Beispiel Wartungsprotokolle, Kalibrierungsaufzeichnungen, Konfigurationen usw.), die benötigt werden, um die Validität von Rohdaten zu verifizieren oder um die gesamte Prüfung oder Teile davon zu rekonstruieren, müssen gesichert und in den Archiven aufbewahrt werden. Wenn nötig, muss Software zum Lesen oder zum Rekonstruieren von Daten im Archiv aufbewahrt werden.

76. Bezüglich elektronischer Aufzeichnungen muss die Leitung der Prüfeinrichtung:

a) alle prüfungsrelevanten elektronischen Aufzeichnungen (z. B. Rohdaten, abgeleitete Daten) identifizieren. Es ist erforderlich, dass für jedes computergestützte System Rohdaten benannt werden, ungeachtet dessen, wie die Rohdaten mit dem System in Verbindung stehen (z. B. durch

Speicherung auf einem elektronischen Speichermedium, durch Computer- oder Geräteausdrucke usw.);

b) die Kritikalität der elektronischen Aufzeichnungen für die Qualität der Prüfergebnisse beurteilt haben;
c) potentiellen Risiken, die für die elektronischen Aufzeichnungen bestehen, beurteilt haben;
d) Verfahren zur Risikominimierung eingeführt haben;
e) die Effektivität der Risikovermeidung im Verlaufe des Lebenszyklus überwacht haben.

77. Im Hinblick auf die Verfahren muss die Leitung der Prüfeinrichtung beschreiben, wie elektronische Aufzeichnungen gespeichert werden, wie die Aufzeichnungsintegrität geschützt wird und wie die Lesbarkeit von Aufzeichnungen erhalten wird. Dies beinhaltet für alle GLP-relevanten Zeiträume unter anderem:

a) die physische Zugriffskontrolle auf elektronische Speichermedien (zum Beispiel Maßnahmen zur Kontrolle und Überwachung des Zutritts von Personal zu Serverräumen usw.);
b) die logische (elektronische) Zugriffskontrolle auf gespeicherte Aufzeichnungen (zum Beispiel Berechtigungskonzepte für computergestützte Systeme als Bestandteil der Validierung von computergestützten Systemen, die die Rollen und Rechte in einem GLP-relevanten computergestützten System definieren);
c) den physischen Schutz der Speichermedien vor Verlust oder Zerstörung (z. B. durch Feuer, Feuchtigkeit, schädliche elektrische Fehler oder Anomalien, Diebstahl usw.);
d) den Schutz von gespeicherten elektronischen Aufzeichnungen gegen Verlust und Änderung (z. B. Validierung der Backup-Verfahren einschließlich der Verifizierung von Backup-Daten und ihrer ordnungsgemäßen Speicherung, Anwendung von Audit-Trail-Systemen); und
e) das Sicherstellen des Zugriffs auf und der Lesbarkeit von elektronischen Aufzeichnungen durch Bereitstellung einer geeigneten physischen sowie Software-Umgebung.

78. Die Datenspeicherung muss für jedes computergestützte System berücksichtigt werden, das zur Durchführung von GLP-Prüfungen während der Prüfungsphase und während des Archivierungszeitraums genutzt wird. Die Einbeziehung der Evaluierung in die Prüfungsdokumentation ist nicht erforderlich. Bei der Leitung der Prüfeinrichtung muss jedoch eine Richtlinie vorhanden sein, die erläutert, wie die Datenspeicherung erfolgt und wie die Anforderungen an die Datenspeicherung erfüllt werden. Diese Informationen müssen Bestandteil der Dokumentation zur Systemvalidierung sein. Falls die Prüfeinrichtung die elektronischen Prüfungsdaten an einen Auftraggeber übergibt, geht die Verantwortung für die Datenübertragung an den Auftraggeber über.

3.3. Ausdrucke

79. Erfolgt ein Ausdruck von Daten zur Darstellung von Rohdaten, müssen alle elektronischen Daten, einschließlich der abgeleiteten Daten sowie der Metadaten (und der Informationen über Datenänderungen, wenn diese Änderungen für den Erhalt des korrekten Inhalts und des korrekten Sinngehalts von Daten notwendig sind) ausgedruckt werden. Alternativ müssen alle elektronischen Aufzeichnungen auf einem Bildschirm überprüfbar und in einem von Menschen lesbaren Format vorhanden sein und aufbewahrt werden. Dies umfasst alle Informationen über an Aufzeichnungen vorgenommene Änderungen, wenn diese Änderungen für den korrekten Inhalt und die korrekte Bedeutung relevant sind.

3.4. Audit-Trails

80. Ein Audit-Trail liefert einen dokumentarischen Nachweis über Aktivitäten, die zu einem bestimmten Zeitpunkt Einfluss auf den Inhalt oder die Bedeutung einer Aufzeichnung hatten. Audit-Trails

müssen verfügbar sein und in eine von Menschen lesbare Form umgewandelt werden können. In Abhängigkeit vom System können, um diese Vorgabe zu erfüllen, Log-Dateien in Betracht gezogen werden (oder sie können zusätzlich zu einem Audit-Trail-System herangezogen werden). Sämtliche Änderungen an elektronischen Aufzeichnungen dürfen die ursprünglichen Eintragungen nicht verbergen und müssen mit einem Zeit- und Datumsstempel versehen sein. Sie müssen auf die diejenige Person, die die Änderung vorgenommen hat, rückführbar sein.

81. Audit-Trails müssen für ein computergestütztes System aktiviert und angemessen konfiguriert sein und die Rollen und Verantwortlichkeiten des Prüfungspersonals widerspiegeln. Die Möglichkeit, Modifikationen an den Einstellungen für den Audit-Trail vorzunehmen, muss auf dazu befugtes Personal beschränkt bleiben. Das gesamte an einer Prüfung beteiligte Personal (z. B. Prüfleiter, Leiter von analytischen Abteilungen, Analytiker usw.) darf keine Berechtigung haben, Änderungen an den Audit-Trail-Einstellungen vorzunehmen.

82. Es muss ein System vorhanden sein, das eine risikobasierte Überprüfung der Funktionen des Audit-Trails sowie seiner Einstellungen und der aufgezeichneten Informationen sicherstellt. Die Leitung der Prüfeinrichtung kann unter anderem einzelne Ereignisse zum Anlass nehmen (z. B. das Benutzerverhalten, vermutete Datenintegritätsprobleme), um die Aufzeichnungen des Audit-Trails zu prüfen. Vollständigkeit und Tauglichkeit der Audit-Trail-Funktionen und -einstellungen können betrachtet werden. Das QS-Personal muss mit einbezogen werden. Eine Überprüfung der Audit-Trail-Funktionen muss basieren auf dem Verständnis Systemnutzung, auf der Möglichkeit zur Modifizierung der Aufzeichnungen und Kontrollen, die verhindern sollen, dass böswillige Änderungen an den Aufzeichnungen vorgenommen werden.

83. Das System muss in der Lage sein, Änderungen, die an vorher eingegebenen Daten vorgenommen wurden, kenntlich zu machen, sowohl auf dem Bildschirm als auch in allen Ausdrucken. Die originalen und modifizierten Eintragungen sind vom System aufzubewahren. Audit-Trails können in einigen Systemen als Änderungsnachweis verwendet werden, ergänzend zur Anzeige der Daten (auf dem Bildschirm oder im Ausdruck). Die Originaldaten müssen gemeinsam mit den modifizierten Daten abgespeichert werden. So müssen erneut integrierte Chromatogramme, die für eine Neuberechnung modifiziert worden sind, unveränderbar gekennzeichnet sein.

3.5. Änderungs- und Konfigurationsmanagement

84. Die Leitung der Prüfeinrichtung muss über geeignete Verfahren, die das Konfigurationsmanagement und das Änderungsmanagement in der Betriebsphase ermöglichen, verfügen. Sowohl das Änderungsmanagement als auch das Konfigurationsmanagement sind für Hardware und Software anzuwenden. Änderungskontrollmaßnahmen müssen gewährleisten, dass Änderungen an der Konfiguration des computergestützten Systems, die den Validierungsstatus beeinflussen können, kontrolliert umgesetzt werden. Eine Änderung muss auf die entsprechenden Aufzeichnungen, die über die erfolgte Änderungs- und Konfigurationskontrolle angefertigt wurden, rückführbar sein. Verfahren müssen die Bewertungsmethode beschreiben, die für die Festlegung des Umfangs der Nachprüfung nötig ist, um den validierten Status des Systems aufrecht zu erhalten.

85. Änderungskontrollverfahren müssen die Rollen und Verantwortlichkeiten für den Zugriff auf und die Genehmigung von Änderungen eindeutig definieren und die Verfahren zur Bewertung der Änderung detailliert beschreiben. Ungeachtet der Herkunft der Änderung (Lieferanten- oder eigenentwickeltes System) sind entsprechende Informationen als Bestandteil des Änderungskontrollprozesses zur Verfügung zu stellen. Während des Änderungskontrollprozesses ist die Datenintegrität sicherzustellen.

86. Die Konfiguration eines computergestützten Systems muss zu jedem Zeitpunkt seines Lebenszyklus bekannt sein, angefangen von den ersten Schritten der Systementwicklung bis zur Stilllegung. In einer GLP-Prüfung, ungeachtet ihrer Komplexität, ist die Übereinstimmung der Konfiguration eines analytischen Gerätes mit den Bestimmungen der Methodenvalidierung zu dokumentieren, um die angemessene Nutzung des computergestützten Systems verdeutlichen. Sämtliche Ergebnisse von GLP-Prüfungen müssen auf die relevante und validierte Systemkonfiguration rückführbar sein, um die Verifizierung der Einstellungen zu ermöglichen, die durch den Prüfplan oder die relevante Methode vorgegeben sind.

87. Änderungen können als Reaktion auf Zwischenfälle oder einrichtungs- bzw. prüfungsspezifische Zwecke erforderlich sein. Nach vorgenommener Modifizierung oder Reparatur ist der Validierungsstatus des Systems zu verifizieren und zu dokumentieren.

88. Änderungen, die durch routinemäßige Automatisierung (z. B. Virenschutz oder Betriebssystem-Patches) implementiert werden, müssen Teil des formalen Änderungs- oder Konfigurationsmanagement sein. Das Fehlen eines Änderungsmanagements für ein computergestütztes System muss begründet werden und auf einer Risikobeurteilung basieren.

3.6. Regelmäßige Überprüfung

89. Computergestützte Systeme sind regelmäßig zu überprüfen, um sicherzustellen, dass sie sich weiterhin in einem validierten Zustand befinden, sich in Compliance mit GLP befinden und auch zukünftig die festgelegten Leistungskriterien erfüllen (z. B. Zuverlässigkeit, Antwortverhalten, Kapazität usw.) Die Überprüfung muss gegebenenfalls den aktuellen Funktionsumfang, Abweichungsaufzeichnungen, Störfälle, die Upgrade-Historie, die Leistung, Zuverlässigkeit und Sicherheit umfassen, die möglicherweise Auswirkungen auf den Validierungsstatus des Systems gehabt haben könnten. Die Häufigkeit und Intensität der regelmäßigen Überprüfungen muss basierend auf einer Risikobeurteilung festgelegt werden, wobei die Komplexität und GLP-Kritikalität zu berücksichtigen ist. Die regelmäßige Überprüfung muss sämtliche gemeldete unerwartete Ereignisse berücksichtigen, die möglicherweise Auswirkungen auf den Validierungsstatus des Systems gehabt haben könnten. Die Angemessenheit der Überprüfungsmaßnahmen und die Einbeziehung von Fachpersonal sowie von GLP-relevantem Personal (z. B. Leitung der Prüfeinrichtung, Qualitätssicherung, Personal für den IT-Support, Lieferanten usw.) ist zu begründen. Die Verantwortlichkeiten des bei der regelmäßigen Überprüfung des Validierungsstatus von computergestützten Systemen beteiligten Personals müssen festgelegt werden. Der Bedarf für eine Interaktion zwischen den regelmäßigen Überprüfungsaktivitäten und dem Störfall-Erfassungssystem kann über eine Risikobeurteilung erwogen werden. Ergebnisse der regelmäßigen Überprüfungen und von gegebenenfalls durchgeführten Abhilfemaßnahmen sind zu dokumentieren.

90. Computergestützte Systeme mit geringerer Kritikalität und Komplexität können von der Überprüfung ausgenommen werden, wenn diese Ausschließung auf Grundlage eines Risikos begründet wird. Die regelmäßige Überprüfung kann eventuell unnötig sein, wenn wichtige (Re)validierungsmaßnahmen in jüngster Vergangenheit stattgefunden haben. Aus diesem Grund kann die regelmäßige Überprüfung verschoben werden. Wenn keine unerwarteten Ereignisse gemeldet wurden, die gegebenenfalls Auswirkungen auf den validierten Status gehabt haben könnten, können automatische COTS-Systeme von der Überprüfung ausgenommen werden. Eine regelmäßige Überprüfung der Benutzer ist bei Bedarf durchzuführen (z. B. im Falle von organisatorischen Veränderungen), mindestens jedoch einmal im Jahr, da es Veränderungen bei Personen und bei den Zugriffsrollen geben kann. Die Überprüfung der Benutzer muss auch für COTS erfolgen.

3.7. Physische, logische Datensicherheit und Datenintegrität

91. Es müssen dokumentierte Sicherheitsverfahren, die vom Prüfeinrichtungsmanagement genehmigt sind, zum Schutz der Hardware, Software und der Daten vor Beschädigung, unbefugter Modifikation oder Verlust vorhanden sein. Es müssen geeignete physische und/oder logische Steuerungsmechanismen implementiert sein, in Abhängigkeit von der Komplexität und Kritikalität eines Systems und den Anforderungen des Unternehmens, in dem das System betrieben wird.

92. Geeignete Kontrollmethoden zur Verhinderung unberechtigter physischen Zugriffe auf das System (zum Beispiel Computerhardware, Kommunikationsausrüstungen, periphere Komponenten und elektronische Speichermedien) können sein: die Verwendung von Schlüsseln, Berechtigungskarten, persönliche Codes mit Passwörtern, biometrische Erkennung oder Zugangsbeschränkungen zu speziellen Computeranlagen (z. B. Datenspeicherbereiche, Schnittstellen, Computer, Serverräumen usw.). Die Erstellung, Änderung und Löschung von Zugriffsberechtigungen ist zu protokollieren. Berechtigungsaufzeichnungen müssen regelmäßig überprüft werden, basierend auf der Kritikalität des vom computergestützten System unterstützten Prozesses und wenn relevante organisatorische Veränderungen in der Prüfeinrichtung vorgenommen worden sind.

93. Da die Erhaltung der Datenintegrität ein primäres Ziel der GLP-Grundsätze ist, muss die Leitung der Prüfeinrichtung sicherstellen, dass das Personal um die Bedeutung der Datensicherheit weiß und die vorhandenen Verfahren und Systemfunktionen zur Gewährleistung der Sicherheit kennt und sich bewusst ist, welche Folgen Verstöße gegen die Sicherheitsbestimmungen haben. Diese Systemfunktionen können sein: eine routinemäßige Überwachung des Systemzugriffs, die Implementierung von Datei-Verifizierungsroutinen sowie Ausnahme- und/oder Trendmeldungen.

94. Für Ausrüstungen, die nicht in den speziellen „Computerräumen“ aufbewahrt werden (z. B. Personalcomputer und Endgeräte) muss es eine Zugriffskontrolle zu dem Bereich, in dem die Hardware sich befindet, geben (z. B. Zutrittskontrolle zu einem Gebäude, einem Laborbereich oder einem bestimmten Raum). Sind diese Ausrüstungen voneinander entfernt (remote) untergebracht (z. B. tragbare Komponenten und Modemanbindungen) können zusätzliche Maßnahmen ergriffen werden, die zu begründen sind und risikobasiert sein müssen (z. B. die kryptografische Steuerung).

95. Es ist essentiell, dass nur qualifizierte und genehmigte Softwareversionen zum Einsatz kommen. Alle Daten oder Software aus externen Quellen sind zu kontrollieren. Diese Kontrollen können vom Betriebssystem des Computers vorgenommen werden, durch spezielle Sicherheitsroutinen, durch in Anwendungen eingebettete Routinen oder durch Kombinationen der genannten Möglichkeiten. Systeme zum Speichern von Daten und Dokumenten müssen so designt sein, dass sie Datum, Uhrzeit und Identität von Benutzern aufzeichnen, die Daten eingeben, ändern, bestätigen oder löschen.

96. Der Möglichkeit für die Verfälschung von Daten durch einen bösartigen Code oder durch andere Ursachen ist entgegenzuwirken, wenn dies als notwendig erachtet wird. Es müssen Sicherheitsmaßnahmen ergriffen werden um die Datenintegrität zu gewährleisten sowohl bei einem kurz- als auch langfristigen Systemausfall.

97. Über eine geeignete und gut gepflegte Berechtigungsstrategie müssen die logische Zugriffsrechte zu Domains, Computern, Anwendungen und Daten spezifiziert werden. Benutzerrechte müssen für Betriebssysteme und Anwendungen definiert sein. Sie müssen nach den Vorgaben der Prüfeinrichtung und in Kombination mit den Anforderungen der jeweiligen GLP-Prüfung angepasst werden. Rollen und Verantwortlichkeiten des Personals, die Benutzerrechte vergeben, sind festzulegen.

98. Benutzerrechte innerhalb eines computergestützten Systems dürfen die Datenintegrität nicht beeinträchtigen. Die Aktivitäten des GLP-Prüfungspersonals müssen auf Benutzerrechte und -aktivitäten in

allen relevanten computergestützten Systemen zurückführbar sein, wie sie in den Benutzerberechtigungsdokumenten beschrieben sind. Administratorrechte dürfen nicht an Personen ausgegeben werden, die ein potenzielles Interesse an den Daten haben (z. B. ist in einem Chromatographie-Datenverwaltungssystem die Laborfunktion „Analytiker“ nicht mit der Systemfunktion „Administrator“ vereinbar). In einem System darf ein Benutzer keine zweite Rolle innehaben, die die Anforderungen an die Datenintegrität beeinträchtigen könnte.

3.8. Störfallmanagement

99. Im Laufe des täglichen Systembetriebs sind Aufzeichnungen über alle festgestellten Probleme oder Inkonsistenzen sowie über die durchgeführten Abhilfemaßnahmen zu führen. Der Prüfleiter, die Leitung der Prüfeinrichtung, die Qualitätssicherung und gegebenenfalls der Auftraggeber müssen über Störfälle, die Abhilfemaßnahmen erfordern, informiert werden. Der Prüfleiter ist verantwortlich für die Festlegung der Kritikalität der Störfälle und für die Einschätzung, ob die Störfälle Einfluss auf die Prüfung haben. Die Grundursache eines Störfalls, die Abhilfemaßnahmen erfordert, muss ermittelt werden und muss die Basis für Korrektur- und Vorbeugemaßnahmen darstellen. Für die Korrektur- und Vorbeugemaßnahmen sind Prioritäten festzulegen. Es muss möglich sein, alle Störfälle, die für ein computergesteuertes System dokumentierte Abhilfemaßnahmen erfordern, bis zu den GLP-Prüfungen und umgekehrt nachzuverfolgen.

100. Störfallaufzeichnungen sind mit der Systemdokumentation aufzubewahren und müssen regelmäßig archiviert werden. Störfallaufzeichnungen müssen innerhalb der systemrelevanten (Validierungs)dokumentation archiviert und gespeichert werden, da sie zur Überwachung und regelmäßigen Überprüfung benötigt werden.

Die Leitung der Prüfeinrichtung muss das Störfallmanagement mit dem Änderungsmanagement, dem Konfigurationsmanagement, der regelmäßigen Überprüfung und der Aus- und Fortbildung verknüpfen bzw. integrieren. Die Überprüfung von Störfällen muss Bestandteil der regelmäßigen System-Evaluierung sein.

3.9. Elektronische Unterschrift

101. Elektronische Aufzeichnungen können elektronisch durch Anbringen einer elektronischen Unterschrift unterschrieben werden.

102. Von elektronischen Unterschriften wird erwartet, dass sie

a) die gleichen rechtlichen Konsequenzen haben wie handschriftlich geleistete Unterschriften, zumindest in der Prüfeinrichtung;
b) auf Dauer mit ihren (ihrer) entsprechenden Aufzeichnung(en) verknüpft ist (sind);
c) Uhrzeit und Datum beinhalten, zu der (dem) sie geleistet wurden;
d) die Identifizierung des Unterzeichneten ermöglichen und die Bedeutung der Unterschrift angeben.

103. Eine elektronische Unterschriftsfunktion eines computergestützten Systems muss in den Systemanforderungen erwähnt sein und in den Systemverfahren validiert und beschrieben sein. Die Leitung der Prüfeinrichtung muss festgelegen, welche Aufzeichnungen eine handschriftliche Unterschrift oder eine elektronische Unterschrift benötigen. Es ist die Entscheidung der Leitung der Prüfeinrichtung, die elektronische Unterschriftsfunktion einzusetzen, auch wenn andere Möglichkeiten zur Verfügung stehen (z. B. das Ausdrucken und Unterzeichnen von Hand). Das zur Anwendung kommende Verfahren ist in geeigneter Weise zu beschreiben.

104. Die Leitung der Prüfeinrichtung muss sicherstellen, dass eine Richtlinie zum Thema elektronische Unterschrift erarbeitet wird, das die ordnungsgemäße Verwendung und Wartung der elektronischen Unterschriftsfunktionen des computergestützten Systems gewährleistet. Personen, die berechtigt sind, elektronische Unterschriften zu leisten, sind eindeutig unter Angabe ihres Namens zu benennen. Der Name muss in die Richtlinien zur elektronischen Unterschrift eingebunden sein. Die Rolle einer Person in einer GLP-Prüfung muss sich in der Bedeutung der dazugehörigen elektronischen Unterschrift, eingefügt durch ein prüfungsrelevantes computergestütztes System, widerspiegeln und muss bis zur Berechtigungsrichtlinie des Systems rückführbar sein. Gegebenenfalls muss das Berechtigungskonzept des computergestützten Systems an prüfspezifische Anforderungen anzupassen.

105. Die Leitung der Prüfeinrichtung muss gewährleisten, dass die elektronische Unterschrift äquivalent zur handschriftlich geleisteten Unterschrift ist und dass deren Authentizität unumstritten ist, zumindest innerhalb der Grenzen der Prüfeinrichtung oder des Prüfstandortes. Die erneute Passworteingabe ist als Mindestvoraussetzung für eine elektronische Unterschrift anzusehen. Die Betätigung einer Funktionstaste durch eine am System angemeldete Person ist nicht als elektronische Unterschrift anzusehen.

106. Metadaten, die mit der elektronisch unterzeichneten Aufzeichnung verbunden sind, müssen eindeutig identifiziert sein (z. B. Methodenparameter und Systemkonfiguration, falls für das elektronisch unterzeichnete analytische Ergebnis relevant, usw.) Die Signaturfunktion des computergestützten Systems muss die Gleichzeitigkeit der Verknüpfung zwischen der elektronisch unterzeichneten Aufzeichnung und den erläuternden Metadaten gewährleisten. Es darf für den Benutzer keine Möglichkeit geben, Änderungen an der geleisteten elektronischen Unterschrift oder an der Verknüpfung zu den verbundenen Metadaten vorzunehmen. Wenn elektronisch unterzeichnete Aufzeichnungen oder die unterstützenden Metadaten geändert werden, ist diese Änderung durch die für die Änderung verantwortliche Person zu erläutern, (elektronisch) zu unterzeichnen und mit Datum zu versehen. Der Einfluss der Änderung auf eine elektronisch unterzeichnete Aufzeichnung oder auf die verbundenen Metadaten muss evaluiert werden, da eine Änderung die elektronische Unterschrift außer Kraft setzt.

107. Die Leitung der Prüfeinrichtung kann zur Unterzeichnung von Aufzeichnungen, die von einem elektronischen System ausgedruckt werden, eine „papierbasierte“ Verfahrensweise anwenden. Es muss darauf hingewiesen werden, dass Papierausdrucke von elektronischen Aufzeichnungen möglicherweise nicht alle Informationen enthalten, die für eine vollständige Rekonstruktion der Aktivitäten benötigt werden und den Sinngehalt der Daten zum Ausdruck bringen. Bestimmte unterstützende Metadaten, die für die ausgedruckte/unterzeichnete Aufzeichnung relevant sind, können elektronisch in einer Hybridlösung aufbewahrt werden. Die Verwendung eines solchen Systems muss vollständig in den Verfahrensanweisungen der Prüfeinrichtung erläutert und mittels einer Risikoabschätzung begründet sein. Basierend auf einer Risikobeurteilung muss das Ausdrucken auf Basis eines klaren Verständnisses des Prozesses und der Informationen, die nicht im Ausdruck erfasst sind, erfolgen. Die Hybridlösung muss eindeutig beschrieben werden, um alle zusätzlichen elektronischen Aufzeichnungen oder unterstützenden Metadaten zu identifizieren, welche durch die gedruckte oder unterschriebene Version dargestellt werden. Ein geeignetes System zur Versionskontrolle muss die Gleichzeitigkeit der Verknüpfung zwischen der gedruckten/unterzeichneten und den elektronisch aufbewahrten Aufzeichnungen sicherstellen. Der Zugriff auf modifizierte oder ersetzte Aufzeichnungen zwecks Rückverfolgbarkeit von Änderungen und zwecks Dokumentation von ungültigen Ergebnissen muss möglich sein. Diese Aufzeichnungen müssen jedoch von der routinemäßigen Verwendung ausgeschlossen werden. Wird ein kompletter Satz elektronischer Aufzeichnungen und seine gedruckte Entsprechung parallel aufbewahrt, muss die Leitung der Prüfeinrichtung festlegen, welches die vorgeschriebene Aufzeichnungsart ist, um das entsprechende Kontrollverfahren zur Anwendung zu bringen (Beispiel: Wenn der vollständige Datensatz eines analytischen Systems ausgedruckt und gleichzeitig elektronisch aufbewahrt wird, muss festgelegt sein, welcher Datensatz der vorgeschriebene ist).

3.10. Datenfreigabe

108. Wenn ein Verfahren einen der elektronischen Datenfreigabeprozesse beinhaltet, muss die Datenfreigabefunktion Bestandteil der Systemvalidierung sein. Der Freigabeprozess muss in den Verfahrensanweisungen der Prüfeinrichtung geschrieben sein und im System elektronisch ausgeführt werden.

3.11. Archivierung

109. Im Hinblick auf die Archivierung ergänzt das vorliegende Beratungsdokument das OECD GLP-Beratungsdokument Nr. 15 „Establishment and Control of Archives that Operate in Compliance with the Principles of GLP“.

110. Sämtliche GLP-relevanten Daten können elektronisch archiviert werden. Die GLP-Grundsätze zur Archivierung müssen einheitlich auf elektronische und nichtelektronische Daten angewendet werden. Es ist daher wichtig, elektronische Daten mit der gleichen Zugriffslevelkontrolle, Indexierung und dem gleichen zweckmäßigen „Abruf“ abzuspeichern wie nichtelektronische Daten.

111. Das Anzeigen und Lesen von elektronischen Aufzeichnungen ohne die Möglichkeit, Änderungen oder Löschungen der archivierten elektronischen Aufzeichnungen vorzunehmen oder die Replizierung innerhalb eines computergestützten Systems oder auf ein anderes computergestütztes System stellt kein „Abrufen“ von Aufzeichnungen dar. Nur dann, wenn die Möglichkeit einer Änderung oder Löschung der archivierten Aufzeichnungen besteht, ist dies als Zugriff, Entnahme, „Abruf“ oder Entfernung von Aufzeichnungen und Materialien anzusehen. Der Archivar muss in der Lage sein, die Vergabe des „Lesezugriffs“ auf archivierte elektronische Daten zu kontrollieren, um nachzuweisen, dass die Anforderungen für archivierte Daten eingehalten werden.

112. Während der Archivierungsfrist müssen elektronische Daten zugänglich und lesbar sein, und ihre Integrität muss gewahrt bleiben. Wenn eine Hybridlösung gewählt wird (d. h. Daten in Papierform und elektronische Daten werden parallel aufbewahrt), muss die Leitung der Prüfeinrichtung die für die Archivierung relevanten regulierten Aufzeichnungen festlegen.

113. Die elektronische Archivierung ist als unabhängiges Verfahren zu betrachten, das ordnungsgemäß validiert werden muss. Bei der Konzipierung und Validierung des Archivierungsverfahrens ist eine Risikobeurteilung vorzunehmen. Relevante Hosting-Systeme und Datenformate müssen im Hinblick auf die Zugänglichkeit, Lesbarkeit und die Einflüsse auf die Datenintegrität während der Archivierungsfrist evaluiert werden. Gegebenenfalls muss die Archivierung elektronischer Daten in einem offenen Format in Betracht gezogen werden, das unabhängig von einem proprietären Dateiformat z. B. von dem eines Geräteherstellers ist. Ist Datenkonversion erforderlich, gelten die im Abschnitt 2.8 angeführten Vorgaben. Der Archivar, der die alleinige Verantwortung trägt, kann im Laufe der Verwaltung von elektronischen Daten Aufgaben an qualifiziertes Personal oder automatisierte Prozesse vergeben (z. B. die Zugriffskontrolle). Rollen und Verantwortlichkeiten im Archivierungsprozess sind im OECD GLP-Advisory Dokument Nr. 15 beschrieben.

114. Es sind Verfahren zu implementieren, die die Langzeitintegrität der elektronisch gespeicherten Daten garantieren. Wenn sich Datenmedien, Datenformate, Hardware oder Software von Archivierungssystemen (nicht von Datenerfassungssystemen) im Laufe der Archivierungsfrist ändern, muss die Leitung der Prüfeinrichtung sicherstellen, dass Zugänglichkeit, Lesbarkeit und Integrität der archivierten Daten dadurch nicht negativ beeinflusst werden. Es muss gewährleistet sein und geprüft werden, dass ein Abruf der Daten kontinuierlich möglich ist. Dort, wo Probleme mit Langzeitzugriffen auf Daten festgestellt werden oder wenn computergestützte Systeme stillgelegt werden müssen, sind Verfahren auszuarbeiten, die eine kontinuierliche Lesbarkeit der Daten garantieren. Dies kann beispielsweise die Erstellung von Ausdrucken in Papierform oder die Umwandlung von Daten in ein anderes Format oder die

Übertragung von Daten in ein anderes System umfassen. Wenn die Datenmigration, einschließlich der Umwandlung in ein anderes Datenformat oder Ausdrucken relevant ist, müssen die Anforderungen der vorliegenden Leitlinien in Bezug auf die Datenmigration erfüllt sein. Risikobeurteilung, Änderungskontrolle, Konfigurationsmanagement und das Prüfungsverlauf müssen als relevante Standardverfahren angesehen werden, wenn Änderungen am Archivierungssystem erforderlich sind. Da Inhalt und die Bedeutung sämtlicher elektronischer Daten im Laufe der Archivierungsfrist erhalten werden müssen, ist das komplette Informationspaket zu identifizieren und zu archivieren (z. B. Rohdaten, Metadaten, die benötigt werden, um die Bedeutung einer Aufzeichnung oder deren Herkunft, elektronische Unterschriften, Audit-Trails usw. richtig zu verstehen).

115. Wenn eine elektronisch unterzeichnete Aufzeichnung elektronisch archiviert wird, ist deren Integrität für den relevanten Zeitraum zu garantieren. Innerhalb der Archivierungsfrist muss es möglich sein, eine Verifizierung der Integrität der mit der Unterschrift versehenen Aufzeichnung, der unterstützenden Metadaten und der elektronischen Unterschrift vorzunehmen. Die Verifizierung muss innerhalb der Archivierungsfrist einer Evaluierung unterzogen werden. Die Periodizität der Evaluierung muss seitens der Leitung der Prüfeinrichtung basierend auf der Risikoabschätzung legitimiert werden.

116. Im Prüfbericht muss der Prüfleiter sämtliche GLP-relevanten elektronischen Daten angeben, die elektronisch zu archivieren sind, weiterhin muss er den Speicherort des elektronischen Archivs benennen.

117. Alle zur Unterstützung der relevanten computergestützter Systeme aufbewahrten Daten, wie Quellcode und Aufzeichnungen zu Entwicklung, Validierung, Betrieb, Wartung und Überwachung müssen mindestens so lange aufbewahrt werden, wie die Aufzeichnungen der Prüfungen, für die das System verwendet wurde.

118. Elektronisch gespeicherten Daten dürfen nicht ohne Genehmigung durch die Leitung der Prüfeinrichtung oder, wenn zutreffend, des Auftraggebers und ohne entsprechende Dokumentation vernichtet werden.

3.12 Desaster Recovery (Wiederherstellung nach Systemausfällen)

119. Es sind Vorkehrungen zu treffen, die bei einem Systemausfall die Kontinuität der Unterstützung für computergestützte Systeme, die für GLP-relevante Prozesse verwendet werden, gewährleisten (z. B. manuelle Dateneingabe oder Einsatz eines alternativen computergestützten Systems). Die für den Einsatz der alternativ vorgesehenen Technik benötigte Zeit muss auf einer Risikobeurteilung basieren, die für ein bestimmtes System und den Geschäftsprozess, den das System unterstützt, angemessen sein muss. Die Vorkehrungen müssen entsprechend dokumentiert und getestet sein.

120. Es müssen Verfahren vorliegen, die die für den Fall des teilweisen oder totalen Ausfalls des computergestützten Systems zu treffenden Maßnahmen beschreiben. Diese Maßnahmen können von geplanter Hardware-Redundanz bis zum Rückgriff auf ein alternatives System reichen. Notfallpläne zur Fortsetzung der Prüfung nach Systemausfällen müssen validiert und ausreichend gut dokumentiert sein, sie müssen die Datenintegrität in allen Phasen sicherstellen und dürfen die Prüfung nicht verfälschen. Personal, das an der Durchführung von Prüfungen nach den GLP-Grundsätzen beteiligt ist, muss diese Notfallpläne kennen.

121. Die zur Wiederherstellung der Funktion eines ausgefallenen computergestützten Systems erforderlichen Verfahren hängen von der Kritikalität des Systems ab. Essentiell ist, dass Sicherungskopien der gesamten eingesetzten Software in der für das validierte computergestützte System relevanten Version aufbewahrt werden, bei einem Dritten hinterlegt sind oder gemäß Service Level Agreement verfügbar sind. Wenn Wiederherstellungsverfahren Änderungen an Hard- oder Software zur Folge haben, gelten die Validierungsanforderungen dieser Leitlinie.

122. Wenn ein alternatives Verfahren zur Datenerfassung zur Anwendung kommt, bei dem die manuell aufgezeichneten Daten danach in den Computer eingegeben werden, müssen die Daten deutlich als solche gekennzeichnet werden. Der Dateneingabeprozess muss validiert werden, und es muss eine Aussage getroffen werden, dass die eingegebenen Daten äquivalent den manuell aufgezeichneten Rohdaten sind. Die manuell aufgezeichneten Rohdaten sind als Originalrohdaten zu erhalten und zu archivieren. Der komplette Aufbewahrungszeitraum ist für die manuell aufgezeichneten Rohdaten erforderlich. Alternative Back-up-Verfahren müssen dazu dienen, das Risiko des Datenverlustes zu minimieren und garantieren, dass diese alternativen Aufzeichnungen erhalten bleiben.

4. STILLLEGUNGSPHASE

123. Die Systemstilllegung ist als eine Phase des Lebenszyklus des Systems zu betrachten. Sie ist zu planen, muss risikobasiert sein und dokumentiert werden. Für den Fall der Notwendigkeit der Migration oder Archivierung GLP-relevanter Daten sind Risiken für die Daten auszuschließen. Es gelten die Vorgaben der vorliegenden Richtlinie.

5. REFERENZEN

„Good Practices for Computerised Systems in Regulated GxP Environments" [gültige Fassung vom 25.09.2007] PIC/S PI 11-3

„Computerised Systems used in Nonclinical Safety Assessment: Current Concepts in Validation and Compliance" [veröffentlicht 2008, DIA, Red Apple II]."

„GAMP 5 - A Risk Based Approach to Compliant GxP Computerised Systems" ISPE Good Automated Manufacturing Practice © ISPE 2007

„Establishment and Control of Archives that Operate in Compliance with the Principles of GLP", [ENV/JM/MONO(2007)10], OECD GLP-Advisory Dokument Nr. 15.

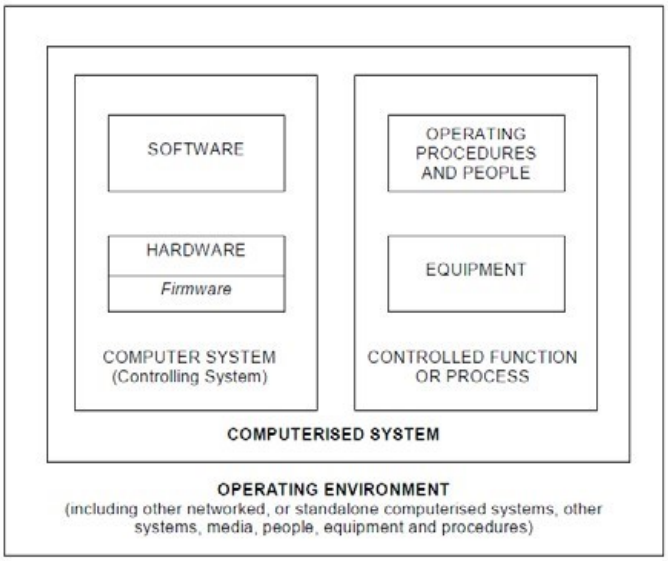
Die Regelung der Arzneimittel in der Europäischen Union. Band 4 - Guidelines for good manufacturing practices for medicinal products for human and veterinary use. Anhang 15 zur EU-Richtlinie Guidelines for Good Manufacturing Practice betreffend „Qualification and Validation", Oktober 2015.

Anlage 1: Rollen und Verantwortlichkeiten

Rolle	Verantwortlichkeit
Geschäftsprozesseigner	Person oder Unternehmen, verantwortlich für die Bereitstellung von Ressourcen für einen Geschäftsprozess (z. B. für eine präklinische Studie)
IT-Personal	Am Kauf, der Installation und der Wartung eines computergestützten Systems beteiligtes Personal. Die Zuständigkeit umfasst beispielsweise den Betrieb und die Wartung der Hardware und Software, die Durchführung von Datensicherungen (Backups), das Lösen von Problemen usw.
Personal	Alle an der Validierung, dem Betrieb bzw. dem Support eines computergestützten Systems beteiligte Personen.
Qualitätssicherung	(*Siehe* ENV/MC/CHEM(98)17 „OECD Principles of GLP", (1997), 2.2.8.)
Auftraggeber	(*Siehe* ENV/MC/CHEM(98)17 „OECD Principles of GLP", (1997), 2.2.5.)
Prüfleiter	(*Siehe* ENV/MC/CHEM(98)17 „OECD Principles of GLP", (1997), 2.2.6.)
Lieferant	Dritte, Anbieter, interne IT-Abteilungen, Dienstleister einschließlich Anbieter von Hosting-Diensten usw.
Systemeigner/IT-Eigner	Diejenige Person, die für die Verfügbarkeit, den Support und die Wartung eines Systems sowie für die Sicherheit der auf diesem System befindlichen Daten zuständig ist. Der Systemeigner trägt die Verantwortung dafür, dass Support und Wartung des computergestützten Systems in Übereinstimmung mit den geltenden Verfahrensanweisungen erfolgen. Der Systemeigner fungiert im Auftrag der Leitung der Prüfeinrichtung. Globale IT-Systeme können einen globalen Systemeigner haben sowie über lokal ansässige Systemeigner verfügen, die die Implementierung vor Ort organisieren (siehe GAMP 5).
Leitung der Prüfeinrichtung	(*Siehe* ENV/MC/CHEM(98)17 „OECD Principles of GLP", (1997), 2.2.3.)
Benutzer	Person, die das computergestützte System in einer GLP-Prüfung betreibt.
Validierungsleiter	Eine benannte für ein Validierungsprojekt zuständige Person.

Anlage 2: Glossar

Begriff	Definition
Akzeptanzkriterien	Dokumentierte Kriterien, die erfüllt werden müssen, um eine Testphase erfolgreich abzuschließen oder den Anforderungen für die Auslieferung zu entsprechen.
Akzeptanztest	Formaler Test des gesamten computergestützten Systems in der voraussichtlichen Systemumgebung zur Feststellung, ob alle Akzeptanzkriterien der Prüfeinrichtung erfüllt wurden und ob das System für den Einsatz geeignet ist.
Berechtigungskonzept	Ein Berechtigungskonzept ist ein formelles Verfahren zur Festlegung und Steuerung von Zugriffsrechten auf ein computergestütztes System und von Rechten in einem computergestützten System.
Datensicherung (Backup)	Vorsorgliche Maßnahmen zur Wiederherstellung von Datenfiles oder Software zur Wiederaufnahme/zum Neustart der Datenverarbeitung oder der Benutzung einer Ersatz-Computeranlage nach einer Betriebsstörung oder einem Ausfall des Systems.
Änderungskontrolle	Laufende Evaluierung und Dokumentation der Systemfunktionen und Änderungen, um zu bestimmen, ob ein Validierungsprozess nach einer Änderung des computergestützten Systems erforderlich ist.
Änderungsmanagement	Änderungsmanagement ist der Prozess der Steuerung des Lebenszyklus von Änderungen.
Handelsübliches Standardprodukt (COTS)	Software oder Hardware ist ein handelsübliches Standardprodukt (COTS), wenn es der allgemeinen Öffentlichkeit durch einen Anbieter zur Verfügung gestellt wird, wenn es in mehreren und identischen Exemplaren erhältlich ist und wenn es von der Leitung der Prüfeinrichtung ohne Anpassung oder mit einigen kundenspezifischen Anpassungen implementiert wird.
Computergestütztes System	„Ein computergestütztes System ist eine Funktion (ein Prozess oder eine Operation), die in ein Computersystem integriert ist und von ausgebildetem Personal ausgeführt wird. Die Funktion wird vom Computersystem gesteuert. Der Steuerungscomputer besteht aus Hardware und Software. Die zu steuernden Funktionen bestehen aus Geräten, die gesteuert werden und aus Bedienungsabläufen, die von Personal vorgenommen werden.” *PIC/S PI 11-3 „Good Practices for Computerised Systems in Regulated GxP Environments*”



Konfiguration	Eine Konfiguration ist eine Anordnung von Funktionseinheiten und bezieht sich auf die Auswahl von Hardware, Software und Dokumentation. Sie hat Einfluss auf Funktion und Leistung des Systems.
Konfigurations-management	Das Konfigurationsmanagement umfasst Maßnahmen, die erforderlich sind, damit es möglich ist, ein computergestütztes System zu einem bestimmten Zeitpunkt exakt zu definieren.
Gesteuerte Funktion	Eine gesteuerte Funktion ist ein Prozess oder eine Operation, der bzw. die in ein Computersystem integriert ist und von ausgebildetem Personal ausgeführt wird.
Korrektur- und Vorbeugemaßnahmen	Das Konzept von Korrektur- und Vorbeugemaßnahmen konzentriert sich auf die systematische Untersuchung der Grundursachen festgestellter Probleme bzw. Risiken und versucht, deren erneutes Auftreten bzw. deren Auftreten zu verhindern.
Kundenspezifisches computergestütztes System	Ein individuell konzipiertes computergestütztes System, das so gestaltet ist, dass es für spezielle Geschäftsprozesse geeignet ist.
Daten (abgeleitete Daten)	Abgeleitete Daten sind abhängig von Rohdaten und können aus Rohdaten rekonstruiert werden (z. B. mittels Tabellenkalkulation berechnete Endkonzentrationen, gestützt auf Rohdaten, Ergebnistabellen, wie von einem LIMS zusammengefasst usw.).
Daten (Rohdaten)	Daten (Rohdaten) können als messbares oder beschreibbares Attribut einer physischen Einheit, eines Prozesses oder Ereignisses definiert werden. Die GLP-Grundsätze definieren Rohdaten als die gesamten Laboraufzeichnungen und Dokumentationen, einschließlich der Daten, die direkt über eine automatische Geräteschnittstelle in einen Computer eingegeben wurden, wobei die Daten das Ergebnis von Erstbeobachtungen und Maßnahmen in einer Prüfung sind und diese für die Rekonstruktion und Evaluierung des Berichts zu dieser Prüfung benötigt werden.

Datenfreigabe	Datenfreigabe bedeutet die Sperrung von Daten nach deren Erfassung, Validierung und beispielsweise Umwandlung, um die Daten für eine Verwendung in Aufzeichnungen einsetzbar zu machen.
Datenerfassung	Unter Datenerfassung versteht man Maßnahmen, die typischerweise erfolgen, um Daten und dazugehörige Metadatenelemente zu planen, zu erfassen und zu verifizieren.
Datenmigration	Datenmigration ist die Aktivität, die zum Beispiel den Transport von elektronischen Daten von einem Computersystem zu einem anderen, die Übertragung von Daten zwischen Speichermedien oder schlichtweg die Umwandlung von Daten aus einem Stadium in ein anderes (zum Beispiel die Umwandlung von Daten in ein anderes Format) beinhaltet. Der Begriff „Daten“ bezeichnet sowohl „Rohdaten“ als auch „Metadaten”.
Abweichungs-management (Störfallmanagement)	Das Abweichungsmanagement (Störfallmanagement) beinhaltet Aktivitäten zur Identifizierung, Dokumentation, Evaluierung und (wenn nötig) Untersuchung, um die eigentlichen Ursachen für die Abweichung (den Störfall) zu ermitteln und einem erneuten Auftreten vorzubeugen.
Elektronische Aufzeichnung	Alle Kombinationen von textlichen, grafischen, Daten-, Audio-, bildlichen oder sonstigen Informationsdarstellungen in digitaler Form, die mithilfe eines Computersystems erstellt, modifiziert, gepflegt, archiviert, abgerufen oder verteilt werden.
Elektronische Unterschrift	Ein elektronisches Mittel, das an die Stelle einer mit der Hand geleisteten Unterschrift oder an die Stelle von Paraphen treten kann, und zwar zum Zweck der Erteilung von Genehmigungen, Berechtigungen oder zur Verifizierung von speziellen Dateneinträgen.
Hybridlösung (System)	Parallele Existenz von Papieraufzeichnungen, elektronischen Aufzeichnungen und Unterschriftskomponenten. Beispiele sind Kombinationen von Papieraufzeichnungen (oder von anderen nichtelektronischen Medien) und elektronischen Aufzeichnungen, von Papieraufzeichnungen und elektronischen Unterschriften mit der Hand geleisteten Unterschriften, verknüpft mit elektronischen Aufzeichnungen.
Lebenszyklus	Eine Herangehensweise an die Entwicklung von computergestützten Systemen, die mit der Feststellung der Anforderungen des Benutzers beginnt, sich über die Konstruktion, Integration, Zulassung, Benutzervalidierung, Kontrolle und Wartung fortsetzt und mit der Stilllegung des Systems endet.
Lebenszyklusmodell	Ein Lebenszyklusmodell beschreibt die Phasen bzw. Aktivitäten eines bzw. innerhalb eines Projekts, von der Konzeption bis hin zu Stilllegung des Produktes. Er spezifiziert die Beziehungen zwischen Projektphasen, einschließlich Übergangskriterien, Feedbackmechanismen, Meilensteine, Ausgangsbasen, Überprüfungen (Reviews) und abzuliefernde Projektergebnisse

Metadaten	Metadaten sind Daten über Daten. Metadaten sind Informationen, die für die Identifizierung, Beschreibung und das Wirkungsgefüge von elektronischen Aufzeichnungen genutzt werden. Metadaten verleihen Daten ihren Sinngehalt, liefern Kontext, definieren Strukturen und ermöglichen die Wiederauffindbarkeit über Systeme hinweg sowie die Nutzbarkeit, Authentizität und Auditierbarkeit im Laufe der Zeit.
Betriebssystem	Ein Programm oder eine Sammlung von Programmen, Routinen und Subroutinen, die den Betrieb eines Computers steuern. Ein Betriebssystem kann Dienste wie die Zuteilung der Systemressourcen, der Rechenzeit, die Ein-/Ausgabesteuerung und die Datenverwaltung zur Verfügung stellen.
Periphere Komponenten	Alle angeschlossenen Geräte oder Hilfs- bzw. dezentrale Komponenten, wie Drucker, Modems, Terminals etc.
Prozess	Ein Prozess ist eine Reihe von Maßnahmen, die zur Erzielung eines bestimmten Ergebnisses konzipiert sind. Ein Prozess definiert erforderliche Arbeitsaktivitäten und die Verantwortlichkeiten des Personals, das mit der Arbeit betraut wurde. Geeignete Werkzeuge und Ausrüstungen, Verfahren und Methoden definieren die Aufgaben und die Beziehungen der Aufgaben zueinander.
Zulassung	Vorgang der Nachweiserbringung, dass alle Ausrüstungen, einschließlich der Software, ordnungsgemäß funktionieren und auf ihren Zweck ausgerichtet sind.
Anerkannte technische Standards	Standards, die von nationalen oder internationalen Standardisierungsinstitutionen (ISO, IEEE, ANSI etc.) veröffentlicht wurden.
Vorgeschriebene Aufzeichnung	Hierbei handelt es sich um eine Aufzeichnung, die gemäß den GLP-Vorschriften zu pflegen bzw. vorzulegen ist. Eine vorgeschriebene Aufzeichnung kann in verschiedenartigen Formaten vorliegen, z. B. elektronisch, in Papierform oder sowohl als auch.
Risiko	Kombination aus Wahrscheinlichkeit des Eintritts eines Schadens und Schwere dieses Schadens.
Risikoanalyse	Einschätzung des mit den festgestellten Gefährdungen verbundenen Risikos Es ist der qualitative bzw. quantitative Prozess des Verknüpfens der Wahrscheinlichkeit des Auftretens mit dem Schadensausmaß.
Risikobeurteilung	Risikobeurteilung beinhaltet das Feststellen von Gefährdungen und die Analyse und Evaluierung von Risiken, die mit der Gefährdungsexposition in Verbindung stehen. Nach der Risikobeurteilung folgt die Risikokontrolle.

Risikokontrolle	Prozess, durch den Entscheidungen erreicht und Schutzmaßnahmen umgesetzt werden, mit dem Ziel, Risiken so weit zu reduzieren, dass sie ein bestimmtes Niveau erreichen bzw. mit dem Ziel, Risiken auf einem bestimmten Niveau zu halten.
Risikoerfassung	Eine systematische Nutzung von Informationen zur Erfassung von Gefährdungen in Bezug auf die Risikofrage oder Problembeschreibung. Die Informationen können historische Daten, theoretische Analysen, geäußerte Standpunkte und die Bedenken von Beteiligten umfassen.
Risikomanagement	Das Konzept des Qualitäts-Risikomanagements wird als „ein systematischer Prozess" zur Beurteilung, Steuerung, Kommunikation und Überprüfung von für die Qualität bestehenden Risiken beschrieben.
Risikominimierung	Durchführung von Maßnahmen zur Verringerung der Wahrscheinlichkeit des Eintritts eines Schadens und Abschwächung der Schwere dieses Schadens.
Sicherheit	Der Schutz der Computerhardware und -software vor unbeabsichtigtem oder beabsichtigtem Zugriff, Benutzung, Änderung, Zerstörung oder Offenlegung. Sicherheitsüberlegungen betreffen auch Personal, Daten, Kommunikation sowie den physischen und logischen Schutz der Computerinstallationen.
Software	Ein Programm, das erworben oder entwickelt, angepasst oder nach den Anforderungen der Prüfeinrichtung speziell angefertigt wurde zum Zweck der Steuerung von Prozessen, Datenerfassung, Datenbearbeitung, Berichterstattung und/oder Archivierung der Daten.
Quellcode	Das Original eines Computerprogramms in für den Menschen lesbarer Form (Programmiersprache) formuliert, das in eine maschinenlesbare Form übersetzt werden muss, bevor es durch den Computer ausgeführt werden kann.
Benutzeranforderungsspezifikationen	Benutzeranforderungsspezifikationen legen in Schriftform fest, was der Benutzer vom computergestützten System dahingehend erwartet, was es zu leisten in der Lage ist.
Benutzerkontrolle	Kontrolle der Benutzerzugriffsrechte und sonstigen Rechte
Validierung	Vorgang der Nachweiserbringung, dass ein Prozess zu den erwarteten Ergebnissen führt. Die Validierung eines computergestützten Systems erfordert die Gewährleistung und das Nachweisen der Gebrauchstauglichkeit des Systems.
Validierungsstrategie	Die Validierungsstrategie legt in einem Dokument den Prozess und alle Aktivitäten fest, die sich auf die einzelnen Schritte der Validierung des computergestützten Systems beziehen.

Weitere Begriffsbestimmungen finden Sie in den *„OECD-Grundsätzen der Guten Laborpraxis"*.