Die Durchführung von GLP-Inspektionen in Deutschland

Handbuch
Anhang 3:
Inspektion von computergestützten Systemen (CS)

Teil 1:
Erläuterungen zum OECD-Papier

Bund/Länder-Arbeitsgemeinschaft Chemikaliensicherheit
Ausschuss „GLP und andere Qualitätssicherungs-Systeme“
BLAC-AS GLP

Stand: 15.Juni 2019

Anhang 3: Inspektion von computergestützten Systemen (CS)

Mit der Veröffentlichung des Advisory Dokuments Nr. 17 „Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme“ am 22. April 2016 wurde das alte OECD-Konsensdokument Nr. 10 aus 1995 vollständig ersetzt. Dieses Dokument stellt inhaltlich eine Anpassung an die Entwicklungen im Bereich der IT der letzten 20 Jahre dar. Die Erweiterungen betreffen vor allem die Bereiche Risikobetrachtung/-management, Qualifizierung und Validierung sowie Change Management (Veränderungskontrolle).

Deshalb ist der hier vorliegende Anhang auch grundsätzlich neu erstellt worden und orientiert sich am OECD-Dokument Nr. 17. Gleichzeitig wurde aber auch versucht, die Erfahrungen aus den Inspektionen der letzten Jahre einfließen zu lassen. Dies führte dazu, dass ein Wichtung der Inhalte erfolgte, manche Abschnitte des OECD-Papiers wurden intensiver dargestellt, andere nur kurz abgehandelt. Der Anhang wurde bewusst in Erläuterungen zum OECD-Papier und den Fragenkatalog untergliedert.

0. Abkürzungen

Abkürzung	Bedeutung englisch	Bedeutung deutsch
ALCOA	**A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, **A**ccurate	zuschreibbar, lesbar, zeitnah, original, korrekt (Anforderungen an Daten-integrität aus GAMP)
ALCOA +	Complete, Consistent, Enduring, Available *(zusätzlich zu ALCOA)*	vollständig, konsistent, dauerhaft und verfügbar *(zusätzlich zu ALCOA)*
COTS	Commercial of the Shelf System	kommerzielle Standardsysteme
CS	Computerised System	Computergestütztes System
DQ	Design Qualification	Designqualifizierung
eIDAS-(Verordnung)	**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices	elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
GAMP	**G**ood **A**utomated **M**anufacturing **P**ractice	Gute Automatisierte Herstellungspraxis
GAMP 5	Bedeutung: 'A Risk Based Approach to Compliant GxP Computerised Systems"	Bedeutung: 'Leitfaden für die computergestützte Validierung' aus GAMP-Bereich
GC/MS	Gas Chromatography / Mass Spectromety	Gaschromatographie mit Massenspektrometrie-Kopplung
HPLC	High Performance Liquid Chromatography	Hochleistungsflüssigkeitschromatographie
IQ	Installation Qualification	Installationsqualifizierung
IT	Information Technology	Informationstechnik
LIMS	Labor Information and Management System	LaborInformations- und Management-System
LPE	Test facility management	Leitung der Prüfeinrichtung
OQ	Operational Qualification	Funktionsqualifizierung
PC	Personal Computer	Personal Computer
PDF	Portable Document Format	(trans)portables Dokumentenformat
PE	Test facility	Prüfeinrichtung
PL	Study director	Prüfleiter
PP	Study personnel	Prüfendes Personal
PQ	Performance Qualifizierung	(Verfahrens-) Leistungsqualifizierung
QS	Quality Assurance	Qualitätssicherung
SOP	Standard Operting Procedure	Standardarbeitsanweisungen
URS	User Requirement Specification	Benutzeranforderungsspezifikation
TCP/IP	Transmission Control Protocol / Internet Protocol	Bedeutung: Wichtigstes Standardprotokoll für Intranet- und Internet-Datenübertragung

1. Anwendungsbereich und Begriffsbestimmung

(siehe auch Glossar – OECD Nr. 17)

Die Leitlinien sollen für alle Arten von computergestützten Systemen (CS) gelten, unabhängig von der Aufbauweise und Zusammensetzung der Hardware und der Komplexität/Funktionalität der Software.

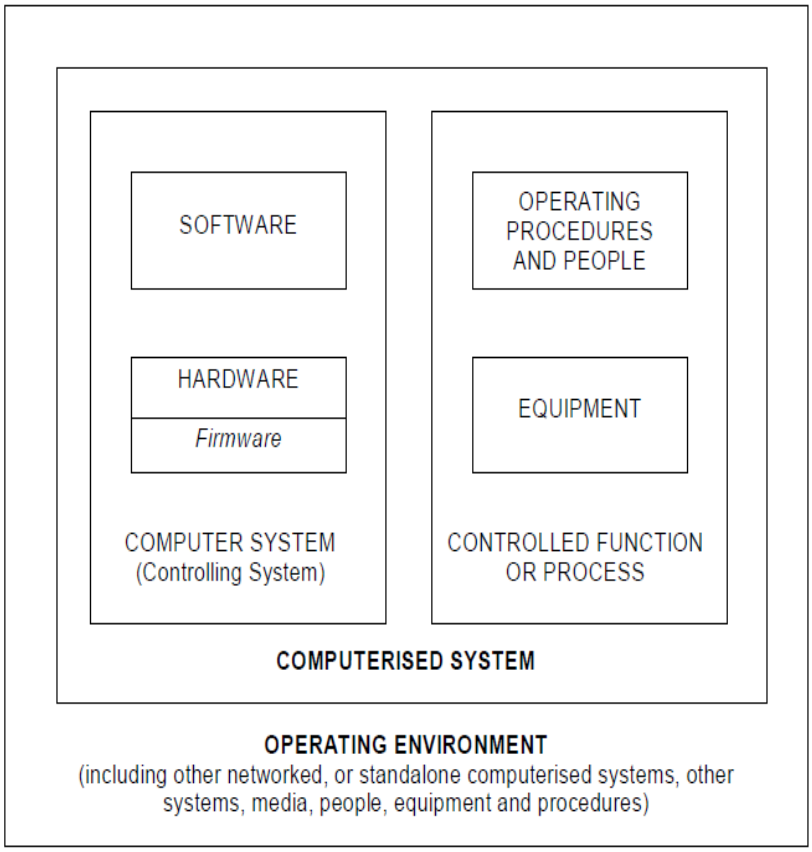

Abb. 1 Computergestütze Systeme (CS) – schematische Darstellung
Quelle: Glossar advisory document bzw. PIC/S PI 11-3 "Good Practice for Computerised Systems in Regulated GxP Environments"

1.1. Computergestützte Systeme

Der Anwendungsbereich der OECD Nr. 17 erstreckt sich von der Waage bis hin zu komplexen Datenmanagementsystemen.

- **einfache Geräte:**
  Waagen, Titrierautomaten, einfache Aufzeichnungsgeräte für Temperatur, Luftfeuchte usw.
- **Komplexe Systeme/Geräte:**
  alle Arten von physikalisch-chemischen Messsystemen mit Steuer- und Auswerte-software (Chromatographen, Spektrometer usw.)

- **Labordatenmanagementsysteme**
  Labor Informations- und Managementsysteme (LIMS) , Datenerhebungs- und -erfassungssysteme, Dokumentenmanagement, elektronische Archivierungssysteme, komplexe Raummonitoringsysteme (z. B. Raumlufttechnische Anlagen).

1.1.1. Validierung

Validierung *oder* Validation steht in der Informatik allgemein für die Nachweisführung, dass ein System die Praxisanforderungen während seines Lebenszyklus erfüllt. Die Validierung erstreckt sich auf

- alle verwendeten CS, die zum Gewinnen, Messen, Berechnen, Bewerten, Transferieren und Archivieren von Daten eingesetzt werden und
- GLP-relevante Daten, wie beispielsweise Rohdatensätzen, Umweltbedingungen, Personal- und Schulungsprotokolle, Instandhaltungsprotokolle.

Vor jeder Validierung ist ein Validierungsplan bis zur endgültigen Nutzung zu erstellen. Der Abschluss der Validierung ist in einem Bericht festzuhalten. Die Validierungsumgebung muss äquivalent zur Laborumgebung sein. Die Validierung sollte immer prospektiv erfolgen, also bei bzw. vor Beschaffung von CS. Prinzipiell ist **keine** retrospektive Validierung möglich, es sei denn, dass sich das CS, die Anwendung des CS oder die GLP-Relevanz des CS geändert haben. Der gesamte Prozess der Validierung ist Teil des Lebenszyklus (Life Cycle – fortlaufende Validierung) eines CS und sollte risikobasiert erfolgen. In dem nachfolgenden Lebenszyklus-schema sind die wesentlichen Begriffe der risikobasierten Validierung eines CS aufgeführt.

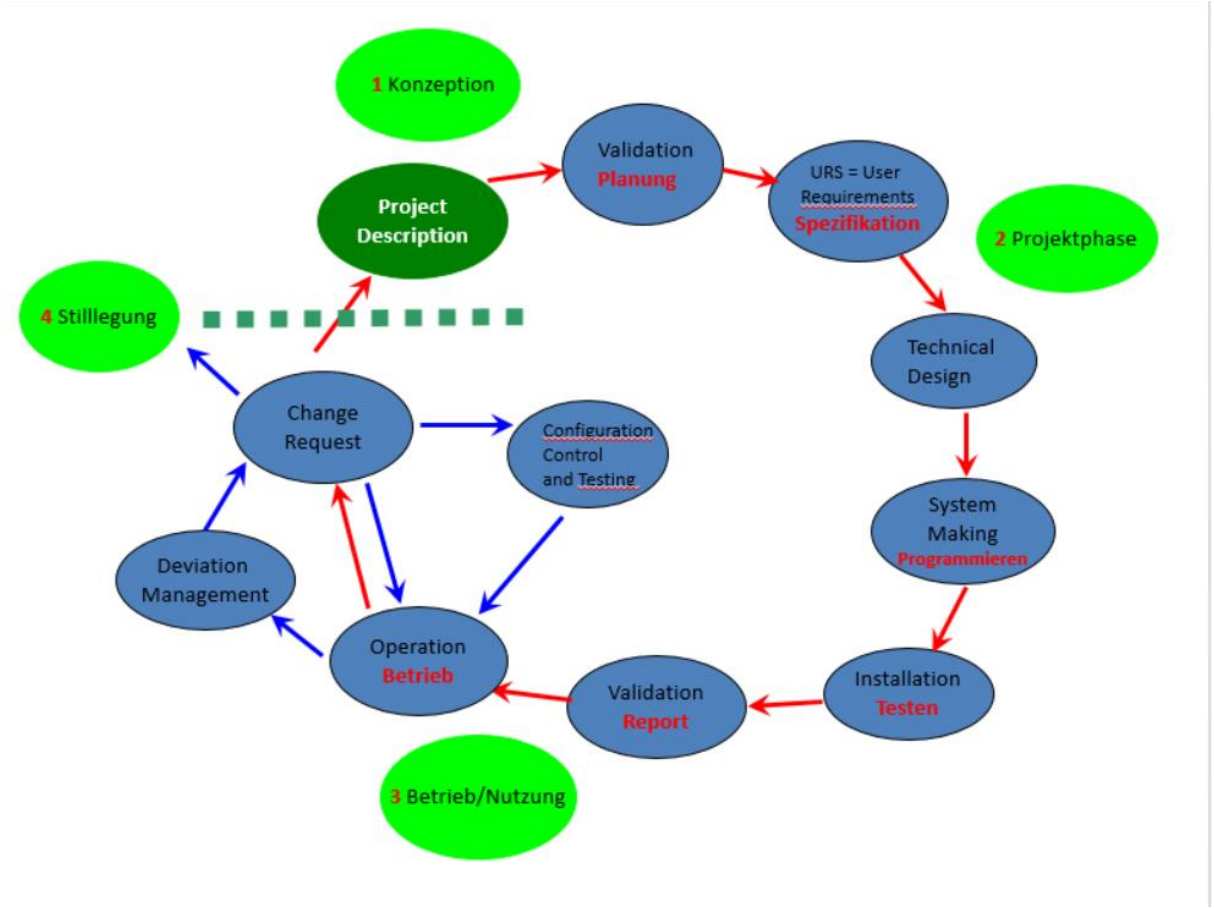

Abb. 2 Schematische Darstellung des Lebenszyklus eines CS mit den einzelnen Phasen

1.1.2. Qualifizierung

Die Qualifizierung von CS ist der Nachweis dafür, dass es für den vorgesehenen Verwendungszweck geeignet ist. Prinzipiell geht man von folgenden Arten der Qualifizierung aus:

- DQ Designqualifizierung — Geräteevaluation und -auswahl
- IQ Installationsqualifizierung — Geräteinstallation
- OQ Funktionsqualifizierung — Gerätefunktionsprüfung
- PQ Verfahrensqualifizierung — Einsatztauglichkeitsprüfung

Bei kommerziellen Standardsystemen (Commercial of the Shelf Systems - COTS), wie Standard-PCs und –Software aber auch einfache Geräte (geringe Komplexität) wie elektronische Pipetten, Waagen, Photometer, Kühlgeräte usw. kann eine formale Qualifizierung anstatt einer Validierung zulässig sein. Diese Systeme müssen aber anhand klarer Spezifikationen konsequent kalibriert bzw. gewartet werden.

Prinzipiell sind für den gesamten Lebenszyklus eines CS kritische Prozessparameter sowie Maßnahmen zur Prozessüberwachung festzulegen. Dabei ist von einem risikobasierten Ansatz auszugehen.

1.1.3. Lebenszyklus

Der Lebenszyklus eines CS besteht in der Regel aus vier Phasen:

- Konzeption/Kauf
- Projektphase (Entwicklung und Freigabe)
- Betrieb/Nutzung und
- Stilllegung.

Für jede dieser Aktivitäten muss eine Risikobeurteilung erstellt werden, die abhängig von der Komplexität des Systems (Waage – einfach, LIMS-Einbindung – komplex) ist. Der Lebenszyklus und die dazugehörigen Verfahren sind in der Abb. 2 dargestellt.

1.2. Risikomanagement

Das Risikomanagement ist auf den gesamten Lebenszyklus eines CS anzuwenden. Es besteht aus den Teilen Risikoerfassung, Risikobeurteilung, Risikominimierung und Risikokontrolle. Das Ziel ist immer die Sicherung der Datenintegrität und Qualität der Prüfungsergebnisse.
Ein wichtiger Bestandteil dieses Prozesses ist die Risikoabschätzung. Sie dient dazu, den Validierungsaufwand (Optimierung der Validierung) in Abhängigkeit von der Komplexität des Systems (von Waage bis LIMS) abzuschätzen. Auf jeden Fall sind die Validierungsergebnisse zu bewerten.
Die Anwendungen des Risikomanagements/Validierungsanforderungen erstrecken sich auch auf *non-GLP-Prüfungen* in der Prüfeinrichtung. Dabei ist der Einfluss der non-GLP-Systeme auf die GLP-Prüfungen abzuschätzen und eine klare Unterscheidung zwischen GLP- und non-GLP-Daten vorzunehmen.

1.3. Personal, Rollen und Verantwortlichkeiten

Zum IT-Personal gehören der Leiter IT, Systemadministratoren, Programmadministratoren, technisches Personal etc.
Das eingesetzte Personal (IT- und sonstige GLP-Mitarbeiter) muss angemessen qualifiziert sein und über entsprechende Erfahrungen verfügen. Dieses ist entsprechend zu dokumentieren. Sämtliche Aufgaben im Zusammenhang mit CS sind für alle beteiligten Personen im GLP-System (LPE, PL, QS, PP, IT-Personal) festzulegen und zu beschreiben.
Weiterhin sind klare Verantwortungen und Zugriffsberechtigungen für alle Beteiligten zu definieren. Eine Personalunion von IT-Personal und PL (ggf. auch Prüfpersonal) mit Zugang zum Serverraum ist zu vermeiden. Alternativ sind Verfahren festzulegen, die sicherstellen, dass Interessenkollisionen beider Funktionen ausgeschlossen sind.
Das Personal ist ausreichend intern oder auch extern zu schulen. Aus den Schulungsunterlagen muss ersichtlich sein, dass das Personal seiner GLP-Funktion/-Verantwortung gerecht wird und mit den Aufgaben und Abläufen (Validierung, Durchführung und Wartung) in Übereinstimmung mit den GLP-Grundsätzen vertraut ist.
Der Nachweis der GLP-Schulungsanforderungen muss auch bei Beteiligung externer Dienstleister vorgelegt werden.

1.3.1. Leitung der Prüfeinrichtung (LPE)

Die LPE besitzt die generelle Verantwortung für das implementierte GLP-System. Demzufolge hat sie auch die Gesamtverantwortung für den Einsatz von CS. Dazu gehören:

- dass die CS den Anforderungen der GLP-Grundsätze entsprechen,
- die Festlegung von Kriterien, wann die Validierungs- und/oder Qualifizierungsansätze anzuwenden sind,
- dass die CS für den beabsichtigten Einsatz geeignet sind, alle Forderungen der Validierung erfüllt sind und regelmäßig gewartet werden,
- dass definierte Funktion und Verantwortung für die Entwicklung, Validierung, Betrieb/Nutzung und Wartung eines CS beschrieben sind,
- dass die Schnittstellen in der Validierung zwischen der PE und den Lieferanten beschrieben sind,
- dass Kenntnis über die Struktur und Austauschwege der GLP-relevanten Daten incl. einer Risikobetrachtung besteht, bei der die Kritikalität der elektronischen Aufzeichnungen für die Qualität der Prüfergebnisse beurteilt wird,
- dass eine Rohdatendefinition für jedes CS existiert,
- dass der physikalische und logische Zugang zu elektronischen Systemen und Daten im Betrieb und bei der elektronischen Archivierung GLP-konform geregelt ist und die Datenintegrität, -sicherheit und Lesbarkeit für den GLP-relevanten Zeitraum gewährleistet ist,
- dass bei Verwendung von elektronischen Unterschriften eine Richtlinie vorhanden ist, die festlegt, welche Dokumente eine handschriftliche oder eine elektronische Unterschrift benötigen und wie die ordnungsgemäße Verwendung und Wartung der elektronischen Unterschriftsfunktionen des computergestützten Systems gewährleistet wird.

Die LPE besitzt die Möglichkeit, die Verantwortung für die CS auf geschultes Personal zu delegieren. Die Organisationsverantwortung der LPE (Ressourcenbereitstellung, Überwachung etc.) bleibt immer erhalten. So hat sie z.B. darauf zu achten, dass keine Verantwortungskonflikte, wie z. B. Systemeinstellung von Prüfpersonal zum Audit Trail, auftreten können.

1.3.2. Prüfleiter (PL)

Der PL besitzt prinzipiell die Verantwortung für die Durchführung der Prüfung und GLP-Konformität. Demzufolge ist er auch verantwortlich für die Gewinnung von elektronischen Daten.

Sämtliche Daten müssen **zuschreibbar, lesbar, zeitnah, original, korrekt, vollständig, konsistent, dauerhaft und verfügbar** sein (Siehe 3.2, Tabelle 1).

Vor Beginn einer Prüfung hat der PL den Validierungsstatus des CS zu verifizieren.

1.3.3. Qualitätssicherung (QS)

Die QS muss alle GLP-relevanten CS, die in der PE bzw. in den Prüfstandorten eingesetzt werden (Inventarliste, siehe 1.5) kennen. Sie muss in der Lage sein, die valide Verwendung von CS zu prüfen. Die Überprüfung der Einhaltung der Standards in allen Lebenszyklen eines CS ist Teil des QS-Programms bzw. soll in die Inspektionstätigkeit der QS einfließen. Diese Überprüfung kann auch an externe Fachleute oder spezialisierte Auditoren (z. B. Systemadministrator, Systemeigner, externe Fachleute) delegiert werden.
Die QS muss ausreichend geschult sein und über direkte Lesezugriffe verfügen, um, falls nötig, spezielle Computerprozesse (Überprüfung des Audit Trails, Methode zur Datenanalyse, Überprüfung der Rohdaten) zu überprüfen.

1.4. Einrichtungen

Die Standorte für die Computerhardware, hier vor allem Serverräume = elektronische Archive usw. sind so zu wählen, dass die Umgebungsbedingungen (z.B. Temperatur, Luftfeuchte, Staub, elektromagnetische Störungen usw.) so eingehalten werden, dass keine technischen Schäden an den Systemen auftreten können. Des Weiteren ist eine Notfallstromversorgung (doppelt ausgelegte oder unterbrechungsfreie Stromversorgung) zur Vermeidung von Systemausfällen vorzuhalten. Diese Anforderung bezieht sich nicht auf Einzelplatzrechner.

1.5. Inventar

Eine aktuelle Aufstellung (Inventarliste) GLP-relevanter CS und ihrer Funktionen ist vorzuhalten und zu pflegen (unabhängig von ihrer Komplexität, aber bezogen auf die Kritikalität der Generierung der Prüfergebnisse). Die Inventarliste sollte das CS (Modell, Hersteller, Version usw.), den Validierungs-/Qualifizierungsstatus und den Systemeigner (verantwortliche Person) beinhalten.

1.6. Lieferant

Als Lieferanten kommen IT-Anbieter, Verkäufer, interne IT-Abteilung, Provider inklusive Hosting Service usw. in Frage. Die Aufgaben können sehr vielfältig sein, z. B. Lieferung, Installation, Integrierung, Validierung, Modifizierung und Wartung eines Systems aber auch Datenverarbeitung oder Archivierung. Die genaue Beschreibung der Aufgabe/Verantwortung des Lieferanten und klare Definition über den Datenbesitz (z. B. Hosting Service) muss beschrieben sein. Die PE muss die QS-Systeme der Lieferanten (GLP nicht erforderlich) kennen.

1.7. Handelsübliche Standardprodukte (Commercial-of-the-shelf products - COTS)

Darunter fallen z.B. sogenannte Standard-PC-Anwendungen, die ohne oder mit begrenzter Modifikation oder auf Kundenwunsch erstellt werden. Falls die Applikation nicht komplex ist,

reicht die Funktionsprüfung entsprechend den festgelegten Anforderungen aus, wobei die eingesetzte Software risikobasiert zu validieren ist. In der Regel handelt es sich um solche Anwendungen wie z. B. *Tabellenkalkulationsprogramm*e, wo vordefinierte Formulare, selbstgeschriebene Gleichungen oder Makros als in-house entwickelte Applikationen zu betrachten sind. Der eingesetzte Computer und das Tabellenkalkulationsprogramm (z.B. MS-Excel) mit den eigenentwickelten Excel-Arbeitsblättern (worksheets)) sollten als Einheit betrachtet und in geeigneter Form als CS qualifiziert werden.

1.8. Änderungs- und Konfigurationskontrolle (Change control)

Jede Änderung an einem computergestützten System ist in einer kontrollierten Weise sowie in Übereinstimmung mit den schriftlichen Verfahrensweisen für die Änderungskontrollprozeduren durchzuführen. Dieses Verfahren gilt sowohl für die Hardware als auch die Software.

Diese Änderungskontrollen betreffen alle Phasen des Lebenszyklus (Validierung, Betrieb, Stilllegung). Auch in der Änderungskontrolle sind die Aufgaben und Verantwortungen der beteiligten Akteure zu definieren. Das Verfahren der Änderungskontrolle ist klar strukturiert und besteht im Wesentlichen aus Überprüfung, Genehmigung, Austestung und Risikobetrachtung. Zur Risikobeurteilung können die Regeln der Softwarekategorisierung entsprechend GAMP5 angewandt werden. Prinzipiell läuft das Änderungsverfahren immer nach dem gleichen Schema ab. Dabei ist die Vorgehensweise chronologisch:

1. Zunächst wird die Änderung (festgestellt oder beabsichtigt) dokumentiert.
2. Die mögliche Auswirkung der Änderung wird analysiert und bewertet.
3. Die Implementierung der Änderung im Prozess wird geplant.
4. Die Änderungen werden erarbeitet.
5. Anschließend erfolgt die Austestung.
6. Nach erfolgreicher Austestung werden die Änderungen implementiert.
7. Es erfolgt die endgültige Freigabe und der Abschluss des Change Verfahrens.

1.9. Anforderungen an die Dokumentation

Für jedes computergestützte System muss eine Dokumentation vorhanden sein. Der Umfang der Dokumentation hängt von der Komplexität und Validierungsstrategie des computergestützten Systems ab und ist Bestandteil des Qualitätssicherungsprogramms. Die Dokumentation sollte sich auf drei Bereiche konzentrieren:

- Allgemeine Regelungen zu CS
- Validierung von CS
- Betrieb/Stilllegung (Operation) von CS.

In der nächsten Abbildung findet sich eine Zusammenstellung der grundlegenden Elemente, die in der Dokumentation zum CS berücksichtigt werden sollten, auf die drei genannten Bereiche.

Abbildung 3: Übersicht der wichtigsten Dokumentationen eines CS (Vortrag Dr. Bauer, Dr. Schütz BfR Berlin 2019)

Das OECD-Dokument Nr. 17 enthält eine Übersicht der wichtigsten Angaben zur Beschreibung eines CS, wie z. B. Namen und Version der Software, Hardware, Betriebssystem, auszuführende Funktionen usw.. Die aufgeführten Punkte sowie die Dokumentation zum Betrieb und Einsatz eines CS und die Regelung der Verantwortlichkeiten werden ausführlich im Fragenkatalog erfasst.

Für die zu erstellenden Dokumente gelten die gleichen Archivierungsfristen, wie für die damit gewonnenen Daten.

2. Projektphase

2.1. Validierung/Qualifizierung

Die CS sind so zu konzipieren, dass sie nachweislich für ihren Einsatz in einer GLP-Umgebung geeignet sind. Der Validierungsaufwand kann auf der Grundlage einer dokumentierten Risikobeurteilung an die Art des Systems angepasst werden. Die Validierungsergebnisse können auf die Benutzeranforderungsspezifikation (User Requirement Specification – URS, siehe 2.4), einem Validierungsplan, die Durchführung von Benutzerakzeptanztests und einem Validierungsbericht reduziert werden, wenn dies durch eine Risikobewertung nachgewiesen werden kann.

Letztendlich muss der Nachweis vorliegen, dass das System auf Einhaltung der Abnahmekriterien geprüft worden ist, bevor der Routinebetrieb startet.

Sowohl die Entwicklung eines computergestützten Systems als auch der Validierungsprozess sind durch Qualitätsmanagementsysteme zu regeln. Vorzugsweise sollten anerkannte Qualitätsmanagementsysteme zum Einsatz kommen. Erfolgt die Entwicklung durch einen externen Anbieter, so erfolgt die Überprüfung des Qualitätsmanagementsystems risikobasierend im Rahmen der Lieferantenqualifizierung (siehe auch 2.6).

Retrospektive Evaluierung ist nach dem vorliegenden Lebenszyklusmodell nicht mehr anwendbar. Auch Altsysteme müssen genauso behandelt werden wie Neusysteme. In Ausnahmefällen kann auf alte historische Dokumentationen über das CS zurückgegriffen werden. Zusätzlich müssen Anforderungen definiert werden, wie der Validierungsstatus der GLP-Anforderungen (siehe nachfolgende Abschnitte) erfüllt werden kann

2.2. Änderungskontrolle während der Validierungsphase

Mit dem Beginn des Validierungsprozesses muss ein Änderungskontroll- und Abweichungsmanagement-Prozess vorhanden sein, der klar von der Änderungskontrolle während des Systembetriebs unterschieden wird. Die Validierungsdokumentation muss Protokolle zur Änderungskontrolle (wenn zutreffend) und Berichte zu allen im Verlauf des Validierungsprozesses beobachteten Abweichungen enthalten.

2.3. Systembeschreibung

Wie schon in Kapitel 1.9 aufgeführt, gehört eine Systembeschreibung zur Dokumentation von CS. Dazu zählen die physischen und logischen Anordnungen von CS (z.B. Serverstruktur, Netzaufbau), zu Datenflüssen und Schnittstellen mit anderen Systemen oder Prozessen, Hardware- und Softwarevorgaben sowie vorgehaltene Sicherheitsmaßnahmen.

2.4. Benutzeranforderungsspezifikationen

Die Benutzeranforderungsspezifikation (User Requirement Specification – URS) beschreibt die Funktion und die Anwendung des Systems unabhängig von deren Komplexität. Sie umfasst

den gesamten Prozess aus Sicht des Nutzers und muss alle GLP-Funktionen/-Anwendungen enthalten, inklusive aller kritischen Funktionen. Dabei müssen abhängig von der Komplexität des Systems alle Spezifikationsunterlagen nachvollziehbar sein. Sollten nicht alle Funktionen des CS genutzt werden, sollten nur die „GLP-Funktionen“ beschrieben und getestet werden. Die Validierung muss aber auch die non-GLP-Funktionen beinhalten. Alle „anderen“ außerhalb der Anwendungen vorhandenen Funktionen sollten beschrieben sein, müssen aber nicht getestet werden.

2.5. Qualitätsmanagementsystem und unterstützende Verfahren

Siehe 2.1

2.6. Kundenspezifische Systeme, Lieferantenqualifizierung

Systeme, die für spezielle Anwendungszwecke im Auftrag der Prüfeinrichtung entwickelt werden, bergen aufgrund fehlender Erfahrungen mit der Software das höchste intrinsische Risiko. Da auch der Entwickler Teile der Validierung übernehmen kann, sind Rollen und Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer schriftlich zu vereinbaren. Natürlich greift auch hier der risikobasierte Ansatz. Bei einfacheren Aufträgen (z.B. Software für Standardberechnungen) kann eine formularbasierte Lieferantenqualifizierung ausreichen. Werden komplexe Systeme in Auftrag gegeben, ist ein vollständiges Lieferantenaudit erforderlich. Der Auftragnehmer kann z.B. beim Entwurf des Validierungskonzepts und bei der Erstellung der Testpläne unterstützen, sowie bei der Durchführung von Risikoanalysen mitarbeiten und auch Validierungsaufgaben wie IQ, OQ übernehmen. Deshalb muss für die Validierung von komplexen kundenspezifischen Systemen mit ausgelagerten Aktivitäten eine Standardarbeitsanweisung vorhanden sein, die die Beurteilung und Berichterstattung von Qualitäts- und Leistungsmaßnahmen für alle Lebenszyklusstufen sicherstellt.

2.7. Prüfungen

Bei computergestützten analytischen Messgeräten mit Auswerteeinheit, wie z. B. Chromatographiesystemen, kann ein sogenannter „Black Box-Test“ unter Verwendung von Kontrollproben als Akzeptanztest herangezogen werden (Weiteres zu Validierung/Qualifizierung von Geräten siehe 1.1).

2.8. Datenmigration

Die Datenmigration beschreibt den Umzug von Daten von einer Plattform auf die andere. Das betrifft Versionsupdates und -upgrades[1], sowie Umzüge von einer Datenbank in eine neue

[1] Update beschreibt kleine Verbesserungen oder Fehlerbehebungen an einer Software. In der Regel ändert sich nur die Versionsnummer.

Upgrade beschreibt umfangreiche Änderungen an einem Softwareprodukt und kann technische Neuerungen beinhalten.

Umgebung. Updates bzw. Upgrates müssen immer kontrolliert und dokumentiert durchgeführt werden. Bei wichtigen/kritischen Updates muss die PE informiert werden. Können die Rohdaten nicht oder nur sehr umständlich in ein neues System integriert werden, ist es erforderlich, die Daten z.B. nach PDF zu exportieren, oder Papierversionen zu erzeugen. Im letzteren Fall ist darauf zu achten, dass alle Daten inklusive Audit Trail gedruckt werden, um die Rekonstruierbarkeit zu gewährleisten.

Eine Datenmigration erfordert immer eine Validierung, bei der sichergestellt wird, dass Meta- und Rohdaten unverändert bleiben. Deshalb ist nach Abschluss der Migration ein Abgleich der Roh- und Metadaten unumgänglich. Eventuelle elektronische Signaturen müssen erhalten bleiben.

Beispiele für Migrationen:

- Ein LIMS wird durch ein anderes Produkt ersetzt,
- Ein LIMS oder die zugehörige Datenbank wird auf eine neue Version upgegradet oder upgedatet,
- Zwei oder mehrere Datenbanken werden zu einer zusammengefasst.

2.9. Datenaustausch

Unter Datenaustausch im Sinne der GLP versteht man die Kommunikation zwischen den CS. Dabei wird grob in zwei Kategorien unterteilt, CS untereinander (Netzwerke) und CS mit peripheren Geräten (z.B. Analysengeräte mit PC). Besonders beim Austausch von elektronischen Daten müssen geeignete Kontrollen der Schnittstellen bezüglich Sicherheit und Systemintegrität durchgeführt werden (z.B. sichere Verschlüsselung bei Nutzung von Funkstrecken zur Kommunikation). In der Regel aber werden Standard-Kommunikationsinfrastrukturen und deren Verfahren (z.B. TCP/IP) verwendet, die als validiert gelten. Zusätzlich spielt auch die Rohdatendefinition eine Rolle. Es muss analysiert und definiert werden, auf welchem Gerät die Rohdaten gespeichert sind (z. B. Speicher Messgerät, Auswerte-PC oder Server).

3. Betriebsphase

3.1. Genauigkeitskontrolle

Einer der Hauptursachen in der Anwendung von CS ist die fehlerhafte Dateneingabe. Hierbei sind Strategien zur Risikominimierung zu beschreiben und einzuführen. Dies kann z. B. durch die Kontrolle durch einen zweiten Mitarbeiter oder ein elektronisches System erfolgen. Letzteres ist bei der Validierung eines CS zu berücksichtigen. Nicht validierte Dateneingabesysteme dürfen nicht eingesetzt werden. Das Kontrollverfahren zur manuellen Dateneingabe ist geeignet zu beschreiben, so dass es plausibel nachvollziehbar ist.

3.2. Daten und Datenspeicherung

Zur Abspeicherung von Daten müssen in der PE klare Regelungen festgelegt werden. Diese müssen so ausgelegt sein, dass eine Wiederherstellung nach einem die Systemintegrität gefährdenden Fehler möglich ist. Dabei ist Folgendes zu beachten:

- 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
- der Zugriff auf gespeicherte Daten muss während der Aufbewahrungsfrist sichergestellt sein.

Die Datenlesbarkeit muss auch nach erfolgtem System- oder Softwareupdate gewährleistet sein. Wenn nötig, muss Software zum Lesen oder zum Rekonstruieren von Daten im Archiv aufbewahrt werden und die Lesbarkeit der archivierten Rohdaten regelmäßig überprüft werden.

Für jedes computergestützte System müssen die Rohdaten definiert werden, ungeachtet dessen, wie die Rohdaten mit dem System in Verbindung stehen. Dies kann z. B. durch Speicherung auf elektronischen Medien oder aber auch durch Computer- oder Geräteausdrucke erfolgen. Entscheidend ist die Nachvollziehbarkeit der Prüfung anhand der Rohdaten und Metadaten. Hier ist die Kritikalität der elektronischen Aufzeichnungen für die Qualität der Prüfergebnisse hervorzuheben.
Unter **Kritikalität** versteht man, welche Auswirkung der direkte oder indirekte Fehler einer physischen oder logischen Einheit zugemessen wird. Sie ist abhängig vom Umfang und Art der Anwendung des CS. Hohe Kritikalität wäre zum Beispiel der Zugang zu Daten durch unberechtigte Personen. Das Gegenteil wären klare administrative Regelungen.

Für die elektronischen Aufzeichnungen sind potenzielle Risiken zu erfassen und zu beurteilen sowie Maßnahmen zur Minimierung vorzuhalten. Generell muss nachgewiesen werden, wie elektronische Daten gespeichert werden, wie die Aufzeichnungsintegrität geschützt wird und wie die Lesbarkeit der Daten erhalten wird.
Diese Anforderungen gelten sowohl für Papier als auch für computerisierte Systeme. Ein hilfreiches Akronym bezüglich der Datenintegrität ist das **ALCOA +**- Konzept aus dem GAMP-Bereich.

Tabelle 1. ALCOA + - Konzept:

ALCOA – Kürzel	Anforderung	Fragen an PE
A - Attributable (zuschreibbar)	Rohdaten sollten immer in unveränderbarer Form vorliegen.	Wenn ein Datensatz geändert wurde, wer hat was, warum und wann gemacht?
L - Legible (lesbar)	Daten müssen dauerhaft in einem beständigen Speichermedium aufgezeichnet und lesbar sein.	Sind die Daten lesbar und dauerhaft aufgezeichnet?

C - Contemporaneous (zeitnah)	Daten sind immer zeitnah, chronologisch oder mit Zeitstempel aufzuzeichnen.	Wurden die Daten zeitnah aufgezeichnet?
O - Original (original)	Rohdaten und Aufzeichnungen entsprechen den tatsächlichen Daten.	Sind es die Originaldaten oder zertifizierte, echte Kopien?
A - Accurate (korrekt)	Die Aufzeichnungen spiegeln genau das wieder, was passiert ist.	Sind die Aufzeichnungen fehlerfrei bzw. wurden nicht verändert oder dokumentiert ergänzt?
+ Complete (vollständig)	Die Aufzeichnungen sind vollständig.	Liegen sämtliche Rohdaten inklusive Auswertungen vor?
+ Consistent (konsistent)	Die Daten sind stimmig und widerspruchsfrei.	Spiegeln die Zeit- und Datumsstempel die chronologische Abfolge wieder?
+ Enduring (dauerhaft)	Die Daten sind unverändert über den gesamten Aufbewahrungszeitraum.	Wie erfolgt die Aufzeichnung über den gesamten Archivierungszeitraum?
+ Available (verfügbar)	Die Aufzeichnungen sind lesbar und druckbar.	Sind die Daten jederzeit verfügbar und zugänglich z.B. beim Audit?

Für alle mit CS gewonnenen Daten gelten in GLP-relevanten Zeiträumen weiterhin folgende Anforderungen:

- die physische Zugriffskontrolle auf elektronische Speichermedien (z. B. Maßnahmen zur Kontrolle und Überwachung des Zutritts von Personal zu Serverräumen usw.)
- die logische (elektronische) Zugriffskontrolle auf gespeicherte Aufzeichnungen (z.B. Berechtigungskonzepte für computergestützte Systeme, die die Rollen und Rechte in einem GLP-relevanten computergestützten System definieren)
- den physischen Schutz der Speichermedien vor Verlust oder Zerstörung (z. B. durch Feuer, Feuchtigkeit, schädliche elektrische Fehler oder Anomalien, Diebstahl usw.)
- 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
- das Sicherstellen des Zugriffs auf und der Lesbarkeit von elektronischen Aufzeichnungen durch Bereitstellung einer geeigneten physischen sowie Software-Umgebung.

3.3. Ausdrucke

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 vorgenommenen Änderungen, wenn diese Änderungen für den korrekten Inhalt und die korrekte Bedeutung relevant sind.

3.4. Audit-Trails

Bei vielen (insbesondere bei neueren und komplexeren) computergestützten Systemen ist ein Audit-Trail integriert. 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 diejenige Person, die die Änderung vorgenommen hat, rückführbar sein. Das Audit-Trail muss als Teil des CS validiert werden.

Audit-Trails müssen für ein computergestütztes System aktiviert und so konfiguriert sein, dass die Rollen und Verantwortlichkeiten des Prüfungspersonals widergespiegelt werden. 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.

Das Audit-Trail ist eine kritische Phase, die ins QS-Programm integriert und besonders überwacht werden muss.

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 Rohdaten (z.B. Chromatogramme), die für eine Neuberechnung modifiziert worden sind, unveränderbar gekennzeichnet sein.

Auch ohne das Vorhandensein eines integrierten Audit-Trails gelten die Anforderungen an die Nachvollziehbarkeit und Integrität der Daten. Änderungen an Datensätzen müssen sichtbar und nachvollziehbar im Sinne eines Audit-Trails erfolgen (wer hat was, warum und wann gemacht)?

3.5. Änderungs- und Konfigurationsmanagement

Auch in der Betriebsphase ist das Change-Verfahren für Hard- und Software in geeigneter Weise zu beschreiben, da diese Änderungen den Validierungsstatus und somit die Datenintegrität beeinflussen können. Entsprechend sind auch die Verantwortlichkeiten zu regeln.

Solche Änderungen können beispielsweise sein:

- Software-Versionsänderungen
- Modulfreischaltungen

- Erweiterungen des Systems
- Änderungen im Netzwerk
- Einsatz von selbstentwickelten Makros
- Aktualisierung von Gerätetreibern oder Virenschutz
- Wechsel der Speichermedien
- neue Ausgabegeräte usw.

Dabei ist immer zu beachten, dass diese Änderungen die GLP-Prüfung (Datenintegrität) beeinflussen können. Dazu sind Bewertungsmethoden zu beschreiben, die für die Festlegung des Umfangs der Nachprüfung (Revalidierung) nötig ist.

Die Konfiguration eines CS muss über den gesamten Lebenszyklus, also von der Projektphase bis zur Stilllegung bekannt sein. Bei CS im analytischen Bereich ist die Konfiguration des CS Bestandteil der Methodenvalidierung.

Nach Eingriffen in ein CS (geplant = Wartung, ungeplant = Reparatur) ist der Validierungsstatus zu prüfen und zu dokumentieren.

3.6. Regelmäßige Überprüfungen

Regelmäßige Überprüfungen des CS sollen sicherstellen, dass der valide Zustand weiterbesteht und den GLP-Status der Datengewinnung/ –verarbeitung bestätigen. Der Inhalt und Umfang der Überprüfung hängt von der Komplexität und Kritikalität des Systems ab. Der Aufwand der Überprüfung eines COTS ist in der Regel gering und kann in Abhängigkeit von der Validität des Systems von der Überprüfung ausgenommen werden. Bei zunehmender Komplexität und Kritikalität der Systeme z.B. GC-MS, HPLC ist der Umfang wesentlich größer. Hier muss der volle Funktionsumfang, die Abweichungsaufzeichnungen, Störfälle, die Upgrade-Historie, die Leistung, Zuverlässigkeit und Sicherheit des Systems überprüft werden. Die Häufigkeit und die Intensität einer solchen regelmäßigen Überprüfung müssen risikobasiert erfolgen. Die verantwortlichen Personen sind zu benennen. Die Überprüfung ist zu dokumentieren.

Bei den in analytischen Prüfungen verwendeten komplexen Gerätesystemen sollten Geräteverantwortliche benannt werden. Der Status des Gerätes ist regelmäßig zu überprüfen und zu dokumentieren bzw. am Gerät kenntlich zu machen. Die Festlegung des Umfangs der Überprüfung von komplexeren Systemen, wie Datenbanken, LIMS, Netzwerken usw. ist festzulegen. Ebenso ist die Verantwortlichkeit von hinzugezogenen IT-Fachpersonal festzulegen und zu dokumentieren.

Prinzipiell müssen bei den regelmäßigen Überprüfungen sämtliche gemeldete unerwartete Ereignisse (z.B. Fehlermeldungen, Systemabstürze) erfasst werden, da sie möglicherweise den Validierungsstatus des Systems beeinflusst haben könnten.

3.7. Physische, logische Datensicherheit und Datenintegrität

Die physische IT-Sicherheit bezieht sich auf mittelbare und unmittelbare, physische Einwirkungen auf Computersysteme. Das betrifft den Zugangsschutz zu ganzen

Gebäuden, Räumen oder zu kritischen Systemen und die Abwehr elementarer Bedrohungen. Elementare Bedrohungen sind: Feuer, fehlerhafte Klimatisierung, Wasser, Ausfall oder Störung der Stromversorgung, elektromagnetische Störstrahlung, Diebstahl, Manipulation (Hard- und Software, Informationen) und Integritätsverluste durch Alterung von Datenträgern.

Die logische Sicherheit wird unterteilt in die programmtechnische und organisatorische Sicherheit. Bei der logischen Sicherheit sind die elementaren Bedrohungen unter anderem unbefugtes Eindringen in IT-Systeme, Schadprogramme und Sabotage. Zum Schutz vor Bedrohungen von außen sind Produkte wie Firewalls und Virenscanner erforderlich.

Zur Wahrung der Integrität ist es entscheidend, dass Daten nur von befugten Personen geändert werden können. Deshalb ist die Verrechtung von Ordnerstrukturen bei der Speicherung GLP-relevanter Rohdaten und die Rollendefinitionen sowie Rollenvergabe bei Fachanwendungen wie LIMS-Systemen von entscheidender Bedeutung. Rechte und Rollen sind so zu vergeben, dass Änderungen nur von berechtigten Personen durchgeführt werden, die diese für die Erfüllung einer konkreten Aufgabe benötigen (Need-to-know-Prinzip). Personal, welches bei der Durchführung von Prüfungen involviert ist, sollte keine Administratorenreche haben. Das Verfahren zur Rechte- und Rollenvergabe ist zu dokumentieren.

Die genannten Einwirkungen können durch geeignete technische Maßnahmen erkannt bzw. verhindert werden. Dies ist allerdings nicht nur eine Frage der Technik. Wichtige Elemente zur Abwehr von elementaren Bedrohungen und zum Schutz der Datenintegrität und Datensicherheit sind dokumentierte Verfahren, die vom Management der Prüfeinrichtung eingeführt werden müssen. Dazu gehören:

- dokumentierte Sicherheitsverfahren zum Schutz von Daten, Soft- und Hardware (z.B. eine IT-Sicherheitsrichtlinie)
- ein Konzept zur Vergabe von Zugangsberechtigungen zu Computerhardware
- ein Konzept zur Vergabe von Berechtigungen für den logischen Zugriff zu Domains, Computern, Anwendungen und Daten
- Das Personal muss entsprechend geschult sein.

3.8. Störfallmanagement (Incident Management)

Das Störfallmanagement umfasst alle erkannten oder vermuteten Störungen, die eine definierte Kritikalität überschreiten. Nach der allgemeinen Definition sind Störfälle (Incidents) Ereignisse, die nicht zum standardmäßigen Betrieb eines Services gehören und tatsächlich oder potenziell eine Unterbrechung dieses Services oder eine Minderung der vereinbarten Qualität verursachen könnten.

Besteht nur der Verdacht, dass Prüfungen betroffen sein können, sind LPE, Prüfleiter und QS zu informieren. Der Prüfleiter entscheidet, ob der Vorfall Auswirkungen auf Prüfungen hat. Die Störfälle sind zu archivieren und müssen von der GLP-Prüfung zum Computersystem und umgekehrt rückführbar sein. Störungen müssen regelmäßig

ausgewertet werden und tragen zu einer Verbesserung und Weiterentwicklung verschiedener Elemente, wie Änderungs- und Konfigurationsmanagement, der regelmäßigen Überprüfung sowie der Aus- und Fortbildung bei. Klassische Beispiele sind der Ausfall des zentralen Klimadatenerfassungssystems, Störung eines LIMS-Datenbankservers oder auch Virenbefall.

3.9. Elektronische Unterschrift

Elektronische Aufzeichnungen können elektronisch durch Anbringen einer elektronischen Unterschrift (Signatur) unterschrieben werden, von denen erwartet wird, dass sie

- die gleichen rechtlichen Konsequenzen haben wie handschriftlich geleistete Unterschriften, zumindest in der Prüfeinrichtung;
- auf Dauer (über den gesamten Archivierungszeitraum) mit ihren (ihrer) entsprechenden Aufzeichnung(en) verknüpft ist (sind);
- Uhrzeit und Datum beinhalten, zu der (dem) sie geleistet wurden („Elektronischer Zeitstempel“);
- die Identifizierung des Unterzeichneten ermöglichen und die Bedeutung der Unterschrift angeben.

Bei der Genehmigung des Prüfplans und der Unterzeichnung des Abschlussberichtes (claim of compliance) durch den Prüfleiter sowie bei der dem Abschlussbericht beizufügenden Erklärung der QS ist die Verwendung von qualifizierten Signaturen, Siegeln und Zeitstempeln gemäß elDAS-Verordnung (EU) Nr. 910/2014 erforderlich. Für andere elektronische Freigaben (z. B. SOP oder Prüfgegenstände) reichen andere sichere und validierte Verfahren, wie z.B. fortgeschrittene Signatur, Siegel und Zeitstempel aus. Für das übliche Datenhandling ist ein Audit-Trail angemessen.

Die elektronische Unterschriftsfunktion eines computergestützten Systems muss in den Systemanforderungen erwähnt und in den Systemverfahren validiert und beschrieben sein.

Es muss eine Richtlinie zum Thema elektronische Unterschrift vorhanden sein, die den ordnungsgemäßen Betrieb der elektronischen Unterschriftsfunktionen des computergestützten Systems regelt und gewährleistet. Darin wird festgelegt:

- welche Aufzeichnungen eine handschriftliche Unterschrift oder eine elektronische Unterschrift benötigen,
- welche Personen berechtigt sind, elektronische Unterschriften in welcher Rolle prüfungsbezogen zu leisten,
- wie gewährleistet wird, 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,
- in welcher Form Metadaten, die mit der elektronisch unterzeichneten Aufzeichnung verbunden sind, eindeutig identifiziert sind (z.B. Methodenparameter und

Systemkonfiguration). Die Signaturfunktion des computergestützten Systems muss die Gleichzeitigkeit der Verknüpfung zwischen der elektronisch unterzeichneten Aufzeichnung und den erläuternden Metadaten gewährleisten (Siegelfunktion),

- wie Änderungen an der geleisteten elektronischen Unterschrift oder an der Verknüpfung zu den verbundenen Metadaten verhindert werden,
- 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 (Audit-Trail).

Es können zur Unterzeichnung von Aufzeichnungen, die von einem elektronischen System stammen, „papierbasierte" Versionen ausgedruckt und unterschrieben werden. Diese enthalten möglicherweise nicht alle Informationen, die für eine vollständige Rekonstruktion der Aktivitäten benötigt werden. 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. 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.
Wird ein kompletter Satz elektronischer Aufzeichnungen und seine gedruckte Entsprechung parallel aufbewahrt, muss festgelegt werden, 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

Wenn ein Verfahren einen der elektronischen Datenfreigabeprozesse beinhaltet, muss die Datenfreigabefunktion Bestandteil der Systemvalidierung sein (z.B. elektronische SOP-Freigabe). Der Freigabeprozess muss in den Verfahrensanweisungen der Prüfeinrichtung beschrieben sein und im System elektronisch ausgeführt werden.

3.11. Archivierung

Die in der Guideline No. 17 definierten Vorgaben zur elektronischen Archivierung ergänzen das OECD Beratungsdokument der Arbeitsgruppe GLP Nummer 15 (Establishment and Control of Archives that Operate in Compliance with the Principles of GLP). Neben den speziellen Anforderungen zur elektronischen Archivierung müssen auch die Bedingungen für die Archivierung von Papierdokumenten beachtet werden.
Die Hardwareanforderungen für die elektronische Archivierung lassen sich nicht auf spezielle

Hersteller und Produkte beschränken. Mittlerweile gibt es viele Anbieter, die mit einer Compliance zur Langzeitarchivierung werben und auch für das GLP-Umfeld geeignet sind. Die wesentlichen Prüfpunkte sind im Fragekatalog unter 3.11 abgelegt.

Bei der elektronischen Archivierung ist nicht nur die reine Speicherung von Daten relevant. Im Zeitraum der Archivierung können sich Hardwareumgebungen, Datenträger, Datenbanken, Datenbankversionen und Dateiformate ändern und lösen Revalidierungen und Migrationsprozesse aus. Die elektronische Archivierung ist als eigenständiges Verfahren zu validieren.

3.12. Desaster Recovery (Wiederherstellen nach Systemausfällen)

Für den Fall eines Systemausfalls ist eine Risikobeurteilung durchzuführen, die die vorzunehmenden Maßnahmen in Abhängigkeit ihrer Bedeutung (Kritikalität) für die Qualität der Prüfergebnisse und des zeitlichen und personellen Aufwandes festlegt. Diese Notfallpläne müssen entsprechend validiert, dokumentiert und getestet 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.

Sicherungskopien der gesamten eingesetzten Software müssen (in der für das validierte computergestützte System relevanten Version) aufbewahrt werden, bei einem Dritten hinterlegt oder gemäß Service Level Agreement verfügbar sein. Wenn Wiederherstellungsverfahren Änderungen an Hard- oder Software zur Folge haben, gelten die Validierungsanforderungen dieser Leitlinie.

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, ob 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

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.

I. Referenzen

OECD GLP Advisory Dokuments Nr. 17 *„Anwendung von Grundsätzen der Guten Laborpraxis auf computergestützte Systeme*“ (22. April 2016)

„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.

Die VERORDNUNG (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (**eIDAS-Verordnung** (electronic IDentification, Authentication and trust Services).

II. 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.
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.
Anerkannte technische Standards	Standards, die von nationalen oder internationalen Standardisierungsinstitutionen (ISO, IEEE, ANSI etc.) veröffentlicht wurden.
Benutzeranforde-rungsspezifikation	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.
Berechtigungskonzept	Ein Berechtigungskonzept ist ein formelles Verfahren zur Festlegung und Steuerung von Zugriffsrechten auf ein computergestütztes System und von Rechten in einem computergestützten System.
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.
Black Box Test	Überprüfung des Funktionsumfang einer Software durch Abgleich des sichtbaren Verhaltens (z. B. erhaltene Mess- bzw. Berechnungswerte) gegenüber der Benutzeranforderungsspezifikation. Eine Kenntnis der inneren Funktionsweise (z.B. Quellcode) des Systems wird nicht vorausgesetzt.

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.
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.
Datenerfassung	Unter Datenerfassung versteht man Maßnahmen, die typischerweise erfolgen, um Daten und dazugehörige Metadatenelemente zu planen, zu erfassen und zu verifizieren.
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.
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“.
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.
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.

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.
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.
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.
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.
Korrektur- und Vor-beugemaßnahmen	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.
Lebenszyklusmodell	Ein Lebenszyklusmodell beschreibt die Phasen bzw. Aktivitäten eines bzw. innerhalb eines Projekts, von der Konzeption bis hin zur 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.
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.
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.
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.
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.
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.
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.
Störfallmanagement (Incident Management) (Abweichungsmanage-ment)	Das 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.
Validierung	Vorgang der Nachweiserbringung, dass ein Prozess zu den erwarteten Ergebnissen führt. Die Validierung eines computergestützten 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.
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.
Zulassung	Vorgang der Nachweiserbringung, dass alle Ausrüstungen, einschließlich der Software, ordnungsgemäß funktionieren und auf ihren Zweck ausgerichtet sind.

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

Die Durchführung von GLP-Inspektionen in Deutschland

Handbuch
Anhang 3:
Inspektion von computergestützten Systemen (CS)

Teil 2:
Fragenkatalog

Bund/Länder-Arbeitsgemeinschaft Chemikaliensicherheit
Ausschuss „GLP und andere Qualitätssicherungs-Systeme“
BLAC-AS GLP

Stand: 15.Juni 2019

Im folgenden Katalog sind die wesentlichen Elemente aus dem Anhang 3 (Teil 1: Erläuterungen zum OECD-Papier) in Frageform formuliert. Allein aufgrund des Umfangs der OECD-Guideline 17 ist die Aufzählung zwar nicht abschließend, die wichtigen Eckpunkte sind jedoch enthalten. Die Reihenfolge der Fragen orientiert sich an dem OECD-Papier, ist aber nicht relevant für die Inspektion. Zur Optimierung des Ablaufs können viele Elemente in den normalen Inspektionsablauf eingebaut werden.

Es gibt nachfolgend einige Dopplungen in den Fragen, die sich daraus ergeben haben, dass der Fragenkatalog sich an die Nummerierung der OECD Nr. 17 hält.

1. Anwendungsbereich und Begriffsbestimmung

1.1. Computergestützte Systeme (CS) - Einstiegsfragen

1.1.1.1. In welchem Umfang werden computergestützte Systeme (CS) in der PE angewendet?

1.1.1.2. Gibt es eine Inventarliste der CS mit dem Validierungsstatus?

1.1.1.3. Gibt es Dokumentationen zum Netzwerk der PE, wie z.B. Netzwerkarchitektur (Elektronische Komponenten, Datenbanken und ihre physikalischen und logischen Verbindungen) sowie zur Netzwerktopologie (Verkabelungsstruktur)?

1.2. Risikomanagement

1.2.1.1. Hat die PE ein dokumentiertes Risikomanagementsystem zur Sicherung der Datenintegrität und Qualität der Prüfergebnisse (siehe auch Qualifizierung/ Validierung/ Konfigurationsmanagement, mit Datenhandling-Prozesse usw. (Einzelfragen in 2.1 ff)?

1.3. Personal, Rollen und Verantwortlichkeiten

1.3.0. Allgemein

1.3.0.1. Sind die Verantwortlichkeiten und Berechtigungen von IT-Personal im Zusammenhang mit dem GLP-gerechten -Einsatz in SOPs (intern), Service-Level-Agreements (SLAs, für externe Einheiten) oder Verträge (extern) definiert?

1.3.0.2. Sind die Funktionen von IT-Personal und PL (ggf. auch Prüfpersonal) personell getrennt (z. B. Zugang zum Serverraum)?

1.3.0.3. Sind klare Verantwortungen und Zugriffsberechtigungen für alle Beteiligten definiert?

1.3.0.4. Sind zumindest Verfahren festgelegt, die sicherstellen, dass Interessenkollisionen beider Funktionen ausgeschlossen werden?

1.3.0.5. Liegen Nachweise über aufgabenbezogene, regelmäßige Aus- und Fortbildungen der betroffenen Mitarbeiter zum Umgang mit CS vor?

1.3.0.6. Ist das IT-Personal mit den grundsätzlichen Anforderungen der Guten Laborpraxis vertraut?

1.3.1. Leitung der Prüfeinrichtung (LPE)

Grundsätzlich liegt die Gesamtverantwortung für den Einsatz computergestützter Systeme bei der Leitung der PE. Die Wahrnehmung dieser Verantwortung ist schriftlich zu dokumentieren. Daraus ergeben sich folgende Fragen im Einzelnen:

1.3.1.1. Hat die Leitung der PE die organisatorische Gesamtverantwortung für den Einsatz von IT-Systemen in der PE (IT-Verantwortung als Führungsaufgabe) verinnerlicht?

1.3.1.2. Ist genügend Personal, bei dem die jeweilige Verantwortung für die Entwicklung, Validierung, den Betrieb und die Wartung computergestützter Systeme liegt (ggf. IT-Personal, Systemadministrator etc.) durch die Leitung benannt?

1.3.1.3. Werden Aus- und Fortbildungsmaßnahmen veranlasst und dokumentiert?

1.3.1.4. Hat die Leitung folgende Maßnahmen für den Betrieb von CS vor der Inbetriebnahme etabliert?

Aufzählung relevanter Standardarbeitsanweisungen (SOP) bzw. sonstiger interner Regelungen:

- Anforderungen (z.B. Benutzeranforderungsspezifikation, Validierung, Change-Control) für die interne Entwicklung von Software (z.B. Excel-Datasheets, Statistik-Anwendungen),
- Anforderungen (z.B. Benutzeranforderungsspezifikation, Validierung, Change-Control) für die externe Entwicklung von Software (z.B. Excel-Datasheets, Statistik-Anwendungen),
- Zugangskontrollen zum Schutz vor Verfälschung, unbefugter Änderung oder Verlust von Daten,
- Verfahren zur Verhinderung nicht dokumentierter Änderung von Daten und zum Datenverlust bei Systemausfall und Wartungsarbeiten,
- Festlegung der Verantwortlichkeiten zur Vergabe und Änderung von Zugangsberechtigungen und zur Verwaltung und Überwachung der Zugangskontrollen,
- persönliche Identifizierung beim Zugang zu IT-Systemen,
- ausreichende Schulung des Personals bezüglich Bedienung, Sicherheitsanforderungen und Kenntnis von „Ausweichplänen“,
- Festlegung der Kommunikationswege und deren Dokumentation, speziell bei elektronischer Rohdatenerfassung, z. B. E-mails,
- Rohdatendefinition für alle computergestützten Systeme,
- Definition der Änderungen, die ein formales Change-Control Verfahren (formal fest gelegtes Verfahren zur kontrollierten Systemänderung) erforderlich machen oder

Etablierung eines entsprechenden Bewertungsverfahrens,

- Festlegung von Aufgaben und Verantwortlichkeiten bei Change-Control Verfahren,
- Bereitstellung aller erforderlichen Einrichtungen und Ausrüstungen für die Aufbewahrung und Archivierung elektronisch gespeicherter Rohdaten, Dokumente und unterstützender Aufzeichnungen.

1.3.2. Prüfleiter (PL)

1.3.2.1. Verifiziert vor Beginn einer Prüfung den Validierungsstatus des CS (Siehe auch 2.1 ff). (Sämtliche Daten müssen *zuschreibbar, lesbar, zeitnah, original, korrekt, vollständig, konsistent, dauerhaft* und *verfügbar* sein.)

1.3.3. Qualitätssicherung (QS)

1.3.3.1. Ist die QS an der Überprüfung der Einhaltung der Standards zum Betrieb eines CS beteiligt (Lebenszyklus, Validierung, Change-Control) und sind diese Elemente Teil eines QS-Programms?

1.3.3.2. Ist eine adäquate Ausbildung des QS-Personals zur Überwachung der Einhaltung der GLP Grundsätze beim Einsatz computergestützter Systeme vorhanden (ggf. Benennung spezialisierter Auditoren oder Hinzuziehung externer Spezialisten)?

1.3.3.3. Hat die QS Lesezugriff auf alle GLP-relevanten elektronisch bearbeiteten oder gespeicherten Daten (z.B. Rohdaten, Audit-Trail usw.)?

1.3.3.4. Besteht für die QS die Möglichkeit zur Überprüfung aller für GLP-Prüfungen relevanten IT-Vorgänge und Maßnahmen (z.B. elektronische Archivierung, Prüfpläne, Abschlussberichte usw.)?

1.4. Einrichtungen

1.4.1.1. Sind die Standorte der IT-Systeme (z.B. Serverräume) für den störungsfreien Betrieb geeignet und ggf. Abgleich der tatsächlichen Umgebungsbedingungen am Standort mit den Anforderungen aus den Herstellerangaben (siehe Anforderungen Archivierungsdokument OECD 15)?

1.4.1.2. Ist eine doppelt ausgelegte oder unterbrechungsfreie Stromversorgung (USV) vorhanden oder sind alternative Sicherungssysteme zur Absicherung gegen Datenverlust bei Stromausfällen vorhanden?

1.4.1.3. Sind geeignete Einrichtungen für die sichere Aufbewahrung von Rohdaten vorhanden (Zwischenspeicherung vor Archivierung), falls diese nicht unverzüglich nach Durchführung der Prüfung ausgedruckt werden?

1.5. Inventar

1.5.1.1. Gibt es eine Inventarliste der CS mit dem Validierungsstatus? (siehe 1.1; Diese Liste wird am bestem vor der Inspektion zur Vorbereitung angefordert.)

1.6. Lieferant (siehe 2.6)

1.7. Handelsübliche Standardprodukte (Commercial-of-the-shelf products - COTS)

1.7.1.1. Existiert eine Definition, welche Anwendungen als COTS zu betrachten sind?

1.7.1.2. Wird bei diesen COTS zumindest eine Funktionsprüfung entsprechend den User-Requierements (URS) ausgeführt, wobei die eingesetzte Software risikobasiert zu validieren ist?

1.8. Änderungs- und Konfigurationskontrolle

1.8.1.1. Gibt es ein schriftliches Verfahren zur Änderungskontrolle für alle Phasen des Lebenszyklus (Validierung, Betrieb, Stilllegung) mit den Aufgaben und Verantwortungen der beteiligten Akteure?

1.8.1.2. Wie erfolgt das Risikomanagement (Risikobeurteilung und –bewertung)? (Zur Risikobeurteilung können die Regeln der Softwarekategorisierung entsprechend dem Standard GAMP5 der ISPE angewandt werden.)

1.9. Anforderungen an die Dokumentation

1.9.1.1. Sind die wesentlichen Anforderungen zur Dokumentation (gemäß OECD-Dokument Nr. 17) aufgeführt? Dazu gehören u. a.:

a) der 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 sowie anderen Systemen.

Nach dem das CS beschrieben wurde, sind der Einsatz und die Verantwortlichkeiten angemessen zu dokumentieren. Dazu zählen typischerweise 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 routinemäßig vorbeugende Wartung und Mängelbeseitigung umfassen,

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.

1.9.1.2. Gelten für die zu genannten Dokumente die gleichen Archivierungsfristen, wie für die damit gewonnenen Daten?

2. Projektphase

2.1. Validierung/Qualifizierung

Retrospektive Evaluierung ist nach dem vorliegenden Lebenszyklusmodell nicht mehr anwendbar. Auch Altsysteme müssen genauso behandelt werden wie Neusysteme. In Ausnahmefällen kann auf alte historische Dokumentationen über das CS zurückgegriffen

werden. Zusätzlich müssen Anforderungen definiert werden, wie der Validierungsstatus der GLP-Anforderungen (siehe nachfolgende Fragen) erfüllt werden kann.

2.1.1.1. Gibt es einen Validierungsplan für CS in der PE? Welche Anforderungen sind darin enthalten (Software und Hardware, Inputs, Outputs, Schnittstellen, Sicherheit, Audit Trail, regulatorische Forderungen)? Sind diese Anforderungen risikobezogen ausgewählt und gewichtet worden?
2.1.1.2. Sind die entsprechenden Regelungen und Dokumente (SOPs, siehe 1.3.1) vorhanden?
2.1.1.3. Sind/waren die Verantwortlichkeiten festgelegt (Verantwortlichkeitsmatrix)? Ist/war das Personal für die zugewiesenen Verantwortlichkeiten adäquat qualifiziert?
2.1.1.4. Sind Anforderungen für die interne Entwicklung von Software (z.B. Excel-Datasheets, Statistik-Anwendungen) beschrieben?
2.1.1.5. Entspricht der Validierungsbericht den Vorgaben des Validierungsplans?
2.1.1.6. Wurden Abweichungen vom Validierungsplan begründet und liegt die Zustimmung des Benutzers und des IT-Verantwortlichen vor?
2.1.1.7. Ist der Validierungsbericht von der verantwortlichen Person unterschrieben?
2.1.1.8. Wurde ein Test auf erfolgreiche Installation mit klaren Akzeptanzkriterien durchgeführt?
2.1.1.9. Sind die folgenden Punkte im Testprogramm berücksichtigt: Typische Operationen, Berechnungen und Messungen, Verhalten des Programms bei Extrembedingungen und Extremwerten, Warnmeldungen, Systemwiederherstellung nach Programmabsturz?
2.1.1.10. Fand eine Überprüfung der Gesamtfunktion des Systems unter den Bedingungen des Praxis-Betriebs statt?
2.1.1.11. Wie ist das Verfahren der Änderungskontrolle während der Validierung und des Systembetriebs beschrieben und dokumentiert?

2.2. Änderungskontrolle während der Validierungsphase

Siehe 2.1

2.3. Systembeschreibung

2.3.1.1. Existiert eine Systembeschreibung zur Dokumentation von CS (physische und logische Anordnungen von CS (z.B. Serverstruktur, Netzaufbau), zu Datenflüssen und Schnittstellen mit anderen Systemen oder Prozessen, Hardware- und Softwarevorgaben sowie vorgehaltene Sicherheitsmaßnahmen?

2.4. Benutzeranforderungsspezifikationen

2.4.1.1. Sind in der Benutzeranforderungsspezifikation (User Requirement Specifications – URS) alle GLP-Funktionen/-Anwendungen enthalten, inklusive aller kritischen Funktionen?

2.4.1.2. Spiegelt das Systemdesign die Benutzeranforderungen wieder?

2.4.1.3. Fanden Überprüfungen (Reviews) des Systemdesigns statt?

2.5. Qualitätsmanagementsystem und unterstützende Verfahren

Siehe 2.1

2.6. Kundenspezifische Systeme, Lieferantenqualifizierung

2.6.1.1. Liegen allgemeine Prozeduren (SOP, Direktiven) zur Lieferantenqualifizierung vor?

2.6.1.2. Gibt es einen Qualifizierungsplan?

2.6.1.3. Wurde der Lieferant des computergestützten Systems/der Software nach diesem Qualifizierungsplan qualifiziert?

2.6.1.4. Wurden Rollen und Verantwortlichkeiten zwischen Lieferanten und Leitung der Prüfeinrichtung schriftlich definiert?

2.6.1.5. Wurde der Qualifizierungsplan eingehalten?

2.6.1.6. Wurde ein formales Audit beim Lieferanten vor Ort durchgeführt (oder alternativ durch Übersenden und Ausfüllen einer Checkliste)?

2.6.1.7. Wurden Mängel festgestellt und daraufhin Korrekturmaßnahmen vereinbart?

2.6.1.8. Wurden die Korrekturmaßnahmen überprüft?

2.6.1.9. Gab es periodische Audits auf Einhaltung der internen Vorgaben und projekt-spezifischer Anforderungen?

2.6.1.10. Wurde nach Beendigung des Entwicklungs-Projektes eine angemessene Dokumentation ausgehändigt?

2.6.1.11. Stellt der Lieferant laufenden Support für das gelieferte Produkt (Software) zur Verfügung? Gibt es ein festgelegtes Verfahren zur Implementierung von Upgrades und Patches?

2.6.1.12. Bei Verweis auf Entwicklungsdokumentation des Herstellers: Ist eine formale Einschätzung der Zuverlässigkeit und/oder Überprüfung der Zuverlässigkeit des Herstellers durchgeführt worden?

2.6.1.13. Hat der Hersteller bestätigt, dass interne oder anerkannte QM-Standards während der Entwicklung eingehalten wurden?

2.6.1.14. Hat die Inspektionskommission die Möglichkeit, QM-Dokumentationen einzusehen?

2.7. Prüfungen

2.7.1.1. Existieren Verfahrensanweisungen, die beschreiben, wie Prüfungen (z.B. Installationsprüfungen oder Benutzerakzeptanztests) durchzuführen sind?
2.7.1.2. Basieren Intensität und Umfang der Prüfung auf einer Risikobeurteilung?
2.7.1.3. Werden auch COTS-Systeme getestet und bewertet?
2.7.1.4. (Weitere Fragen zum Thema Prüfungen sind unter 2.1 zu finden)

2.8. Datenmigration

2.8.1.1. Wie werden in der Prüfeinrichtung Softwareupdates/-upgrates (Change Control) durchgeführt (kontrolliert, dokumentiert, Information der Nutzer bei wichtigen/kritischen Updates)?
2.8.1.2. Ist der Migrationsprozess selbst validiert worden oder war Bestandteil einer Validierung?
2.8.1.3. Ist nach Migration ein Abgleich der Daten erfolgt?
2.8.1.4. Ist nach Migration die Verbindung zum alten Audit-Trail und zur elektronischen Signatur noch nachvollziehbar und weiterhin lesbar?
2.8.1.5. Sind bei Erzeugung von PDF-Dokumenten oder Papierversionen alle Metadaten und Audit-Trails exportiert worden?

2.9. Datenaustausch

2.9.1.1. Gibt es eine festgelegte verfahrensbezogene Rohdatendefinition für jedes bei GLP-Prüfungen verwendete computergestützte System (elektronisch gespeicherte Rohdaten oder Papierausdruck)?
2.9.1.2. Sind beim Austausch von elektronischen Daten geeignete Kontrollen der Schnittstellen bezüglich Sicherheit und Systemintegrität definiert und überprüft worden (z.B. Überprüfung des Datenformates beim Export sowie sichere Verschlüsselung bei Nutzung von Funkstrecken zur Kommunikation)?

3. Betriebsphase

3.1. Genauigkeitskontrolle

3.1.1.1. Sind dem Prüfleiter die Medienwechsel bekannt?
3.1.1.2. Wird die Richtigkeit von Datenüberträgen geprüft?
3.1.1.3. Sind Strategien zur Risikominimierung beschrieben und implementiert?
3.1.1.4. Sind automatisierte Kontrollen bei der Validierung des Systems mitgeprüft worden?

3.2. Daten und Datenspeicherung

3.2.1.1. Sind die Datenaufzeichnungen vollständig im Sinne des ALCOA-Konzeptes[2]?
3.2.1.2. Sind Änderungen an Datensätzen sichtbar und nachvollziehbar im Sinne eines Audit-Trails (wer hat was, warum und wann gemacht)?
3.2.1.3. Sind die Daten lesbar und dauerhaft aufgezeichnet?
3.2.1.4. Wurden die Daten zeitnah aufgezeichnet?
3.2.1.5. Sind es die Originaldaten oder zertifizierte, echte Kopien?
3.2.1.6. Sind die Aufzeichnungen fehlerfrei bzw. wurden nicht verändert oder dokumentiert ergänzt?
3.2.1.7. Liegen sämtliche Rohdaten inklusive Auswertungen vor?
3.2.1.8. Spiegeln die Zeit- und Datumsstempel die chronologische Abfolge wieder?
3.2.1.9. Wie erfolgt die Aufzeichnung über den gesamten Archivierungszeitraum?
3.2.1.10. Sind die Daten jederzeit verfügbar und zugänglich z.B. beim Audit?

3.3. Ausdrucke

3.3.1.1. Enthält der Ausdruck alle elektronischen Daten, einschließlich der abgeleiteten Daten sowie der Metadaten und ggf. die beim Audit-Trail festgehaltenen Änderungen und erfolgt dieser zeitnah?

3.4. Audit-Trails

3.4.1.1. Bei Verwendung von IT-Systemen zur Rohdatenerfassung und -Verarbeitung, Abschlussberichterstattung: Erzeugung und Aufbewahrung eines vollständigen Audit Trails?
3.4.1.2. Ist die Möglichkeit der Überprüfung des Audit Trails auch nach Abschluss der Prüfung durch die GLP Inspektionskommission möglich?
3.4.1.3. Ist eine eindeutige Zuordnung der erhobenen Daten zu der Person, die die Daten erhoben hat, möglich (z. B. über personenbezogene Rechte, Kombination aus Benutzerkennung und Passwort)?
3.4.1.4. Ist eine vollständige Rückverfolgbarkeit von Änderungen (Datum, Uhrzeit, Person, die die Änderung vorgenommen hat, Gründe für Änderung) gegeben?
3.4.1.5. Sind die ursprünglichen Daten nach Änderung weiterhin unverändert vorhanden? Sind alle geänderten Daten auch nach mehrfacher Änderung noch sichtbar?
3.4.1.6. Ist gesichert, dass die Möglichkeit, Modifikationen an den Einstellungen für den Audit-Trail vorzunehmen auf dazu befugtes Personal beschränkt bleiben? Das gesamte an einer Prüfung beteiligte Personal (z. B. Prüfleiter, Leiter von

[2] ALCOA: **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, **A**ccurate (zuschreibbar, lesbar, zeitnah, original, korrekt). Anforderungen an Datenintegrität aus GAMP, ergänzt um weitere Anforderungen als ALCOA+. Siehe auch Anhang 3, Teil 1.

analytischen Abteilungen, Analytiker usw.) darf keine Berechtigung haben, Änderungen an den Audit-Trail-Einstellungen vorzunehmen.

3.4.1.7. Wird das Audit-Trail-Verfahren im QS-Programm als kritische Phase integriert und überwacht?

3.5. Änderungs- und Konfigurationsmanagement

3.5.1.1. Gibt es ein Änderungs- und Konfigurationsmanagement-Verfahren, welches von der LPE genehmigt wird?

3.5.1.2. Z.B. Software-Versionsänderungen, Modulfreischaltungen, Einsatz von selbstentwickelten Ergänzungen/Erweiterungen des Systems, Einsatz von selbstentwickelten Makros, Einsatz neuer Betriebssystem-Versionen, Einsatz neuer Gerätetreiber/ Datenübertragungsprotokolle, Einsatz neuer Speichereinheiten, Erweiterung des Systems (z. B. Einbindung in ein Netzwerk), Einsatz neuer Ausgabegeräte/Treibersoftware.

3.5.1.3. Ist das Änderungs- und Konfigurationsmanagement-Verfahren vor Nutzung des IT-Systems für GLP- Prüfungen etabliert worden?

3.5.1.4. Liegen die formale Genehmigung und die Dokumentation jeder geplanten Änderung während des Einsatzes des IT-Systems vor?

3.5.1.5. Gibt es eine Bewertungsmethode zur Entscheidung über den erforderlichen Umfang einer erneuten Systemüberprüfung (Revalidierung) nach erfolgten Änderungen?

3.5.1.6. Sind die für die jeweiligen Entscheidungen verantwortlichen Personen benannt?

3.6. Regelmäßige Überprüfung

3.6.1.1. Gibt es regelmäßige Überprüfungen des CS, die sicherstellen, dass der valide Zustand weiterbesteht und den GLP-Status der Datengewinnung/ –verarbeitung bestätigen (angemessen bezüglich der Komplexität und Kritikalität des Systems) und wie wird die Überprüfung (siehe Teil 1, 3.6) dokumentiert?

3.6.1.2. Sind die verantwortlichen Personen (z. B. Geräteverantwortliche) benannt?

3.6.1.3. Wird bei der Überprüfung von komplexeren Systemen (wie Datenbanken, LIMS, Netzwerken usw.) IT-Fachpersonal einbezogen?

3.6.1.4. Werden auch die gemeldeten unerwarteten Ereignisse (z.B. Fehlermeldungen, Systemabstürze) erfasst, die möglicherweise den Validierungsstatus des Systems beeinflusst haben könnten?

3.7. Physische, logische Datensicherheit und Datenintegrität

3.7.1. Allgemeines

3.7.1.1. Sind Regelungen zur IT-Sicherheit etabliert?

3.7.1.2. Wurde das Personal auf die Wichtigkeit der Regeln zur IT-Sicherheit aufmerksam gemacht (z.B. durch Schulungen)?

3.7.1.3. Ist das IT-Personal in die GLP Grundsätze und die zutreffenden SOPs eingewiesen?

3.7.2. Physische Sicherheitsvorkehrungen

3.7.2.1. Ist eine Beschränkung des Zugangs zu Gebäuden oder Räumen mit dort fest installierten IT-Systemen auf befugtes Personal durch die üblichen physischen Sicherheitsmaßnahmen (Türschlüssel, Türschlösser mit Zahlencodes, Berechtigungskarten, biometrische Systeme, Werksausweis etc.) gegeben?
3.7.2.2. Wird die Erstellung, Änderung und Löschung von Zugangsberechtigungen protokolliert?
3.7.2.3. Existieren zusätzliche Sicherheitsmaßnahmen bei Verwendung drahtloser Kommunikationswege (WLAN, Funkstrecken)?
3.7.2.4. Ist das WLAN-Passwort ausreichend komplex?
3.7.2.5. Werden bei WLAN-Routern regelmäßig die Zugangsprotokolle geprüft?
3.7.2.6. Werden Techniken wie z.B. SSL-VPN eingesetzt, wenn von außen auf das Netzwerk der Prüfeinrichtung zugegriffen wird?

3.7.3. Logische Sicherheitsvorkehrungen

3.7.3.1. Existieren Zugangskontrollen zu Betriebssystemen und Anwendungen?
3.7.3.2. Sind Regeln für Passwortlänge und Komplexität definiert?
3.7.3.3. Sind Sicherheitsmaßnahmen wie Bildschirmsperre nach Zeit aktiviert?
3.7.3.4. Ist sichergestellt, dass bei Laboranwendungen das Laborpersonal nur auf die Bereiche Zugriff hat, die für die jeweiligen Aufgaben auch relevant sind (need to know Prinzip)?
3.7.3.5. Gibt es eine Standardarbeitsanweisung zur geregelten Vergabe von Zugängen zum Betriebssystem (z.B. Active Directory) und Rollenzuweisungen bei GLP-relevanten Laboranwendungen?
3.7.3.6. Werden Virenscanner und Firewalls zur Abwehr von bösartigen Codes eingesetzt?
3.7.3.7. Wie ist die ausschließliche Verwendung von genehmigten Programmversionen und validierter Software bei GLP Prüfungen gewährleistet?
3.7.3.8. Erfolgt eine Überwachung und ggf. Blockierung der Übernahme von Daten oder Software aus externen Quellen (z. B. durch Voreinstellungen im Betriebssystem oder spezielle Sicherheitssoftware)?
3.7.3.9. Datenintegrität / Datensicherung
3.7.3.10. Ist eine Sicherung der Datenintegrität durch Einhaltung der Sicherheitsmaßnahmen, routinemäßige Systemzugangskontrollen und durch Dateiüberprüfungsroutinen (z. B. Quersummencheck) vorhanden?
3.7.3.11. Sind dokumentierte Verfahren zur Datensicherung durch regelmäßige Kopien erforderlich und werden diese automatisch erstellt und sicher aufbewahrt?
3.7.3.12. Gibt es dokumentierte Verfahren zur Wiederherstellung von Daten im Falle einer Fehlfunktion (z. B. Plattendefekt)?

3.8. Störfallmanagement (Incident Management)

3.8.1.1. Werden die Aufzeichnungen zum Störfallmanagement regelmäßig ausgewertet?

3.8.1.2. Ist die Dokumentation so gestaltet, dass der Störfall von der GLP Studie zum Computersystem und umgekehrt rückführbar ist?

3.8.1.3. Ist sichergestellt, dass der Prüfleiter nötige Informationen über einen Störfall erhält, um die Datensicherheit seiner Studie beurteilen zu können?

3.8.1.4. Werden die Störfall-Aufzeichnungen zusammen mit der Systemdokumentation archiviert?

3.9. Elektronische Unterschrift

3.9.1.1. Werden elektronische Unterschriften (Signaturen) angewendet?

3.9.1.2. Wird bei der elektronischen Genehmigung des Prüfplans und der Unterzeichnung des Abschlussberichtes die Verwendung von *qualifizierten Signaturen, Siegeln und Zeitstempeln* gemäß elDAS-Verordnung (EU) Nr. 910/2014 sichergestellt (Siehe Teil 1, 3.9)?

3.9.1.3. Werden bei anderen elektronischen Freigaben (z. B. SOP oder Prüfgegenstände) andere *sichere und validierte Verfahren,* wie z.B. *fortgeschrittene Signatur, Siegel und Zeitstempel* verwendet? (Für das übliche Datenhandling ist ein Audit-Trail angemessen.)

3.9.1.4. Ist die elektronische Unterschriftsfunktion in den Systemanforderungen erwähnt und in den Systemverfahren validiert worden?

3.9.1.5. Existiert ein Verfahren zum Thema elektronische Unterschrift, das den ordnungsgemäßen Betrieb der elektronischen Unterschriftsfunktionen des computergestützten Systems regelt und gewährleistet. Dazu gehören Fragen wie:

3.9.1.6. Welche Aufzeichnungen benötigen eine handschriftliche Unterschrift oder eine elektronische Unterschrift?

3.9.1.7. Welche Personen sind berechtigt, elektronische Unterschriften in welcher Rolle prüfungsbezogen zu leisten?

3.9.1.8. Wie wird gewährleistet, 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.)

3.9.1.9. In welcher Form werden Metadaten, die mit der elektronisch unterzeichneten Aufzeichnung verbunden sind, eindeutig identifiziert (z.B. Methodenparameter und Systemkonfiguration)? Die Signaturfunktion des computergestützten Systems muss die Gleichzeitigkeit der Verknüpfung zwischen der elektronisch unterzeichneten Aufzeichnung und den erläuternden Metadaten gewährleisten (Siegelfunktion).

3.9.1.10. Wie werden Änderungen an der geleisteten elektronischen Unterschrift oder an der Verknüpfung zu den verbundenen Metadaten verhindert?

3.9.1.11. Wird sichergestellt, dass Änderungen an elektronisch unterzeichneten Aufzeichnungen (oder die unterstützenden Metadaten) durch die für die Änderung verantwortliche Person erläutert, (elektronisch) unterzeichnet und mit Datum zu versehen wird (Audit-Trail)?

3.9.1.12. Ist für den Fall, dass sowohl elektronische Aufzeichnungen und deren gedruckte Entsprechung parallel aufbewahrt werden, festgelegt, welches die vorgeschriebene Aufzeichnungsart ist, um das entsprechende Kontrollverfahren zur Anwendung zu bringen?

3.10. Datenfreigabe

3.10.1.1. Sind die Prozesse, bei denen eine Datenfreigabe elektronisch erfolgt (z. B. Freigabe über Standardarbeitsanweisungen (SOP)) Bestandteil der Systemvalidierung und in SOPs beschrieben?

3.11. Archivierung

3.11.1.1. Ist die elektronische Archivierung validiert worden?

3.11.1.2. Ist im Rahmen der Validierung eine Risikoanalyse erstellt worden, die Hosting-Systeme und Datenformate betrachtet, um Zugänglichkeit, Lesbarkeit und Datenintegrität während der Archivierungsfrist zu beurteilen?

3.11.1.3. Ist ein indexiertes Verzeichnis vorhanden, sind Such-Algorithmen etabliert und sind die verantwortlichen Archivare in der Lage, Daten rasch aufzufinden und lesbar zu machen?

3.11.1.4. Ist sichergestellt, dass es nur einen Archiv-Verantwortlichen (gemäß OECD-Guideline 15) gibt (keine gleichrangigen Papier- und IT-Archivverantwortlichen)?

3.11.1.5. Sind elektronische Rohdaten nach Archivierung so geschützt, dass diese nicht mehr verändert werden können?

3.11.1.6. Können elektronische Signaturen über den Archivierungszeitraum verifiziert werden?

3.11.1.7. Werden die zusätzlichen physischen Anforderungen an elektronische Archive erfüllt (z.B. Temperatur, Luftfeuchte, Notstromversorgung): Lagerungsbedingungen entsprechend der Anforderung der Speichermedien?

3.11.1.8. Ist das IT Personal in die GLP Grundsätze und die zutreffenden SOPs eingewiesen?

3.11.1.9. Untersteht das IT Personal, welches die Verantwortung für das elektronische Archiv hat, dem Leiter der PE oder liegt ein entsprechender Vertrag vor?

3.11.1.10. Ist die QS qualifiziert zur Prüfung der elektronischen Archivierung? (ggf. unter Einbeziehung von externem Sachverstand)

3.11.1.11. Wie ist der logische Zugriff auf archivierte Daten geregelt (Lesezugriff von Mitarbeitern, QS)? Wird der Zugriff protokolliert?

3.11.1.12. Liegt eine Berechtigungsmatrix vor? Sind Zugriffsrechte, Schreibrechte personenbezogen zugeordnet? Wie wird das System administriert? Welcher Administrator hat weiche Rechte? Ist die Administration von Prüfungen unabhängig?

3.11.1.13. Ist die Lesbarkeit aller archivierten Dateiformate über den gesetzlich vorgegebenen Zeitraum von 15 Jahren gesichertt? Werden keine plattformunabhängigen Dateiformate (html, pdf, tiff, ascii) verwendet, sind ggf. die erforderlichen Systeme zusätzlich zu archivieren.

3.11.1.14. Werden geeignete und qualifizierte Speichermedien verwendet?

Geeignet sind unter anderem Hardware-WORMs, die sich physikalisch nur einmal beschreiben lassen, systemische WORMs, die den einmaligen Schreibvorgang durch interne Hardware sicherstellen und Software-WORMs, bei denen durch Programmierung Lösch- und Änderungsvorgänge ausgeschlossen sind. Beispiele für:

- Hardware WORMs sind optische Medien.
- Systemische WORMs sind Magnetbänder oder Festplatten, bei denen die write-once Funktionalität durch Adressierung der Speicherung mit internem Prozessor oder mit CAS Technik (Content Adressed Storage) softwareseitig sichergestellt wird.
- Software-WORMs sind Festplatten oder Magnetbänder in Netzwerkspeichersystemen, bei denen die Software Änderungs- und Löschvorgänge verhindert.

3.11.1.15. Wird die Lesbarkeit der Daten auf den Medien regelmäßig überprüft?

3.11.1.16. Archivierungsumfang: Werden alle zur vollständigen Abbildung einer Prüfung erforderliche Daten archiviert? Dies betrifft neben Rohdaten, bearbeiteten und berichteten Daten auch Meta-Daten, audit trails, Autorisierungen und ggf. elektronische Signaturen.

3.11.1.17. Gibt es ein etabliertes Verfahren bei System- oder Programmwechsel, z.B. Datenübertragung (Migration)? Diese ist nur mit validierten Verfahren (Detailanforderungen in Ziffer 8, des Anhang 6 dieses Handbuchs) zulässig. Alternativ besteht die Option autorisierte Papierausdrucke zu archivieren. .

3.11.1.18. Werden alle Unterlagen zur Entwicklung, Validierung, Betrieb, Wartung und Überwachung von IT-Systemen, die bei GLP-Prüfungen eingesetzt werden, über den gesetzlich vorgeschriebenen Zeitraum aufbewahrt?

3.11.1.19. Sind elektronische Signaturen über den Archivierungszeitraum verifizierbar?

3.11.1.20. Sind in den Prüfberichten sämtliche GLP-relevante elektronische Daten angegeben (inkl. Speicherort)?

3.11.1.21. Sind Sicherungskonzepte zum Schutz vor Datenverlust (z.B. durch Nutzung verschiedener WORM-Medien) vorhanden?

3.11.1.22. Liegt bei Vernichtung elektronisch archivierter Daten die Zustimmung der Leitung vor?

3.12. Desaster Recovery (Wiederherstellen nach Systemausfällen)

3.12.1.1. Existieren validierte, dokumentierte und getestete Maßnahmepläne für den Fall eines Systemausfalls, die risikobasiert Maßnahmen in Abhängigkeit ihrer Bedeutung (Kritikalität) für die Qualität der Prüfergebnisse und des zeitlichen und personellen Aufwandes festlegen?

3.12.1.2. Stellen die Maßnahmepläne die Integrität der Daten und der Prüfung in allen Phasen sicher?

3.12.1.3. Kennt das GLP-Personal diese Notfallpläne?

3.12.1.4. Sind Sicherheitskopien der eingesetzten Software verfügbar (evtl. bei einem Dritten hinterlegt oder im Rahmen eines Service Level Agreement)?

4. Stilllegungsphase

4.1.1.1. Gibt es ein Verfahren zur Stilllegung von CS und ist die Migration bzw. Archivierung der GLP-relevanten Daten gesichert?