Der TMF-Systemvalidierungsmasterplan

(SVMP)

Ein Leitfaden für die Validierung computergestützter Systeme in medizinischen Forschungsverbünden

Version 04, 06.12.2016

Projektgruppe Systemvalidierung (TMF)

Der TMF-Systemvalidierungsmasterplan (SVMP)

Ein Leitfaden für die Validierung computergestützter Systeme in medizinischen Forschungsverbünden

Version 04, 06.12.2016

Projektgruppe Systemvalidierung (TMF)

Inhaltsverzeichnis

1 Zweck und Anwendungsbereich

1.1 Zweck

Dieser Systemvalidierungsmasterplan (SVMP) ist ein Leitfaden zur Validierung computergestützter Systeme in der medizinischen Forschung. Er berücksichtigt die besonderen Bedingungen wie sie beispielsweise in den vernetzt forschenden Mitgliedsverbünden des TMF e.V. anzutreffen sind.

Die generelle Validierungsstrategie beim Einsatz computergestützter Systeme sowie Vorgehen, Verantwortlichkeiten, Nutzen und Ziele der Validierung werden allgemeingültig für derartige Forschungsverbünde beschrieben. Der Leitfaden soll ferner Hinweise und Anleitungen geben, wie von Herstellern einer Anwendungssoftware ein fachlich und rechtlich fundierter Nachweis eingefordert werden kann, der bestätigt, dass der Hersteller über die nötigen Qualifizierungen verfügt, die ihm erlauben, Systeme zu erstellen, zu liefern und zu warten.

Forschungsverbünde, die eigenständig Software entwickeln, soll dieser Leitfaden bei der Konzipierung und Validierung ihrer Systeme unterstützen.

Dem SVMP untergeordnet sind die individuellen Validierungspläne (VP), die die Validierung der dezidierten Systeme in einem Verbund beschreiben.

1.2 Dokumente zum SVMP

In diesem SVMP wird auf die von der Projektgruppe erstellten Dokumente verwiesen (SOPs, Anhänge, Checklisten), die einer Nummerierung und Versionierung unterliegen.

Die Nummerierung ist wie folgt aufgebaut: X-XXX. Die erste Ziffer (beginnend mit 1) beschreibt das Modul, die nächsten Ziffern fortlaufend die entsprechende Dokumentennummer.

Weiterhin stehen ausführliche **Schulungsunterlagen** (PowerPoint-Folien) zur Verfügung.

1.3 Anwendungsbereich

Dieser Leitfaden wurde von den auf dem Deckblatt aufgeführten Personen nach bestem Wissen und Gewissen unter Bezugnahme auf die für die Bundesrepublik Deutschland geltenden rechtlichen Grundlagen und Richtlinien erstellt. Er richtet sich insbesondere an die Mitgliedsverbünde des TMF e.V.

1.3.1 Geschäftsbereiche der TMF

Die bisherige Arbeit der TMF als Dachorganisation für die medizinischen Forschungsverbünde besteht darin, gemeinsam mit Experten aus der Praxis übergreifende Probleme zu identifizieren und gemeinsame Lösungen zu erarbeiten.

Auf diese Weise wird dafür Sorge getragen, dass die Organisation und Infrastruktur medizinischer Forschung in vernetzten Strukturen verbessert wird und auch effektiver erfolgt. Diese langfristig angelegte Zielsetzung erfordert Kontinuität. Nur auf diese Weise können gewünschte Synergien erzielt und Optimierungspotenziale freigesetzt werden. Strategien und Ausbau der IT-Infrastruktur zur Verbesserung der medizinischen Verbundforschung in Deutschland mit der damit verbundenen Validierungsproblematik sollen gemeinsam gelöst werden. Eine aktuelle Auflistung der Mitglieder ist über die Homepage der TMF abrufbar.

Übergreifende Lösungen zur Optimierung der notwendigen Arbeitsprozesse zu schaffen und den Mitgliedern bereitzustellen ist eine der Zielsetzungen der TMF. Beispiele für übergreifende Fragestellungen sind:

- Erhebung, Verarbeitung und Austausch von Forschungsdaten
- Klärung rechtlicher und ethischer Grundlagen
- Qualitätssicherung und Qualitätsmanagement
- Entwicklung und Ausbau leistungsfähiger IT-Infrastrukturen
- Implementierung in vernetzten Strukturen
- Beiträge zu einer nachhaltigen und effizienten Gesundheitsforschung
- horizontale und vertikale Vernetzung zwischen Arztpraxen und Kliniken

Um die Verbünde bei der Validierung eingesetzter Computersysteme in diesen Bereichen zu unterstützen und einen möglichst einheitlichen Validierungsstandard der Computersysteme zu ermöglichen, wurde die Projektgruppe Systemvalidierung gegründet.

1.3.2 Betrachtete Prozesse

Die Durchführung klinischer Studien und das Führen von Patientenregistern gehört zum Hauptgeschäftsbereich der Forschungsverbünde der TMF.

Ohne den Einsatz computergestützter Systeme können die hierfür notwendigen Arbeitsprozesse nicht durchgeführt werden. Der „Lebenszyklus“ einer klinischen Studie beginnt mit der Erstellung des Studienprotokolls und endet mit der Einreichung der Studiendaten bei Zulassungsbehörden bzw. der Erstellung eines Endberichtes oder auch mit Publikationen. Dazwischen liegen Prozesse des Studien- und Datenmanagements sowie die biometrische Auswertung. Zur Unterstützung dieser Prozesse werden unterschiedliche Softwarelösungen eingesetzt: Studienmanagementsystem, CMS, EDC-System, Projektmanagementsystem und Statistiksoftware. Häufig kommen auch zentrale Patientenregister für verschiedene Erkrankungen oder zentrale Randomisierungsdienste zum Einsatz. Darüber hinaus können auch Biomaterialbanken (Serumbank und Gewebebank) angeschlossen sein.

Der daraus resultierende Datenfluss bei der Studiendurchführung oder Einsatz von Patientenregistern (von der Erfassung der Patientendaten bis hin zur Auswertung) muss eine hohe Qualität gewährleisten. Daher müssen sowohl die eingesetzten Softwarelösungen wie auch die Arbeitsbereiche komplett dokumentiert sein.

Ergänzt wird dieser Datenfluss noch durch die Integration von Versorgungs- und Forschungsdaten aus Praxis-Dokumentationssystemen. Diese Dokumentationssysteme werden aus Gründen der Datensicherheit überwiegend als Stand-alone-Programme für Windows-Rechner betrieben und besitzen keine Internetanbindung. Eine Vernetzung mit einer zentralen Datenbank ist somit nicht vorhanden und Daten aus externen Dokumentationssystemen müssen häufig in Register importiert werden.

1.3.3 Betrachtete Systeme

Im Bereich der Systemvalidierung werden verschiedene Schlüsselbegriffe verwendet, die zunächst einmal definiert werden müssen. Zum einen muss das Objekt, also das System beschrieben werden,

das es zu validieren gilt, zum anderen die einzelnen Tätigkeiten des Validierens. Die Tätigkeiten (wie ist zu validieren?) werden in Kap. 2.1 definiert. Im Folgenden werden die Systeme (was ist zu validieren?), Systemarten und Geräte beschrieben.

Begriffsdefinitionen:

1. Computersystem

Ein Computersystem besteht aus den Teilen Hardware und Software. Hardwarekomponenten eines Computersystems bestehen aus Rechner mit Massenspeicher, Bildschirm, angeschlossenen Geräten wie Drucker oder Barcode-Lesegeräte sowie der physischen Verkabelung. Bei der Software wird zwischen Systemsoftware und Applikationssoftware unterschieden. Zur Systemsoftware werden Betriebssysteme, Kommunikationssoftware und Datenbanksysteme gezählt. Die Applikationssoftware dagegen ist das Anwendungsprogramm, das zur Unterstützung klinischer Forschung dient, also überwiegend die Studiensoftware. Die Applikationssoftware ist dabei entweder ein eigen entwickeltes Individual-Softwaresystem, ein Open-Source Produkt oder ein kommerzielles Standard-Softwarepaket.

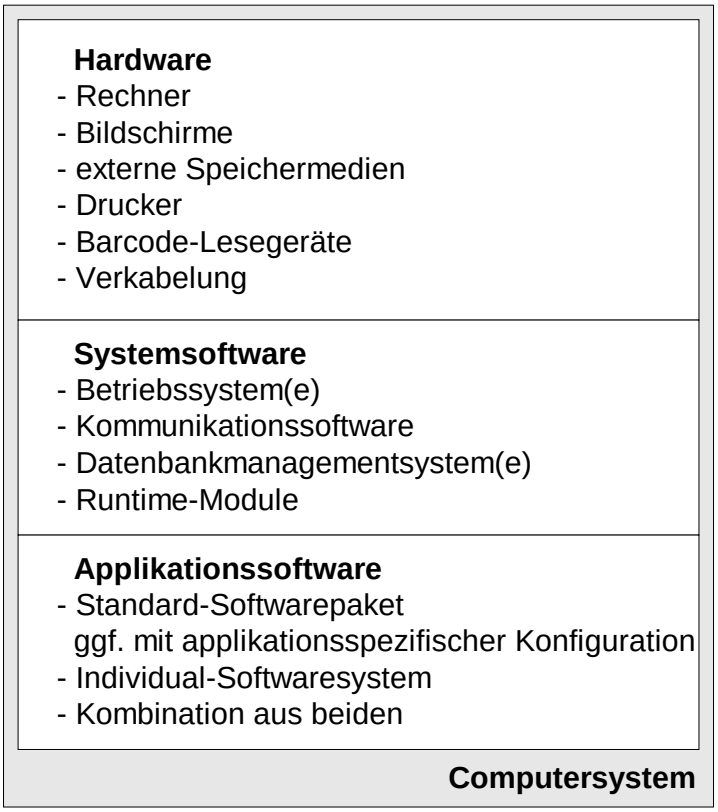

Abb. 1: Computersystem

2. Computerisiertes System

Häufig wird ein Computersystem um Geräte oder Peripherie-Einheiten erweitert (z.B.: Laborgeräte, CMS, mobile Erfassungssysteme, Etikettiersystem, Scanner, etc). Diese werden durch das Computersystem gesteuert oder kontrolliert. Ein solches Computersystem, das um die "kontrollierte Funktion" erweitert wurde, nennt man ein computerisiertes System.

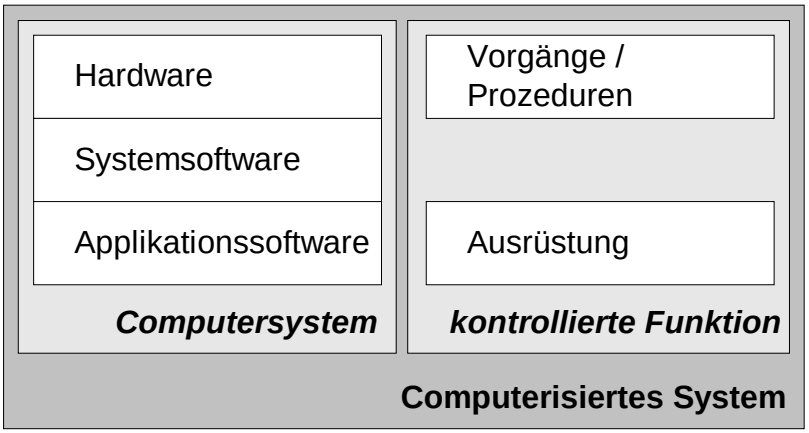

Abb. 2: Computerisiertes System

Ein computerisiertes System führt einen Prozess aus. Dies kann ein Laborprozess, ein Dokumentensteuerungsprozess oder ein anderer validierungspflichtiger Prozess sein.

Dabei wird das computerisierte System in einer Arbeitsumgebung eingesetzt, es erhält Input von Anwendern oder angeschlossenen Geräten, verarbeitet diesen, gibt Informationen aus oder an angeschlossene Geräte weiter. Das computerisierte System ist verschiedensten Faktoren ausgesetzt, die einen Einfluss auf das System haben.

3. Computergestütztes System

Ein computerisiertes System, das seine Funktion in der normalen Produktionsumgebung erfüllt, ist ein computergestütztes System.

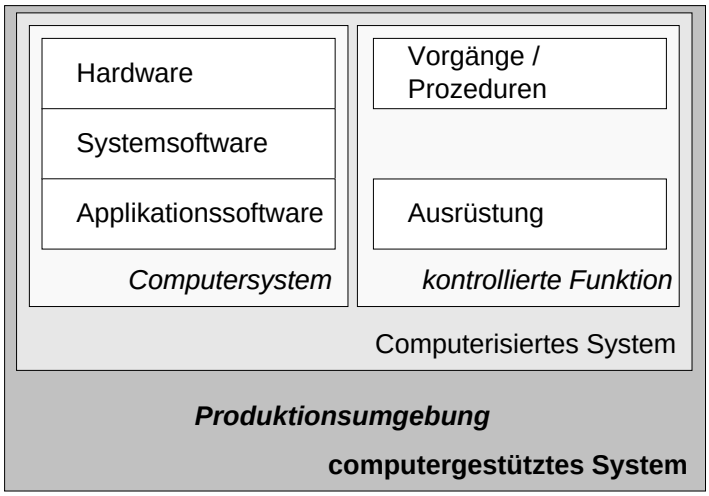

Abb. 3: Computergestütztes System

Daraus ergibt sich, dass die Validierung des *computergestützten Systems* gemeint ist, wenn von einer Software-Validierung oder einer Computer-Validierung gesprochen wird. Um jedoch unmittelbar betroffene Anwender nicht zu verunsichern sind alle drei Begriffe gültig, beziehen sich jedoch grundsätzlich auf das computergestützte Gesamtsystem in der Produktionsumgebung.

1.3.4 GCP-Systeme

Für GCP-Systeme (oder allgemeiner auch GxP-Systeme) müssen Grundsätze und Richtlinien eingehalten werden. Eine einheitliche Vorgehensweise für die Planung einer Validierung sollte vorhanden sein und durch die Qualitätssicherung eines Forschungsverbundes und weitere Verantwortliche (Leitung, Validierungsteam) genehmigt werden.

Die Anwendungsbereiche, in denen GCP relevante Daten verarbeitet werden, müssen definiert und dokumentiert sein. Dies gilt nach neuer 12. AMG-Novelle auch für Investigator Initiated Trials (IITs). Für die elektronische Verarbeitung und Speicherung von Patientendaten und anderer zulassungsrelevanter Daten, sowie deren Freigabe durch elektronische Unterschriften ist die Validierung der computerisierten Systeme zwingend erforderlich. Der Einsatz integrierter Applikationen erhöht dabei die Komplexität des gesamten Systems. Deshalb ist es sinnvoll, jedes integrierte System aufzuteilen in Applikationen, Module oder Interfaces, die Validierung verlangen sowie solche Module, die ohne Validierung auskommen. Das computergestützte System (Applikation, Modul, etc.) wird dann validiert, wenn es

- GCP relevante Daten generiert, modifiziert oder deletiert
- Für GCP-Prozesse oder Funktionen eingesetzt wird
- GCP relevante Daten für andere Systeme oder für GxP-Prozesse bereitstellt

1.3.5 Geräte

Für die Validierung wird eine Beschreibung aller Geräte und Anwendungen erstellt. Die Beschreibung beinhaltet

- Aufgaben der einzelnen Module/Komponenten
- Betrachtung der Vernetzung der Module/Komponenten
- Betrachtung der Schnittstellen der Module/Komponenten
- Beschreibung, wie die Module miteinander vernetzt sind

Hardware

Für die Validierung wird eine Dokumentation der technischen Infrastruktur erstellt, welche eine Beschreibung der eingesetzten Hardware (Hersteller, Typ, Modell, Speicherumfang, Zusatzkomponenten, etc. umfasst. Dabei werden folgende Aspekte berücksichtigt:

- Abgrenzung externer Geräte:
  Beschreibung der von externen Geräten gelieferten Datenstrukturen.
- Beschreibung des Rechnerbetriebs (Hardware und Software):
  Beschreibung des Betriebssystems, ggf. der Netzwerk-Software sowie der eingesetzten Datenbanken;
  Versionsnummer der Software;
  Dokumentation (z.B. Handbuch) über Hardware und Betriebssystemsoftware.

Software

Für die Validierung wird eine Beschreibung der Software erstellt, die folgende Aspekte berücksichtigt:

- Listen der Programme mit Versionsnummern, Art der Dokumentation, etc.,
- Versionsführung und -änderung von Programmen durch Dokumentation von Updates einschließlich der jeweiligen Versionsnummern.

Bei den eingesetzten Produkten kann es sich um kommerzielle Produkte (COTS-commercial-off-the-shelf Lösungen) handeln, aber auch der Einsatz von Eigenentwicklungen sowie Open-Source Produkten und speziell von Softwarefirmen entwickelte Lösungen (bespoken) kommt in Betracht. Der Umfang der Validierung ist bei Eigenentwicklungen und Open Source Produkten in der Regel höher im Vergleich zu kommerziellen Anbietern, da hier der komplette Validation System Life Cycle des Systems betrachtet werden muss. Beim Einsatz kommerzieller Systeme fallen gewisse Bereiche in die Verantwortung des Herstellers.

2 Validierungspolitik

2.1 Definition von Validierung

2.1.1 Verifizierung

Der Begriff Verifizierung ist gleichzusetzen mit der Aktivität "Testen/Prüfen". Durch Testen des Systems (Verifizieren) wird sichergestellt, dass die festgelegten Anforderungen in der praktischen Anwendung erfüllt sind.

2.1.2 Qualifizierung

Qualifizierung wird allgemein als "Beweisführung, dass Ausrüstungsgegenstände einwandfrei arbeiten und tatsächlich zu den erwarteten Ergebnissen führen", definiert. Dies bedeutet für computergestützte Systeme, dass das Computersystem und das computerisierte System qualifiziert werden. Somit ist Qualifizierung ein Teil der Validierung eines computergestützten Systems.

2.1.3 Validierung

Der Begriff "Validierung" wird im Allgemeinen mit zweierlei Bedeutung verwendet. Zum einen ist eine spezifische Tätigkeit gemeint, nämlich die Durchführung eines "Validierungslaufs", der sich an die zuvor erfolgten Qualifizierungsläufe anschließt und den Abschluss des Validierungsprozesses darstellt.

Zum anderen ist mit "Validierung" die Summe der Tätigkeiten des Verifizierens und Qualifizierens gemeint.

Die Validierung computergestützter Systeme ist der dokumentierte Nachweis, dass ein Daten verarbeitendes System mit einer hohen Wahrscheinlichkeit das leistet, geleistet hat und leisten wird, was es laut Pflichtenheft oder Anforderungsbeschreibung leisten soll. Zu diesem Zweck muss ein Validierungsplan aufgestellt werden, nach dem verfahren werden muss.

Als Dokumentation sind Standard Operating Procedures (SOP), Handbücher (Benutzer und Wartung) und Schulungsnachweise erforderlich. Um diese Vielzahl von Dokumenten und Dateien zu strukturieren, zu eigenen Interessen oder zur Veranschaulichung gegenüber der inspizierenden Seite, ist es erforderlich, einen Validierungs-Master-Plan zu erstellen.

Die Validierung computergestützter Prozesse wird erlangt durch die Qualifizierung des jeweiligen computerisierten Systems sowie durch den Nachweis der korrekten Leistung des Systems in seiner Produktionsumgebung. Einen wesentlichen Teil der Qualifizierungsmaßnahmen stellt das Testen (Verifizieren) des computerisierten Systems dar.

Ein System ist validiert, wenn alle nachfolgenden Punkte erfüllt sind:

- Das Systemumfeld ist beschrieben.

- Eine Risikobetrachtung wurde durchgeführt
- Die Systemdokumentation ist vorhanden und von den verantwortlichen Personen genehmigt.
- Alle Arbeitsrichtlinien (SOPs) sind erstellt, und es wird danach verfahren.
- Alle Überprüfungs- und Abnahmeverfahren sind etabliert und durchgeführt.
- Alle Verfahren für Systemänderungen und Normalbetrieb sind etabliert.
- Alle laufenden Ereignisse und Aktionen (Eingriffe) werden aufgezeichnet.
- Alle gesetzlichen oder selbst definierten Anforderungen sind erfüllt

Ein System bleibt validiert, wenn bei Änderungen nach folgenden Kriterien verfahren wird:

- Alle Änderungen werden dokumentiert.
- Die Änderungen wurden klassifiziert (Risikoanalyse)
- Es werden "Revalidierungstests" durchgeführt.
- Überprüfungs- und Abnahmeverfahren werden erneut durchgeführt. Im Normalbetrieb werden "Evaluierungs-Tests" gefahren. Erweiterungen werden nach den gesetzlichen Richtlinien durchgeführt.
- Derzeitiger Stand der Wissenschaft und Technik wird berücksichtigt

2.2 Validierungspolitik der Verbünde

Die Verbünde haben ein einheitliches und konsistentes Vorgehen bei der Validierung, sie besitzen eine Validierungspolitik. Laut FDA bedeutet Validierung: “to establish documentary evidence that provides a high degree of assurance that the computer systems will consistently produce a product or result meeting predetermined specifications, requirements and quality attributes. This evidence is presented to concerned parties to provide assurance that systems and processes as well as test methods are under control and are repeatable.” Die wichtigen Punkte liegen hierbei in der Notwendigkeit, dokumentierte Evidenz zu liefern, und dass das Computersystem vordefinierten Spezifikationen, Anforderungen und Qualitätseigenschaften entsprechen soll. Der SVMP verweist zu diesem Zweck auf eine Reihe von erarbeiteten Checklisten und Dokumenten. Der SVMP basiert weitgehend auf den Vorgaben von GAMP, da dort die „Best Practices“ für Computersysteme gesammelt vorliegen. Es ist die Politik der TMF die benötigten Validierungsprozesse und Validierungsdokumentation möglichst gemeinsam zu erarbeiten und zu evaluieren. Die Validierungspolitik für die TMF-Verbünde sieht vor, dass der Validierungssupport und die Überprüfung der Validierungspraxis (z.B. in Form von internen Audits) generelle Aufgaben der TMF sind.

2.3 Regeln und Gesetze

Die Notwendigkeit der Validierung von Rechnersystemen in akademischen Zentren, in klinischen Forschungsinstituten oder in Arzneimittel produzierenden Unternehmen ergibt sich aus den entsprechenden gesetzlichen Regularien (z.B. AMG, ICH-GCP, etc.). Im Annex 11 1/99-2 und Annex 15 1/2001 von EU-GMP sind die Grundsätze der Validierung computergestützter Systeme beschrieben. Zusätzlich gilt für die Durchführung elektronischer klinischer Studien: US FDA 21 CFR Part 11: Electronic Records; Electronic Signatures; Final Rule, Federal, März 20, 1997; US FDA 21 CFR Part 11: Draft Guidance for Industry (Feb. 2003). Zusätzlich muss auch das Deutsche Signaturgesetz berücksichtigt werden.

2.4 Validierungsphilosophie

Die Validierung computergestützter Systeme für die Verwendung in klinischen Studien gemäß GCP erfordert die Zusammenarbeit zwischen Anwendern und den Herstellern. Es ist dabei die Philosophie dieses Leitfadens, möglichst viele Aspekte der Systemvalidierung vom Hersteller übernehmen zu lassen. Dabei sollte beim Software-Hersteller ein formelles Qualitätsmanagement implementiert sein, das den Entwicklungsprozess und die Produktion der Software kontrolliert und die Qualität sicherstellt. Der Nutzer sollte verifizieren, dass der Software-Hersteller über adäquaten Sachverstand und ent-

sprechende Ressourcen verfügt, um die Anforderungen des Nutzers und seine Erwartungen zu erfüllen. Diese Verifizierung erfolgt durch eine Herstellerbewertung (Konzept zum Vendor Audit). Obwohl die Verantwortung für die Validierung bei dem Nutzer liegt, hat der Hersteller einen beträchtlichen Anteil am Erfolg der Validierung. Der Leitfaden unterstützt deshalb den Ressourcen schonenden Ansatz, bei dem der Nutzer möglichst viele Validierungsaufgaben (z.B. Installation, IQ, etc.) vom Software-Hersteller durchführen lässt.

Die Systemvalidierung ist Teil des Qualitätsmanagements. Zur Sicherstellung der Validität und Qualität sollten die Forschungsverbünde über ein Qualitätsmanagement verfügen, das die Qualitätssicherung gewährleistet und Verantwortlichkeiten regelt. SOPs sind der zentrale Bestandteil des QM-Systems. In SOPs werden alle Prozesse detailliert beschrieben, die zur Durchführung klinischer Studien benötigt werden. Des Weiteren ist dort z.B. auch geregelt, wie mit internen und externen Audits oder Inspektionen zu verfahren ist und wie die Qualifizierung der Mitarbeiter sichergestellt wird.

Die Durchführung multizentrischer klinischer Studien von zulassungsrelevanten Studien und Investigator Initiated Trials (IIT) unter Berücksichtigung von Good Clinical Practice (GCP) und wissenschaftlichen Kriterien erfordert ein hohes Maß an Qualität. Zunehmend werden im Rahmen der TMF-Forschungsverbünde harmonisierte SOPs entwickelt und eingesetzt. Diese einheitliche Vorgehensweise ist eine gute und wichtige Voraussetzung zur Erlangung einer einheitlichen Validierungsphilosophie. Als Teil des Qualitätsmanagements wird die Validierung zunehmend in die Qualitätsprozesse integriert.

2.5 Systematischer Ansatz

2.5.1 Validierung nach dem Life Cycle-Modell

Der Leitfaden behandelt die Validierung von Computersystemen, die für die Unterstützung von klinischen Studien und klinischer Forschung beispielsweise in den Forschungsverbünden der TMF eingesetzt werden. Es werden überwiegend keine isolierten Applikationen betrieben, sondern Software-Systeme, die aus einer Anzahl von Hardware-Komponenten und Software-Lösungen und weiteren Tools bestehen können. Die Validierung dieser Computersysteme wird als Systemvalidierung bezeichnet. Die Systemvalidierung ist ein integrativer Teil der gesamten Lebensdauer und des Lebenszyklus (Lifecycle) dieser Systeme. Im Leitfaden werden daher alle während des Lifecycle eines Computersystems durchzuführenden Validierungsaktivitäten beschrieben und auf die notwendige Dokumentation der Validierung verwiesen.

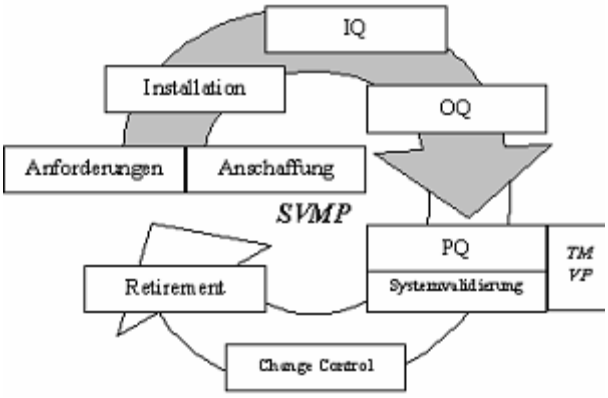

Abb. 4: Vereinfachter Software-Validation Life Cycle (VLC), wie er in diesem Leitfaden (SVMP) beschrieben ist. (Pfeil weiß: Verantwortung des Nutzers, Pfeil grau: Verantwortung des Herstellers), TM: Traceability Matrix, VP: Validierungsplan

Die Validierungsaktivitäten im Rahmen des Lifecycle sind umfassend und reichen von den Anforderungen über die Anschaffung des Systems bis zum Retirement. Der Validierungsmasterplan umfasst deshalb folgende wichtige Aspekte:

- Betrachtungsweise der Validierung nach dem (vereinfachten) V-Modell
- Struktur und Hierarchie der Validierungsdokumente (VMP / VP)
- Qualifizierung nach GAMP gemäß DQ, IQ, OQ, PQ

- Risikoanalyse
- Change Control
- Rolle des Softwareherstellers bei der Validierung
- prospektive, retrospektive, begleitende Validierung
- Revalidierung
- Dokumentenverwaltung
- Projektmanagement
- Retirementplan

Auf Grundlage des SVMP werden für die einzelnen Systeme (z.B. einzelne Studiensoftware) Projekte erarbeitet und die entsprechenden speziellen Validierungspläne abgeleitet und erstellt (**Abb. 5**). Aufbauend auf den Lifecycle werden die Vorgehensweise für die Validierung und die dazu erforderlichen Rahmenbedingungen festgelegt. Dabei kann der Validierungsplan als Projektplan betrachtet werden, der regelmäßig überprüft, erweitert und freigegeben werden sollte. Die im GAMP beschriebene Systematik bei der Computersystemvalidierung ist auf das GCP-Umfeld übertragbar. Somit dient GAMP als Grundlage bei der Planung der Validierungsaktivitäten.

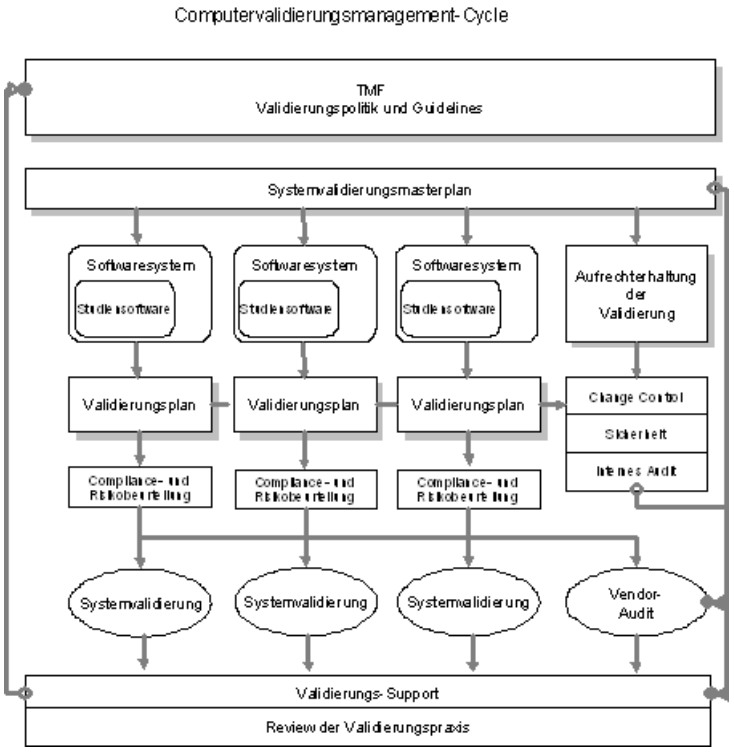

Abb. 5: Schema des systematischen Ansatzes für die Systemvalidierung in den Forschungsverbünden der TMF. Das Beispiel zeigt die Validierung von drei Systemen mit drei Validierungsplänen.

Der Zeit- und Personalaufwand und die damit verbundenen Kosten einer Validierung können erheblich sein und werden durch zahlreiche Faktoren beeinflusst. Durch eingehende und systematische Planung von Validierungsaktivitäten und durch eine gute Organisation der Validierung kann der Aufwand auf ein Minimum beschränkt werden.

- Der Aufwand bei der Validierung kann durch folgendes Vorgehen auf ein gerechtfertigtes Maß beschränkt werden:
- Identifikation qualitätskritischer Größen durch die begleitende Risikoanalyse,
- Formulierung der Anforderungen in einem Lastenheft,
- sinnvolle Einteilung der Validierungsaktivitäten und die entsprechende Verteilung der Verantwortlichkeiten,

- die Wahl der richtigen Methodik für die Qualifizierung und die Nutzung vorhandener technischer Standarddokumente.

Zu den weiteren Maßnahmen für eine kosteneffektive Validierung setzen die Verbünde eine Reihe von Maßnahmen für die Systemvalidierung ein:

- Qualifizierte Plattformen und IT-Infrastrukturen
- Standard-Software und COTS
- Übernahme von Aufgaben durch Software-Hersteller
- Generische Validierungsdokumente
- Risikobasierter Ansatz
- Einsatz von Software-Tools, um Papier zu reduzieren (elektronische Testfälle als z.B. Excel, Word)

2.5.2 Computervalidierung nach GAMP (V-Modell)

Das V-Modell der Computervalidierung nach GAMP ist für die Bedürfnisse einer Validierung nach GCP nicht vollständig übertragbar. Bei der eingesetzten Studiensoftware handelt es sich häufig um "COTS"- Software, die aber zu einem wesentlichen Teil Konfiguration und Anpassung an die Gegebenheiten und an die jeweilige klinische Studie benötigt. Um das V-Modell nach GAMP flexibler zu gestalten, wurden einzelne Phasen aus dem V-Modell zusammengelegt (**Abb. 6**).

Basierend auf der Risikoanalyse folgen im Wesentlichen die Qualifizierungsmaßnahmen gefolgt von der Systemvalidierung, die in einem Validierungsbericht endet. Weitere zentrale Elemente sind die Änderungslenkung (Change Control) und die Revalidierung, die in unmittelbaren Zusammenhang mit der Risikoanalyse stehen.

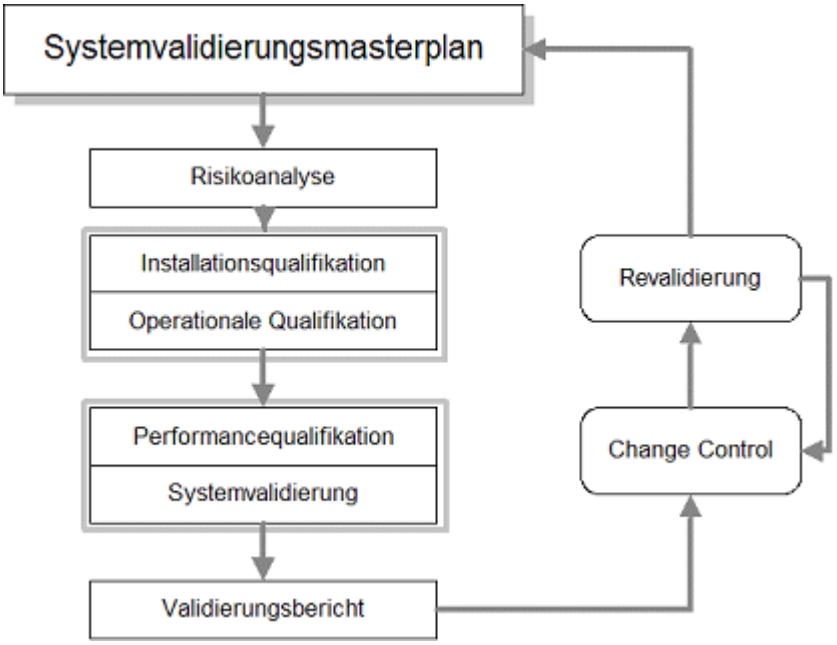

Abb. 6: Vereinfachtes V-Modell

Aus der Ermittlung der Systemkomplexität und GCP-Kritikalität folgt die Vereinigung von Nutzeranforderungen und Funktionale Spezifikation in der Traceability Matrix (= Liste der Nutzeranforderungen). Die Kombination von IQ und OQ zur Systemqualifizierung erfolgt durch den Softwarehersteller und die Kombination von PQ zur Systemvalidierung mit Hilfe einer Teststudie erfolgt durch den Nutzer. Die Traceabilitymatrix stellt dabei das zentrale Dokument der Qualifizierungsmaßnahmen dar. Die Matrix verbindet die Nutzeranforderungen (AS) mit den Ergebnissen der Tests.

Die Kombination von einem risikobasierten Ansatz mit der Übernahme von Validierungsaufgaben durch den Softwarehersteller kann die Kosten für die Validierung erheblich reduzieren.

Abhängig von den GAMP-Kategorien kann die Risikoanalyse in verschiedene Ebenen gemäß den unterschiedlichen Projektphasen der Validierung aufgeteilt werden:

- Identifizierung von GxP-kritischen Funktionen und Modulen
- Design-Spezifikation: Identifizierung GxP-kritischer Kontrollen und Dokumente
- Testphase: unterschiedliche Tiefe der Test, gemäß Risiko und GAMP-Kategorie

3 Rollen und Verantwortlichkeiten

Gemäß GAMP werden verschiedene Rollen definiert, die im Sprachgebrauch der Forschungsverbünde meistens nicht existieren. Für jedes Validierungsprojekt ist es jedoch erforderlich, dass ein Validierungsteam gebildet wird und die Verantwortlichkeiten für das Team festgelegt werden.

Im Rahmen seines Qualitätsmanagement besitzt jeder Verbund eine Dokumentation seiner Arbeitsplätze, Rollen und Verantwortlichkeiten (Funktionslisten, die in SOPs oder Qualitätsmanagement-Handbüchern aufgeführt sind). Für die Systemvalidierung müssen die Verantwortlichkeiten zusätzlich schriftlich festgelegt werden.

Im Folgenden werden nur die Rollen für das Systemvalidierungsteam beschreiben. Für den Betrieb der Infrastruktur bzw. den zugehörigen SOPs müssen ggf. weitere Rollen definiert und beschrieben werden.

Die Festlegung der Rollen und Verantwortlichkeiten erfolgt im Validierungsplan zu dem Projekt oder einer entsprechenden SOP zur Methodik und Rollenverteilung bei der Qualitätssicherung.

3.1 Validierungsteam

Die Rollen und Verantwortlichkeiten können von dem in diesem vorgeschlagenen Systemvalidierungsmasterplan abweichen.

3.1.1 Prozessinhaber

Der Prozessinhaber ist in der Regel durch die Geschäftsführung des Verbundes abgedeckt.

Anforderungsprofil:

- ist vertraut mit den GCP Anforderungen für seinen Bereich

Aufgaben:

- ist verantwortlich für die Ergebnisse, die mit dem IT-System erzeugt werden
- benennt die Projektmitglieder aus seinem Bereich
- ist verantwortlich für die Durchführung der Risikoanalyse
- genehmigt bei neuen Systemen den QS- und Projektplan
- löst bei bestehenden Systemen die retrospektive Validierung aus
- löst die Revalidierung des IT-Systems aus

- beschafft die personellen und finanziellen Ressourcen
- gibt das IT-System frei
- hat Veto-Recht bezüglich Funktionalität und Qualität von IT-Systemen für GxP-relevante Anwendungen in seinem Arbeitsbereich
- ist verantwortlich für die VLC-Dokumentation des Systems nach Einführung

3.1.2 Qualitätsmanagement

Diese Funktion ist prinzipiell durch den Qualitätsbeauftragten des Verbundes gewährleistet. Einzelne Aufgaben (vor allem IT-spezifische) können auch zu anderen Rollen übertragen werden, wenn dies erforderlich ist. Die Zuordnung ist im entsprechenden Validierungsplan/SOP festzuhalten. Das QM berichtet an den Projektinhaber.

Anforderungsprofil:

- beherrscht die einschlägigen IT-QS-Richtlinien und die IT-QS-SOPs (Ausnahmen: IT-technische SOPs)
- versteht den Einsatz von IT-Systemen
- beherrscht die internen IT-QS-SOPs
- kann mit Beratung die SOPs weiterentwickeln

Aufgaben:

- stellt die Validierungs-Relevanz eines Systems fest
- hält die SOPs inhaltlich auf dem neuesten Stand
- pflegt den IT-Validation-Masterplan (IT-VMP)
- veranlasst Projektaudits
- initiiert die Durchführung der Risikoanalyse
- besitzt alle relevanten und gültigen behördlichen Verordnungen über die Entwicklung und Einsatz von IT-Systemen im GxP-Umfeld
- legt die Dokumente des VLC und die anzuwendenden SOPs in IT-Projekten fest
- verteilt die gültigen SOPs an den Projektleiter und die Mitglieder des Projektteams und zieht sie nach Projektende wieder ein
- initiiert ggf. die Erarbeitung projektspezifischer SOPs
- setzt die Prioritäten für die Validierung der IT-Systeme auf Grund des IT-Masterplans und der Risikoanalysen
- verfolgt den Stand der Technik auf dem Gebiet der IT-Qualitätssicherung (Fortbildung)
- pflegt Kontakte zu Behörden und anderen Firmen
- führt Schulungen der SOPs durch
- berät die Projektteams

3.1.3 Projektmanager/Projektleiter

Der Projektleiter wird in jedem Projekt neu bestimmt vom Prozessinhaber, er berichtet an den Prozessinhaber.

Anforderungsprofil:

- versteht das einzuführende bzw. zu entwickelnde IT-System/Systemteil von der IT- und der Anwenderseite
- beherrscht die internen IT-QS-SOPs
- kann mit Beratung die Risiken des Einsatzes eines IT-Systems im GxP-Umfeld abschätzen
- kann ein IT-Projekt hinsichtlich Terminen und Kosten überwachen

Aufgaben:

- plant die Entwicklung/Beschaffung

- genehmigt die Feinspezifikation/das Pflichtenheft
- führt und entscheidet die System- und Lieferantenauswahl gem. den gültigen IT-QS-SOPs und Richtlinien
- ist verantwortlich für die Erstellung und Pflege des Projektplans und die termin- und fachgerechte Durchführung des Projektes bis zur Ersteinführung
- ermittelt den Ressourcenbedarf für die Projektdurchführung einschließlich der QS-Maßnahmen und sorgt für die notwendigen Ressourcen (personell, finanziell)
- verwaltet die VLC-Dokumente bis zur Ersteinführung

3.1.4 Projektteam

Das Projektteam wird aus Mitarbeitern der Anwenderseite (z.B. Key-User) und/oder IT-Fachleuten (interne und eventuell externe) gebildet. Die Aufgaben des Projektteams können auch vom Projektleiter erfüllt werden. Das Projektteam berichtet an den Projektleiter.

Anforderungsprofil:

- ist in der Lage, das IT-System (ggf. unter Anleitung) zu konfigurieren/parametrisieren, zu modifizieren oder zu entwickeln
- beherrscht die IT-QS-SOPs

Aufgaben:

- führt das Projekt zur Systemeinführung bzw. Systementwicklung entsprechend dem QS- und Projektplan und den IT-QS-SOPs durch

3.1.5 Systeminhaber / IT-Administration / Systemtechniker

Der zuständige Administrator wird vom Prozessinhaber für das Projekt bestimmt, er berichtet an den Projektleiter/Prozessinhaber.

Anforderungsprofil:

- beherrscht den Betrieb der Infrastruktur (Hardware/Netze und systemnahe Software) gemäß den dazu gültigen SOPs
- beherrscht Entwicklung, Änderung und Betrieb einer Applikation gemäß den dazu gültigen SOPs

Aufgaben:

- führt alle Arbeiten durch, die zur Aufrechterhaltung des Systembetriebes erforderlich sind
- Entwickelt, ändert, betreibt und installiert eine Applikation
- unterstützt die Anwender bei der Bedienung des Systems und führt ggf. Schulungen durch

3.1.6 Fachexperten / Nutzer des Systems

Geschulte Personen, die die Softwarelösung nutzen. Die Nutzer haben die Möglichkeit, in den Prozess der Change Control einzugreifen, indem sie berechtigt sind, Änderungsmeldungen an das Projektteam oder die Projektleitung zu melden.

3.2 Organisationsstrukturen in den Verbünden – externe Rollen

Computergestützte Systeme sind von großer Bedeutung für die Prozesse der Verbünde. Innerhalb der TMF gibt es verschiedene Organisationsstrukturen und somit auch Planungsebenen, die Auswirkung auf die Benutzung computergestützter Systeme haben. Besonderes Merkmal der Kompetenznetze sind Studiengruppen.

Diese Studiengruppen sind z.T. relativ unabhängig bezüglich der Nutzung von Studiensoftware, da sie eine eigene Studiensoftware betreiben. Diese unterschiedlichen Strukturen sollten bei der Planung der Validierung berücksichtigt werden.

Ferner zu berücksichtigen ist, dass einige Verbünde Services wie z.B. Hosting und ASP anbieten. Durch die verschiedenen Nutzungskonzepte müssen externe Rollen berücksichtigt werden. Die Definition dieser Rollen muss ebenfalls in der Validierungsdokumentation schriftlich festgelegt sein.

Insbesondere die KN sind hochgradig vernetzte Organisationen. Einige haben externe Dienstleistungen in ihre Prozesse integriert.

3.2.1 Softwarehersteller (-provider, -vendor)

Der Softwarehersteller sollte neben dem Support auch den Validierungsprozess unterstützen. Dieses bezieht sich in erster Linie auf die Qualifizierung des Systems (IQ und OQ) sowie Unterstützung beim Vendor-Audit.

3.2.2 Application Service Provider (ASP)

Stellt ein Forschungsverbund für andere FV ein System via ASP zur Verfügung, so ist überwiegend der FV, der den Service anbietet, für die Systemvalidierung verantwortlich.

3.3 Responsibility-Split

Durch die Einführung eines „Responsibility-Split“ kann auch in FV mit geringen personellen Ressourcen gewährleistet werden, dass ein Validierungsteam gebildet werden kann. Dieser soll dazu dienen, dass Personen verschiedene Rollen und Verantwortlichkeiten (Validierungsaufgaben) zugewiesen werden können. Diese müssen schriftlich zu den einzelnen Validierungsprojekten festgelegt sein.

In jedem Fall muss vermieden werden, das einzelne Rollen bzw. Verantwortlichkeiten sich überschneiden und zu einer Vermischung der Interessen und Anforderungen führen (z.B. kann der Systemadministrator als Prozessinhaber kann sich nicht selber Anweisungen erteilen).

4 Validierungsprozedur

4.1 Validierungsprozesse: systematischer Ansatz

Software, die in klinischen Studien eingesetzt wird, unterliegt Richtlinien, die eine umfassende und detaillierte Validierung des gesamten Systems notwendig machen. Des Weiteren ist ein validiertes Computersystem die Grundlage für ein effizientes und fehlerfreies Arbeiten. Eine generelle Stellungnahme zur Computer System Validierung ist als Anhang zum SVMP verfügbar.

Die Validierung besteht aus unterschiedlichen Schritten und steht in Beziehung zum System Life Cycle. Jeder Schritt ist mit gewissen Tätigkeiten der Anwender verbunden. Die Etablierung validierter automatisierter Systeme in der klinischen Forschung erfordert die Zusammenarbeit von Anwendern und Softwareherstellern. Es ist deshalb von Vorteil, wenn der Softwarehersteller ein formelles Managementsystem für die Kontrolle und die Dokumentation der Entwicklungsprozesse einsetzt. Obwohl die Verantwortung für die Validierung des Systems beim Anwender liegt, sollte der Softwarehersteller erheblich in den Vorgang mit eingebunden werden. Jede einzelne Phase der Validierung steht in Beziehung zu ihren notwendigen Validierungstätigkeiten und der entsprechenden Dokumentation und Berichterstellung.

Im Validierungsplan werden die Anwendertätigkeiten genau vorgeschrieben. Die ordnungsgemäße Durchführung der Validierung erzeugt daher eine Reihe von Berichten, die als Nachweis für die Validität des Systems dienen. Der SVMP soll zur Überschaubarkeit der Validierungsaktivitäten für Management, Validierungsteam und Qualitätssicherung beitragen und der inspizierenden Seite den Validierungsansatz veranschaulichen.

Die Validierungsphasen sind Teil der Etablierung von IT-Lösungen, die durch den Validierungs-Life Cycle eines Systems beschrieben werden. Dessen einzelne Schritte bestehen aus:

1. Systemspezifizierung (Spezifizierung und Auswahl)
2. Systemklassifikation
3. Validierungsplanung
4. Etablierung des validen Zustandes (IQ, OQ, PQ)
5. Aufrechterhaltung des validen Zustandes (Change Control)
6. System Retirement

4.2 Systemqualifizierung nach dem V-Modell

Noch vor der Installation wird von dem Anwender zusammen mit dem Softwarehersteller ein Plan zur Implementierung aufgestellt. Die Installation wird weitgehend durch den Softwarehersteller gemäß dem Plan durchgeführt. Mit der Installation beginnt auch die Qualifizierung des installierten Systems, also die Testung des Systems.

In der Literatur werden verschiedene Qualifizierungsphasen beschrieben, nämlich die Design- Installations- und Funktionsqualifizierung. In Veröffentlichungen der Behörden (insbesondere FDA) werden diese Qualifizierungsbegriffe definiert. Sie lassen sich auf computergestützte Systeme folgendermaßen übertragen (s. Kap. 8):

DQ: Design Qualification / Design Qualifizierung
Unter DQ wird der dokumentierte Nachweis verstanden, dass ein computergestütztes System in Übereinstimmung mit den GxP-Anforderungen geplant wurde.

IQ: Installation Qualification / Installationsqualifizierung (IQ)
Unter IQ wird der dokumentierte Nachweis verstanden, dass das computerisierte System entsprechend seines konzeptionellen Systementwurfs (DQ) entwickelt und installiert wurde.

OQ: Operational Qualification / Operationale Qualifizierung oder Funktionsprüfung
Unter OQ wird der dokumentierte Nachweis verstanden, dass das computerisierte System, insbesondere seine aus GxP-Sicht kritischen Funktionen, funktioniert, d. h. das tut, was es laut Spezifikation tun soll.

PQ: Performance Qualification / Performance Qualifizierung oder Leistungsprüfung
Unter PQ wird der dokumentierte Nachweis verstanden, dass ein computergestütztes System auch unter Belastung im Echtbetrieb das tut, was es laut Spezifikation tun soll.

4.2.1 Prospektive Validierung und Retrospektive Validierung

Grundsätzlich sollte eine prospektive Validierung der Systeme durchgeführt werden. In einigen Fällen ist dies jedoch nicht möglich, da bereits Softwarelösungen im Einsatz sind, die ohne eine vollständige Systemvalidierung im Routinebetrieb eingesetzt werden. Diese müssen entsprechend nachträglich (retrospektiv) validiert werden. Grundsätzlich sollte eine retrospektive Validierung nur in Ausnahmefällen durchgeführt werden.

Eine prospektive Validierung wird für Systeme angewandt, die neu entwickelt und eingeführt werden bzw. für Systeme, an denen Änderungen vorgenommen werden. Entsprechend des EU-GMP-Leitfadens sollte das computergestützte System nach den Grundsätzen eines Phasenmodells (auch Lebenszyklusmodell genannt) entwickelt und in Betrieb genommen werden. Dabei sind die Validierungsaktivitäten Bestandteil einer jeden Phase und sie müssen in einer Validierungsdokumentation festgehalten werden.

Eine retrospektive Validierung sollte für Systeme angewandt werden, die bereits in Betrieb waren bzw. nicht nach dem Phasenmodell entwickelt wurden. Die retrospektive Validierung kann daher auch als nachträgliche Validierung angesehen werden. Grundsätzlich muss auch bei dieser Form der Validierung nachgewiesen werden, dass das System gemäß den GxP-Regeln das tut und tun wird, was man laut seiner Spezifikation von ihm erwartet. Zusätzlich muss aber der dokumentierte Beweis erbracht werden, dass das System auch in der Vergangenheit ordnungsgemäß funktioniert hat. Ist dieser Nachweis mangels Dokumenten nicht möglich, müssen diese Nachweise evtl. mit dem Lieferanten erbracht werden. Die nachträgliche Festlegung der Anforderungen, die Durchführung von funktionalen Tests, und Dokumentation des Einsatzes werden analog zur prospektiven Validierung geplant durchgeführt.

4.3 Systemspezifikation und Systemauswahl

4.3.1 Spezifikation

Die Qualifizierungsdokumente sind nur dann ausreichend, wenn sie die vollständige Spezifizierung des Systems umfassen. Die Erstellung und Pflege einer aktuellen Systemspezifikation ist eine GCP-Schlüsselanforderung. Jeder Ebene der Spezifikation ist eine äquivalente Ebene der Testspezifikation zugeordnet, die die Erfüllung der Anforderungen überprüft (V-Modell). Die Dokumentation der Spezifikation basiert im Allgemeinen auf dem Lasten- und Pflichtenheft.

Anforderungsspezifikation (AS)

Die Anforderungsspezifikation (User Requirement Specifications) beschreibt, was das System leisten soll. Es wird vom Anwender erstellt. Es enthält alle Muss-Anforderungen, kann aber auch Wunsch-Anforderungen enthalten. Es kann an Lieferanten als Teil der Lieferantenauswahl verschickt werden.

Funktionsspezifikation (FS)

Das Funktionsspezifikation (Functional Specification) wird normalerweise vom Lieferanten erstellt und beschreibt die Funktionen des Systems im Detail. Die erste Fassung kann als Antwort auf die Projektausschreibung erfolgen, die weiteren Versionen werden generell in Zusammenarbeit mit dem Anwender erstellt. Das Pflichtenheft ist verknüpft mit der DQ.

Entwurfsspezifikationen (Hardware und Software)

Die Entwurfspezifikationen (Design Specifications) beschreiben, wie und womit das System aufgebaut ist. Die Entwurfspezifikationen sind sowohl verknüpft mit der IQ, die überprüft, ob das richtige System geliefert und korrekt installiert worden ist, als auch mit der OQ, die überprüft, ob das System gemäß der Spezifikation arbeitet.

4.3.2 Systemauswahl und Systemanschaffung

Basierend auf den Vorschlägen des SVMP legt jeder Verbund eine Strategie für die Anschaffung und Validierung seiner Computersysteme fest. Typischerweise werden dazu Lasten- und Pflichtenheft erstellt.

Für die Bestimmung der Nutzeranforderungen und die Auswahlmethode wird ein methodisches Vorgehen gewählt. Es können Umfragen, Checklisten und eine Punktebewertungen eingesetzt werden, um die Anforderungen umfassend zu ermitteln und Priorität quantitativ zu bestimmen. Als hilfreiche Instrumente können standardisierte Interviews und ein Bewertungssystem eingesetzt werden. Die Fragen sollten sowohl technische als auch personenbezogene Ressourcen und Anforderungen berücksichtigen. Auf Basis der gewonnenen Erkenntnisse wird ein Anforderungskatalog entwickelt, der als Basis der Anforderungsspezifikationen dient.

4.4 Validierungsstrategie

4.4.1 Risikobewertung

Die Tiefe und das Ausmaß der Systemvalidierung basiert auf einer Risikoabschätzung. Die Risikobewertung dient dazu, folgende Fragen zu beantworten:

- Muss das computerisierte System validiert werden
- Wie viel Validierung benötigt das System
- Welche Aspekte des Systems sind GCP-kritisch (Patientensicherheit, Geschäftsprozesse, etc.)

Die Beantwortung dieser Fragen erlaubt, die Validierung auf kritische Bereiche zu fokussieren und Strategien zur Risikominderung einzusetzen. Aus diesem Grund wird der gesamte Validierungsprozess von einer Risikoabschätzung begleitet.

4.4.2 Bewertung der Systemkomponenten

Als weiterer Schritt werden die Software- und Hardwarekategorien von GAMP verwendet. Die dienen als Hilfe, die unter Berücksichtigung der Systemkonstruktion und Konfiguration benötigten grundsätzlichen Validierungstätigkeiten festzulegen. Die Kategorien basieren auf dem Impact, den ein Auftreten von Systemfehlern hat. Computerisierte Systeme bestehen häufig aus vielfältigen Komponenten, die innerhalb eines einzigen Systems integriert sind, aber in verschiedene Kategorien eingeordnet werden können. Details der Kategorisierung und des entsprechenden Validierungsaufwandes behandelt Kap. 7.3.1 Kategorisierung der Systemkomponenten.

Folgende Softwarekategorien sind generell vorhanden:

- Kategorie 1: Betriebssysteme

- Kategorie 3: Standard-Softwarepakete
- Kategorie 4: Konfigurierbare Softwarepakete
- Kategorie 5: Anwender spezifische Software

Folgende Hardwarekategorien sind generell vorhanden:

- Hardwarekategorie 1: Standard-Hardwarekomponenten
- Hardwarekategorie 2: Anwender spezifische Hardwarekomponenten

Für die meisten Softwaresysteme im Bereich klinischer Forschung kommt nur Kategorie 3 und Kategorie 4 in Betracht. Also kommerziell verfügbare Standard-Softwarepakete, die eine Standardlösung für einen Geschäftsprozess bereitstellen. Außerdem spielen konfigurierbare Standard-Softwarepakete eine große Rolle. Bei den Hardwarekategorien spielen in der Regel nur Standard-komponenten eine Rolle.

4.4.3 Elektronische Dokumentation und Signatur

Klinische Studien werden zunehmend „papierlos“ durchgeführt. Die dazu eingesetzten Systeme erzeugen elektronische Dokumente und setzen digitale Signaturen ein. Für die Validierung der elektronischen Dokumentation dienen die Regularien 21 CFR Part 11 der FDA und Annex 11 der EU. Ein wesentlicher Aspekt der Validierung der elektronischen Dokumentation gemäß diesen Regularien ist der Nachweis eines kompletten Audit Trails (**Abb. 8**).

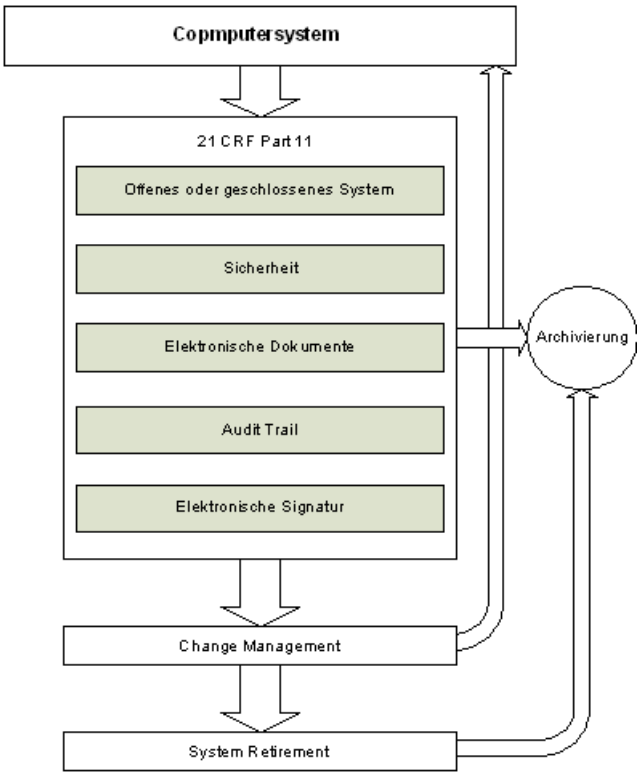

Abb. 7: Systemvalidierung nach 21 CRF Part 11 Validierung von elektronischen Dokumenten und elektronischen Signaturen. Die Verwendung elektronischer Dokumente hat Auswirkungen auf Change Control und Archivierung.

4.4.4 Validierungspläne

Die einzelnen Validierungspläne (s. Kap. 7) beschreiben die Validierungsaktivitäten für jedes individuelle System. Im Validierungsplan wird eine Liste mit Akzeptanzkriterien für eine erfolgreiche Validierung erstellt.

Validierungsbericht

Der Validierungsplan endet mit einem Validierungsbericht, der das Ergebnis der Validierung beschreibt und diskutiert, ob die Akzeptanzkriterien erfüllt wurden. Er definiert, ob ein System freigegeben werden kann.

Freigabe eines Systems

Die Freigabe eines Systems bedeutet, dass das System validiert ist. Dazu sind Unterschriften mindestens des Prozessinhabers und des Qualitätsmanagements notwendig

4.4.5 Validierung von Open Source-Systemen

Die Validierung von Open Source-Software stellt besondere Anforderungen an die Validierung, da in der Regel ein Qualitätsmanagementsystem beim Hersteller nicht vorhanden ist und ein Vendor Audit nicht durchgeführt werden kann. Anstelle eines Vendor Audits kann stellvertretend eine Referenz-installation der Open Source-Software validiert werden. Zur Validierung von Open Source-Systemen wird ein besonderer Validierungsplan erstellt.

4.5 Aufrechterhaltung des validen Zustandes

4.5.1 Systembetrieb

Jeder Verbund besitzt SOPs für den Systembetrieb. Alle SOPs, die für den ordnungsgemäßen Systembetrieb nötig sind, werden vor der Freigabe des Systems erstellt und genehmigt. Besondere SOPs regeln zusätzlich die Validierung (s. Kap. 7.5 Standard Operating Procedures)

4.5.2 Schulung

Die Schulung der Nutzer des Systems ist ein wesentlicher Aspekt der Validierung. Das Ausmaß und der Zeitpunkt der Schulung muss kontinuierlich dokumentiert werden (s. Kap. 7.5). Die Teilnahme an Schulungen ist grundsätzlich zu dokumentieren. Schulungen sollten grundsätzlich vor der produktiven Inbetriebnahme der Applikation erfolgen. Bescheinigungen für die erfolgreiche Teilnahme an der Schulung sollten erstellt und zentral abgelegt werden. Für die Schulung muss eine SOP vorhanden sein.

4.5.3 Begleitende Validierung (Change Control)

Wenn ein System den validen Zustand erreicht hat, sind Maßnahmen festzulegen, damit das System auch für die Zeit seines Einsatzes valide bleibt. Werden Fehler festgestellt, müssen diese mit einem Fehlerprotokoll an den entsprechenden Verantwortlichen gemeldet werden. Durch eine funktionierende Änderungslenkung (Change Control) werden Änderungen der Software systematisch erfasst und über die Notwendigkeit einer begleitenden Validierung entschieden. Das Verfahren für Change Control und die Verantwortlichkeit muss in einer SOP festgelegt sein. Details für die Änderungslenkung sind in Kap. 7.6.1 beschrieben.

Bei Anpassungen und Änderungen der Konfiguration am System sollten diese nicht am produktiven System, sondern zuerst an einem Testsystem oder Prüfsystem vorgenommen werde. Auch die Einrichtung und die Änderungen am Testsystem sollten dokumentiert werden. Diese Vorgehensweise hat den Vorteil, dass das Prüfsystem in einem Katastrophenfall das produktive System eventuell ohne Unterbrechung ersetzen kann. Mit jeder wesentlichen Änderung des Systems oder der Installation einer neuen Komponente oder eines Upgrades muss eine IQ durchgeführt und dokumentiert werden. Die Dokumente für diese IQ werden häufig, wie im Falle von Upgrades, zusammen mit dem Update vom Softwarehersteller geliefert. Die vom Softwarehersteller zur Verfügung gestellte Qualifizierungsdokumentation bei größeren Änderungen am System sollte IQ- und in großen Teilen auch OQ-Dokumentation beinhalten.

4.5.4 Revalidierung und internes Review

Die Notwendigkeit für erneute Validierung des Systems (Revalidierung) kann sich nach größeren Änderungen an der Hard- und Software eines Computersystems ergeben. Es muss festgelegt werden, unter welchen Bedingungen ein valides System nicht mehr valide ist oder zu welchen Zeitpunkten ein

valides System revalidiert werden muss (s. Kap. 7.7 Revalidierung). Wenn ein System einmal vollständig validiert worden ist und in der Folgezeit ohne Änderungen eingesetzt wird, muss trotzdem periodisch eine interne Überprüfung (Review) durchgeführt werden. Zeitpunkt und Umfang für das interne Review sollten festgelegt werden. Es empfiehlt sich eine jährliche Systemüberprüfung durchzuführen, um über die Notwendigkeit zu entscheiden, welche (Re-)Validierungsmaßnahmen notwendig sind. Eine Revalidierung kann eine geringere Testtiefe als die Erstvalidierung aufweisen.

4.5.5 Service Level Agreements (SLA)

Dienstleistungen zwischen einem Softwarehersteller und einem Verbund, wobei auch ein Verbund als Softwarehersteller auftreten kann, werden durch SLA-Verträge geregelt. Hierbei werden die Dienstleistungen im Detail geregelt. Ein Muster-SLA-Vertrag für Verträge zwischen zwei Verbünden ist auf Anfrage bei der TMF erhältlich.

4.5.6 Datensicherheit

Annex 11 und 21CRF Part 11 definieren detaillierte Anforderungen an Zugriffsschutz (z.B. Konzepte für Nutzerberechtigungen) und Datensicherheit. Es gibt Zugriffsschutzkonzepte und Datenschutzkonzepte, u.a. Backup / Recovery) für komplexe Studiensysteme der Verbünde. Da die Sicherheit eines gesamten Netwerkes gewährleistet werden muss, basiert die Sicherheitsinfrastruktur auf einer eigenen Sicherheitspolitik und einer Reihe von Sicherheits-SOPs

4.5.7 Archivierung

Die Archivierung aufbewahrungspflichtiger Dokumente erfolgt zunehmend elektronisch. Hierbei muss die Lesbarkeit der Dokumente und Wiederherstellbarkeit der Daten geprüft werden.

4.5.8 Kontinuitätsplanung

Für den Fall eines Systemausfalls werden alternative Verfahren und redundante Systeme definiert, um eine einwandfreie Fortführung der Studienprozesse zu gewährleisten. Der Kontinuitätsplan ist Teil der Sicherheitsinfrastruktur.

4.6 Systembeendigung (Außerbetriebnahme)

Der Nutzer der Software sollte einen Plan für das Retirement der Software haben, also einen Plan für den Ersatz des Computersystems und für die Migration der Daten. Einzelheiten sind im Kap. 7.9 beschrieben.

5 Systemklassifikation

Zur korrekten Fokussierung der Validierungsaktivitäten muss in einem Verbund zu jedem Zeitpunkt bekannt sein, welche Computersysteme validierungspflichtig sind und welche nicht. Validierungspflichtig sind grundsätzlich alle GCP-relevanten Computersysteme, d.h. Computersysteme, die einen direkten oder indirekten Einfluss auf GCP-Daten haben. GCP-Daten sind alle Daten, die dazu dienen, die Sicherheit, Wirksamkeit und Qualität eines medizinischen Produktes oder einer klinischen Therapie nachzuweisen.

Währen der Systemklassifikation wird die die jeweilige GAMP Kategorie ermittelt und festgelegt inwieweit das Computersystem GCP-kritisch ist. Gegebenenfalls kann man die Systemklassifikation auch um eine Schutzbedarfsanalyse nach IT-Grundschutz ergänzen.

Die Systemklassifiaktion muss im Laufe des Projektes ständig aktualisiert und ergänzt werden (Änderungsmanagament).

➔ Muster 1-xxx Systemklassifikation

6 Systemspezifikation

6.1 Erstellung der Spezifikationsdokumente

6.1.1 Spezifikation der Benutzeranforderungen

Grundlage der Validierung eines Computersystems sind die Benutzeranforderungen an das System. Eine detaillierte Spezifikation der Benutzeranforderungen ist die elementare Voraussetzung, um die Validität eines Systems nachweisen zu können. Die Definition der Benutzeranforderungen ist der erste Schritt bei der Entwicklung eines neuen Systems und erfolgt durch das Projektteam in Zusammenarbeit mit den zukünftigen Anwendern.

Die *SOP 1-040 Anforderungsspezifikation* beschreibt die Vorgehensweise im Detail. Die Benutzeranforderungen werden in der ersten Spalte der Traceability-Matrix referenziert.

- ➔ SOP 1-040 Anforderungsspezifikaion
- ➔ SOP 1-021 Traceabilitymatrix
- ➔ Muster 1-020 Traceabilitymatrix

6.1.2 Funktionale Spezifikation

Die funktionale Spezifikation beschreibt wie die Benutzeranforderungen funktional realisiert werden. Gegenüber der Spezifikation der Benutzeranforderungen, bei der das WAS im Vordergrund steht, geht es bei der funktionalen Spezifikation primär um das WIE. Die *SOP 1-050 Funktionsspezifikation* enthält die detaillierte Vorgehensweise zur Erstellung einer funktionalen Spezifikation. Die funktionale Spezifikation erfolgt nach der Spezifikation der Benutzeranforderungen durch das Projektteam. Die funktionalen Spezifikationen werden in der Traceability-Matrix referenziert und zu den entsprechenden Benutzeranforderungen in Beziehung gesetzt.

- ➔ SOP 1-050 Funktionsspezifikaion
- ➔ SOP 1-021 Traceabilitymatrix
- ➔ Muster 1-020 Traceabilitymatrix

6.1.3 Software Design Spezifikation

Die Software Design Spezifikation definiert, mit welchen Softwarekomponenten die funktionale Spezifikation realisiert werden soll. Die einzelnen Komponenten werden hinsichtlich ihrer Funktionalität, ihres modularen Aufbaus, ihrer zugrunde liegenden Datenstrukturen und ihrer Interaktionen detailliert beschrieben. Die Software Design Spezifikation erfolgt durch das Projektteam im Anschluss an die Erstellung der funktionalen Spezifikation.

➔ Anlage 1-042 Softwaredesign Spezifikation

6.1.4 Hardware Design Spezifikation

Die Hardware Design Spezifikation definiert, mit welchen Hardwarekomponenten die funktionale Spezifikation realisiert werden soll. Die einzelnen Komponenten und ihre Interaktion werden detailliert beschrieben. Die Hardware Design Spezifikation wird im Anschluss an die Software Design Spezifikation durch das Projektteam erstellt.

➔ Anlage 1-041 Hardwaredesign Spezifikation

6.2 Auswahl der Systemkomponenten

Konkrete Produkte für die in der Software und Hardware Design Spezifikation vorgesehenen Komponenten sollten systematisch ausgewählt werden. Hierbei ist nach folgendem allgemein anerkanntem Verfahren vorzugehen:

1. Anforderungsspezifikation erstellen
2. Funktionsspezifikation erstellen
3. Ausschreibung (offen/beschränkt) oder Marktanalyse
4. Angebotsvergleich (Systembewertung)
5. Definition einer engeren Auswahl
6. Produktpräsentationen/Referenzinstallationen
7. Produktentscheidung

Wichtig ist, dass der gesamte Prozess transparent und für Dritte verständlich dokumentiert wird. Für den Angebotsvergleich sind die Einzelsysteme auf der Basis klar definierter Kriterien und einem Punktesystem systematisch zu bewerten. Die Produktentscheidung muss letztendlich für jedermann nachvollziehbar sein.

7 Validierungsplan

Voraussetzung für die systematische Validierung eines Computersystems ist die Erstellung eines Validierungsplanes. Er umfasst neben einer Systembeschreibung alle Maßnahmen zur Herstellung und zur Erhaltung des validen Systemzustandes. Der Validierungsplan ist als Projektplan zu verstehen, der den gesamten Lebenszyklus eines Systems abdeckt.

7.1 Gliederung

Nachfolgend ist eine exemplarische Gliederung eines Validierungsplanes dargestellt. Die Inhalte werden in den folgenden Abschnitten ausführlich erläutert.

1. Einleitung und Geltungsbereich
   1.1. Beschreibung der Geschäftsprozesse
   1.2. Beschreibung des Systems
   1.3. Risikobewertung für das Gesamtsystem
   1.4. Annahmen, Ausschlüsse und Einschränkungen
   1.5. Rollen und Verantwortlichkeiten
2. Herstellung des validen Systemzustandes
   2.1. Kategorisierung der Systemkomponenten
   2.2. Risikobewertung auf Komponentenebene
   2.3. Qualifizierungsmaßnahmen
3. Validierungsdokumentation
4. Standard Operating Procedures
5. Erhaltung des validen Systemzustandes
6. Revalidierung
7. Schulung
8. Außerbetriebnahme
9. Projektmanagement

7.2 Einleitung und Geltungsbereich

Die Einleitung des Validierungsplanes sollte folgende Informationen enthalten:

- Autor(en), Revision, Dokumentfreigabe
- Bezug zum Validierungsmasterplan (VMP) und relevanten Policies
- Beschreibung des übergeordneten Geschäftsprozesses

- Beschreibung des zu validierenden Systems (inkl. klarer Systemabgrenzung)
- Ergebnis u. Begründung der Risikobewertung für das Gesamtsystem
- Grundsätzliche Annahmen, Ausschlüsse und Einschränkungen bzgl. des Gesamtsystems
- Rollen u. Verantwortlichkeiten (Projektmanagement, QA, Systembesitzer, etc.)

7.3 Herstellung des validen Systemzustandes

7.3.1 Kategorisierung der Systemkomponenten

Zur Ermittlung eines adäquaten Validierungsansatzes dient die Kategorisierung der einzelnen Systemkomponenten entsprechend des unten dargestellten Schemas. Grundsätzlich gilt, dass für alle Standard-Hardwarekomponenten und für Betriebsystemkomponenten die Durchführung einer Installations Qualifizierung (IQ) ausreicht. Im Bereich der Anwendungssoftware muss jedoch weiter differenziert werden. So ist hier zu unterscheiden zwischen Standard-Softwarepaketen, konfigurierbaren Softwarepaketen und anwenderspezifischer Software.

Standard-Softwarepakete bieten eine „Off-the-shelf"-Lösung für bestimmte Geschäftsprozesse. Die Konfigurationsmöglichkeiten beschränken sich hier im Wesentlichen darauf, das System in seine technische Umgebung zu integrieren. Die Kategorie der Standard-Softwarepakete ist weiter zu differenzieren in allgemeine Standardsoftware und spezielle Standardsoftware. Unter die Kategorie allgemeine Standardsoftware fallen z.B. Datenbankmangementsysteme oder Textverarbeitungs-systeme. Bei spezieller Standardsoftware handelt es sich um Branchensoftware, wie z.B. Datenmanagementsysteme für klinische Studien. Die Validierungsansätze der beiden Softwareklassen unterscheiden sich in der Notwendigkeit einer Herstellerbewertung im Falle spezieller Standardsoftware.

Bei konfigurierbaren Softwarepaketen umfassen die Konfigurationsmöglichkeiten nicht nur die Integration des Systems in seine technische Umgebung, sondern gehen weit darüber hinaus. So können diese Systeme sehr genau an die einrichtungsspezifischen Geschäftsprozesse angepasst werden. Die Konfigurationsmöglichkeiten reichen von der Deaktivierung nicht benötigter Funktionen über die Änderung benötigter Funktionen bis hin zur Programmierung zusätzlicher Module. Der Validierungsansatz umfasst neben einer Herstellerbewertung insbesondere die Sicherstellung der Erfüllung der Benutzeranforderungen unter besonderer Berücksichtigung des konfigurierten Geschäftsprozesses. Zusätzlich entwickelte bzw. stark veränderte Module fallen unter die Kategorie 5 und erfordern damit den maximalen Validierungsaufwand. Auch die Wartung konfigurierbarer Softwarepakete erfordert besondere Sorgfalt, da z.B. bei der Einführung neuer Versionen durch den Hersteller durch die Abhängigkeit benutzerdefinierter Funktionen von geänderten Standardfunktionen schwerwiegende Probleme auftreten können.

Bei anwenderspezifischer Software handelt es sich um Software, die speziell für eine bestimmte Einrichtung neu entwickelt wurde. Hierbei kann es sich um komplette Systeme oder Systemerweiterungen handeln. Der Validierungsansatz muss den gesamten Systemlebenszyklus abdecken. Bei fremdentwickelter Software ist über ein Herstelleraudit die qualitätsgesicherte Entwicklung sicherzustellen. Bei einer Eigenentwicklung ist es erforderlich, die entsprechenden Maßnahmen im eigenen Hause zu etablieren. Risikobewertung auf Komponentenebene

Zur Ermittlung der notwendigen OQ-Testtiefe muss für jede Anwendungssoftware-Komponente eine Risikobewertung erfolgen. Hierzu ist entsprechend der SOP Risikoanalyse vorzugehen.

7.4 Validierungsdokumentation

Der Abschnitt Validierungsdokumentation enthält eine Liste aller während der Validierung zu erstellenden Dokumente inklusive dem abschließend zu erstellenden Validierungsbericht.

Nachfolgend eine exemplarische Liste mit den üblicherweise anfallenden Dokumenten (s. auch Musterdokumente):

- Spezifikation der Benutzeranforderungen, Anforderungsspezifikation
- Funktionale Spezifikation

- Hardware Design Spezifikation
- Software Design Spezifikation
- Traceability-Matrix
- Berichte zu Herstellerbewertungen
- Hardware-Installationsprotokoll(e)
- Ggf. Netzwerkdiagramm
- Hardware-Liste
- Software-Installationsprotokoll(e)
- Software-Liste
- Ausdrucke ggf. während der Installation automatisch erstellter Log-Dateien
- IQ-Herstellertestskripte (durchgeführt und unterzeichnet)
- OQ-Testskript(e) (durchgeführt und unterzeichnet)
- PQ-Testskript (durchgeführt und unterzeichnet)
- Validierungsbericht
- Systemspezifische Standard Operating Procedures (SOPs)

Des Weiteren ist das Dokumentenmanagement ausführlich zu beschreiben. Hierbei sind folgende Punkte zu berücksichtigen:

Dokumentenerstellung

- Definition von Dokumentenstandards (Layout, Stil, Referenznummerierung)
- Versionskontrolle

Dokumentenprüfung

- Beschreibung des Revisionsprozesses

Dokumentenfreigabe

- Wer ist an der Freigabe beteiligt
- Unter welchen Bedingungen erfolgt die Freigabe

Dokumentenverteilung

- Beschreibung des Dokumentenverteilungsprozesses, insbesondere Beschreibung der Verwaltung kontrollierter Kopien

Änderungskontrolle

- Änderungen an freigegebenen Dokumenten dürfen nur kontrolliert durchgeführt werden, d.h. nach Erstellung einer neuen Entwurfsversion erfolgt die Dokumentenprüfung, -freigabe und –verteilung nach den definierten Prozessen.

Dokumentenrücknahme

- Beschreibung eines Prozesses für die Rücknahme freigegebener Dokumente insbesondere unter Berücksichtigung der Information von Besitzern kontrollierter Kopien und der Kennzeichnung der Dokumente.

Dokumentenaufbewahrung

- Beschreibung der Dokumentenaufbewahrung insbesondere der Sicherheitsmaßnahmen zum Schutz der Dokumente vor zufälliger und mutwilliger Beschädigung und der Maßnahmen zur Sicherstellung des Wiederauffindens von Dokumenten während des gesamten Aufbewahrungszeitraums.

7.5 Standard Operating Procedures

Dieser Abschnitt des Validierungsplanes enthält eine Liste aller SOPs, die in Folge der Systemeinführung neu zu erstellen bzw. anzupassen sind. Für jede SOP ist hierbei anzugeben, wer für ihre Erstellung, Prüfung und Freigabe verantwortlich ist. Folgende Bereiche sollten hierbei von SOPs abgedeckt sein:

- Datenerfassung und –verarbeitung
- Systemwartung
- Backup, Recovery, Notfallplan
- Sicherheit
- Änderungskontrolle

7.6 Erhaltung des validen Systemzustandes

7.6.1 Änderungskontrolle

Maßnahmen zur Änderungskontrolle müssen gewährleisten, dass Systemänderungen nur risikobewertet und dokumentiert durchgeführt werden. Jede Änderung birgt das Risiko den validen Zustand zu verlieren. Das allgemeine Vorgehen ist in der SOP Änderungskontrolle beschrieben. Sie kann in diesem Abschnitt des Validierungsplanes referenziert werden. Darüber hinausgehende projektspezifische Anforderungen an die Änderungskontrolle sind direkt in diesem Abschnitt zu spezifizieren.

7.6.2 Systemsicherheit

Maßnahmen zur Systemsicherheit dienen der Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen. Die hierfür notwendigen Maßnahmen sind allgemein in den SOPs definiert auf die an dieser Stelle des Validierungsplanes verwiesen werden kann. Darüber hinausgehende projektspezifisch notwendige Maßnahmen sind direkt in diesem Abschnitt zu aufzuführen.

7.6.3 Leistungsüberwachung

Maßnahmen zur Leistungsüberwachung dienen der Überprüfung, ob die von einem Computersystem durchzuführenden Prozesse in den für sie geforderten Zeiten bearbeitet werden können. Dies beinhaltet auch die Überprüfung der Verfügbarkeit. Maßnahmen zur Leistungsüberwachung geben die Möglichkeit zur Früherkennung von Problemen und damit zur rechtzeitigen Einleitung von Gegenmaßnahmen. Im Rahmen der Leistungsüberwachung sollten regelmäßige Leistungs- und Verfügbarkeitstests durchgeführt werden. Art und Ablauf der Tests, Zeitpunkte der Durchführung sowie Verantwortlichkeiten sind in diesem Abschnitt des Validierungsplanes detailliert zu spezifizieren.

Folgende Systemkomponenten sind bei den Leistungstests zu berücksichtigen:

- Arbeitsspeicher
- Prozessor(en)
- Datenträger
- Server/Netzwerk
- Anwendungssoftware

Für jede Systemkomponente eines validierungspflichtigen Systems sind geeignete Leistungs-indikatoren mit entsprechenden Basiswerten zu definieren. Davon ausgehend sind individuelle Testfälle zu spezifizieren und in einem Testskript zusammenzustellen.

Es muss weiterhin definiert werden, wer für die Bewertung der Testergebnisse und die ggf. notwendige Ableitung geeigneter Maßnahmen verantwortlich ist.

7.6.4 Support

Ein zuverlässiger Support ist eine unbedingte Voraussetzung für den kontrollierten Betrieb eines Computersystems und damit zur Erhaltung des validen Systemzustandes. An dieser Stelle sollte daher spezifiziert werden, in welchem Umfang Support notwendig ist und wie er zur Verfügung gestellt wird. Folgende Stufen werden hier üblicherweise unterschieden:

Der **First-Level-Support** (auch User Help Desk) ist erste Anlaufstelle für alle eingehenden Unterstützungsfragen. Der Mitarbeiter bearbeitet diese nach seinem Kenntnisstand weitestgehend selbständig. Ziel ist das schnelle Lösen einer möglichst großen Anzahl von Problemen. Unterstützung erhält der First-Level-Support durch den Second-Level-Support.

Der **Second-Level-Support** unterstützt den First-Level-Support, sowohl durch Weiterbildung am Arbeitsplatz als auch durch Übernahme komplexerer Anfragen. Übersteigt die Komplexität einer Anfrage das Know-How oder die technischen Möglichkeiten des Second-Level-Supports, so wird diese an den Third-Level-Support weitergeleitet (eskaliert).

Der **Third-Level-Support** setzt sich aus Spezialisten einzelner Fachabteilungen bzw. des Herstellers zusammen und stellt so die höchste Eskalationsstufe innerhalb einer Supportorganisation.

7.6.5 Interne Audits

Zusätzlich zu den in unregelmäßigen Abständen stattfindenden externen Audits sollte der valide Systemzustand über interne Audits regelmäßig überprüft werden. Das genaue Vorgehen hierzu wird in der SOP Interne Audits beschrieben.

7.7 Revalidierung

In diesem Abschnitt des Validierungsplanes sind eindeutige Kriterien zu definieren, die, wenn sie erfüllt sind, eine Revalidierung des Computersystems erforderlich machen.

Die Erfüllung der Revalidierungskriterien sollte in jedem Fall nach größeren Änderungen im Rahmen der Änderungskontrolle (s. Kap. 7.6.1 Änderungskontrolle) überprüft werden, aber auch nach Verstreichen eines größeren Zeitraumes mit nur kleinen oder gar keinen Änderungen. Für letzteres wird empfohlen, die Überprüfung der Revalidierungskriterien an die regelmäßigen internen Audits (s. Kap. 7.6.5 Interne Audits) zu koppeln.

7.8 Schulung

Schulungen sind eine wichtige Maßnahme zur Herstellung und Erhaltung des validen Systemzustandes. Nur durch gut geschulte Anwender und Systemverantwortliche kann ein Computersystem kontrolliert betrieben werden.

In diesem Abschnitt des Validierungsplanes sind daher alle notwendigen Schulungsmaßnahmen zu definieren. Hierbei zu berücksichtigen sind sowohl Schulungen zur Nutzung eines Computersystems als auch Schulungen zu dessen Betrieb und Wartung.

Die SOP 1-150 Training beschreibt allgemein die Verantwortlichkeiten bzgl. Schulungen, regulatorische Qualifizierungsanforderungen, die Identifikation des Schulungsbedarfs, die Entwicklung des Schulungsplanes, die Durchführung initialer Schulungen für neue Mitarbeiter, die Durchführung von Schulungen von Mitarbeitern mit und ohne Leitungsfunktion sowie allgemeine dokumentarische Anforderungen.

Die Teilnahme an Schulungen muss generell dokumentiert nachgewiesen werden.

7.9 Außerbetriebnahme

In diesem Abschnitt des Validierungsplanes erfolgt die Spezifikation der Vorgehensweise für die Außerbetriebnahme des Computersystems. Insbesondere sollte beschrieben werden

- wie die Außerbetriebnahme dokumentiert wird,

- welche GCP-relevanten Daten wie lange aufbewahrt werden müssen und welche Daten gelöscht werden können,
- inwieweit die Notwendigkeit besteht, Daten auf ein neues System zu migrieren und möglicherweise auf einem neuen System zu archivieren (inkl. der Methode diesen Prozess zu qualifizieren),
- welche Anforderungen an die Abfrage migrierter Daten bestehen,
- inwieweit Altsysteme zum Zwecke der Datenarchivierung und –abfrage aufbewahrt werden müssen,
- welche Möglichkeiten zur Migration auf portable Formate bestehen,
- welche Systemdokumentation aufbewahrt werden muss.

7.10 Projektmanagement

Im Abschnitt Projektmanagement ist der Projektplan für das gesamte Validierungsprojekt darzustellen. Insbesondere die Phase der Herstellung des validen Systemzustandes ist detailliert zu planen. Es wird empfohlen einen Netzplan zu erstellen.

8 Qualifizierung

8.1 Qualifizierungsmaßnahmen

Der Umfang der Qualifizierungsmaßnahmen richtet sich nach der jeweiligen GAMP-Kategorie. Bei der Kategorie Standardsoftware ist zudem noch zwischen allgemeiner Standardsoftware (z.B. Office-Pakete) oder spezieller Standardsoftware z.B. spezielle Statistikprogramme) zu unterscheiden.

Kategorie	Komponententyp	Validierungsansatz
1	**Betriebssystem**	IQ
3	**Standardsoftware:**	
3a	Allgemeine Standardsoftware	IQ, OQ SOPs Schulung
3b	Spezielle Standardsoftware	IQ, OQ SOPs Schulung Herstellerbewertung
4	**Konfigurierbare Softwarepakete**	IQ, OQ SOPs Schulung Herstellerbewertung Jegliche kundenspezifische, individuelle Programmierung ist gemäß Kategorie 5 zu behandeln
5	**Individualsoftware**	DQ, IQ, OQ SOPs Schulung Hersteller-Audit

Tab. 1: Kategorisierung der Systemkomponenten

8.2 Design Qualifizierung (DQ)

8.2.1 Definition

Die Design Qualifizierung ist lediglich für Individualsoftware erforderlich. In der Regel wird sie durch den Hersteller geliefert. Bei Eigenentwicklungen ist eine DQ in eigener Verantwortung erforderlich. Der Prozess der DQ wurde im Projekt Systemvalidierung nicht weiter betrachtet. Für eine nachträgliche Validierung von Eigenentwicklungen kann das Verfahren zum Code Review genutzt werden.

Die Design Qualifizierung umfasst die dokumentierte Verifikation, dass sowohl bzgl. des Gesamtsystems als auch bei allen GCP-relevanten Branchensoftware- und Individualsoftware-Komponenten

- zutreffende Gesetze, sonstige Regularien und Standards in der Spezifikation der Benutzeranforderungen berücksichtigt wurden und
- das System entsprechend seiner Anforderungen konzipiert wurde, d.h. in der funktionalen Spezifikation und der Design-Spezifikation alle Benutzeranforderungen korrekt umgesetzt wurden.

Bei einzelnen Systemkomponenten umfasst die DQ zusätzlich den dokumentierten Nachweis, dass der Entwicklungsprozess die geforderten Qualitätsstandards erfüllt.

8.2.2 Zeitpunkt

Bei der DQ muss unterschieden werden zwischen der DQ des Gesamtsystems, der DQ in Fremdentwicklung erstellter Systemkomponenten und der DQ in Eigenentwicklung erstellter Systemkomponenten. Letztere soll im Rahmen dieses Masterplanes nicht weiter betrachtet werden.

Die DQ des Gesamtsystems ist begleitend zu dessen Spezifikation durchzuführen. Die DQ in Fremdentwicklung erstellter Systemkomponenten ist im Rahmen der Erstellung der Design-Spezifikation des Gesamtsystems durchzuführen.

8.2.3 Verantwortlichkeiten

Da die DQ die Bestätigung zum Ergebnis hat, dass das Systemdesign die Anforderungen erfüllt, sollten in jedem Fall zukünftige Anwender oder deren Vertreter, Systemdesigner und QA-Verantwortliche eingebunden sein.

8.2.4 Maßnahmen zur DQ des Gesamtsystems

Zur DQ des Gesamtsystems dienen drei Design Reviews mit deren Hilfe die Spezifikation der Benutzeranforderungen, die funktionale Spezifikation und die Design-Spezifikation auf Vollständigkeit, Korrektheit und Konsistenz überprüft werden. Diese werden im Folgenden erläutert.

Design Review 1

Ziel des ersten Design Review ist der dokumentierte Nachweis, dass in der Spezifikation der Benutzeranforderungen alle zutreffenden Gesetze, sonstigen Regularien und Standards berücksichtigt wurden. Hierfür ist eine Compliance-Tabelle zu erstellen, in der die Zuordnung aller relevanten Gesetze, Regularien und Standards zu den einzelnen Anforderungen erfolgt. Das Design Review 1 ist unmittelbar nach Fertigstellung der Spezifikation der Benutzeranforderungen durchzuführen. Vorgaben, die nicht berücksichtigt wurden sind dem Autor der Spezifikation der Benutzeranforderungen in einem schriftlichen Design Review Report mitzuteilen. Nach Überarbeitung der Spezifikation der Benutzeranforderungen erfolgt eine neuerliche Prüfung. Werden alle Vorgaben durch entsprechende Anforderungen berücksichtigt, ist dies vom Durchführenden des Design Review durch Unterschrift der Compliance-Tabelle zu bestätigen.

Design Review 2

Das zweite Design Review erfolgt unmittelbar nach Fertigstellung der funktionalen Spezifikation. Ziel ist der dokumentierte Nachweis, dass alle Benutzeranforderungen in der funktionalen Spezifikation korrekt umgesetzt wurden. Hierzu ist die funktionale Spezifikation inhaltlich gegen die Anforderungs-spezifikation zu prüfen. Nicht bzw. falsch umgesetzte Anforderungen sind dem Autor der funktionalen Spezifikation über einen schriftlichen Design Review Report mitzuteilen. Nach Überarbeitung der funktionalen Spezifikation erfolgt eine neuerliche Prüfung. Die korrekte Umsetzung aller Benutzeranforderungen wird durch Unterschrift des Design Reviewers am Ende der funktionalen Spezifikation bestätigt. Des Weiteren sind die entsprechenden Informationen in die Traceability-Matrix einzutragen.

Design Review 3

Das dritte Design Review umfasst die Erstellung eines dokumentierten Nachweises, dass in der Design-Spezifikation alle Benutzeranforderungen korrekt umgesetzt wurden. Sie erfolgt nach Fertigstellung der Design-Spezifikation über eine inhaltliche Prüfung derselben gegen die Benutzeranforderungen. Nicht bzw. falsch umgesetzte Anforderungen sind dem Autor der Design-Spezifikation über einen schriftlichen Design Review Report mitzuteilen. Nach Überarbeitung der Design-Spezifikation erfolgt eine neuerliche Prüfung. Die korrekte Umsetzung aller Benutzeranforderungen wird durch Unterschrift des Design Reviewers am Ende der Design-Spezifikation bestätigt. Des Weiteren sind die entsprechenden Informationen in die Traceability-Matrix einzutragen.

8.2.5 Maßnahmen zur DQ in Fremdentwicklung erstellter Systemkomponenten

Die DQ von in Fremdentwicklung erstellter Systemkomponenten hat durch den Hersteller zu erfolgen. Dies ist im Rahmen der Herstellerbewertung (Supplier Assessment) zu prüfen. Eigene DQ-Maßnahmen sollten sich dann auf evtl. Konfigurations- und Customizing-Maßnahmen beschränken. Die Durchführung einer Herstellerbewertung wird im Konzept zum Vendor Audit umfassend beschrieben.

8.3 Installations Qualifizierung (IQ)

8.3.1 Definition

Die Installations Qualifizierung umfasst die dokumentierte Verifikation, dass ein Computersystem gemäß seiner Design-Spezifikation installiert wurde.

8.3.2 Zeitpunkt

Die IQ ist begleitend zur Installation des Gesamtsystems durchzuführen.

8.3.3 Verantwortlichkeiten und Maßnahmen

Verantwortlichkeiten und Maßnahmen zur IQ sind in der SOP 1-090 Installations Qualifizierung (IQ) definiert.

➔ SOP 1-090 Installations Qualifizierung

8.4 Operationale Qualifizierung (OQ)

8.4.1 Definition

Die Operationale Qualifizierung umfasst die dokumentierte Verifikation, dass eine Systemkomponente alle ihr zugeordneten und in der funktionalen Spezifikation definierten Funktionen korrekt ausführt.

8.4.2 Zeitpunkt

Die OQ ist im Anschluss an die IQ durchzuführen.

8.4.3 Verantwortlichkeiten und Maßnahmen

Verantwortlichkeiten und Maßnahmen zur OQ sind in der SOP 1-010 Operationale Qualifizierung (OQ) definiert.

➔ SOP 1-100 Operationale Qualifizierung

8.5 Performance Qualifizierung (PQ)

8.5.1 Definition

Die Performance Qualifizierung umfasst die dokumentierte Verifikation, dass ein Computersystem als Gesamtsystem alle Benutzeranforderungen erfüllt und in der Lage ist, innerhalb der übergeordneten Geschäftsprozesse im Routinebetrieb alle geforderten Funktionen korrekt auszuführen.

8.5.2 Zeitpunkt

Die PQ ist im Anschluss an die OQ durchzuführen.

8.5.3 Verantwortlichkeiten und Maßnahmen

Zur Durchführung einer Performance Qualifizierung sind auf der Basis der Spezifikation der Benutzeranforderungen für das Gesamtsystem entsprechende Testfälle zu entwickeln und unter Einbeziehung der zukünftigen Anwender durchzuführen. Die Testergebnisse sind zu dokumentieren und zu bewerten. Folgende Dokumente sollten nach Abschluss der PQ minimal vorliegen:

- PQ-Testskript (durchgeführt und unterzeichnet)
- Traceability-Matrix mit PQ-Referenzen

➔ SOP 1-110 Performance Qualifizierung

9 Anhang

9.1 Referenzen

1. Deutsche Übersetzung der Leitlinien zur Guten Klinischen Praxis (GCP), CPMP/ICH/135/95.
2. FDA, 21 CFR Part 11, Electronic records, Electronic Signature; Final Rule, Federal Register, 62, No. 54, 13429 (1997)
3. Guidance for Industry, Computerized Systems Used in Clinical Trials, FDA, ORA
4. EG - GMP-Leitfaden, Annex 11, EWG III/8263/89
5. EU - Clinical Trial Directive 2001/20/EC (2001)
6. W. Kuchinke und C. Ohmann, Endbericht zum TMF-Projekt SY5.1-Softwareunterstützung klinischer Studien mit Schwerpunkt RDE, TMF Berlin, 03/08/2003, (2003).
7. The Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems in Pharmaceutical Manufacture (ISPE), Vol. 5
8. L. Huber: Validation of Computerized Analytical and Networked Systems: Interpharm Press, Inc., Englewood
9. Ludwig Huber: Validation Masterplan - Best Practices: Interpharm Press
10. Ludwig Huber: Network Quality Package - Best Practices: Interpharm Press
11. S. I. Haider: Pharmaceutical Master Validation Plan: Ultimate Guide to FDA, GMP, and GLP Compliance: Saint Lucie Press
12. Computer Validation Survival Kit: IVT Institute of Validation Technology
13. B. Mullendore, Computer Validation Master Plan, Technical Guide, IVT 2002
14. O. Lopez: 21 CFR Part 11: Complete Guide to International Computer Validation Compliance for the Pharmaceutical Industry, CRC Press (2004)
15. S. R. Goldman: Handbook of Computer and Computerized System Validation for the Pharmaceutical Industry (1stbooks Library), Author House (2003)
16. J. O. Grady: System Validation + Verification, CRC Press (1997)
17. Teri Stokes: The Survive and Thrive Guide to Computer Validation: Interpharm Press, Inc., Englewood
18. Teri Stokes: Computer System Validation, Part 1: Software Purchase and GCP Compliance: Applied Clinical Trials: September 1996
19. Teri Stokes: Computer System Validation, Part 1: Software Purchase and GCP Compliance: Applied Clinical Trials: September 1996
20. Teri Stokes: Computer System Validation, Part 2: Installing GCP Systems at Investigator Sites: Applied Clinical Trials: January 1997
21. Teri Stokes: Computer System Validation, Part 3: Validation of GCP Systems at Investigator Sites: Applied Clinical Trials: February 1997
22. Teri Stokes: Computer System Validation, Part 4: Operating GCP Systems at Investigator Sites: Applied Clinical Trials: April 1997
23. Teri Stokes: Computer System Validation, Part 5: A Structured Approach to Retrospective Evaluation: Applied Clinical Trials: June 1997

24. Teri Stokes: Computer System Validation, Part 6: A Survive and Thrive Approach to Audits and Inspections: Applied Clinical Trials: August 1997
25. Teri Stokes: Validating Computer Systems, Part 1: A GCP Computer System Is a Lifetime Responsibility: Applied Clinical Trials: August 2000
26. Teri Stokes: Validating Computer Systems, Part 2: GCP Validation of Platform and Infrastructure Systems: Applied Clinical Trials: September 2000
27. Teri Stokes: Validating Computer Systems, Part 3: GCP Software Verification: Applied Clinical Trials: November 2000
28. Teri Stokes: Validating Computer Systems, Part 4: The QA Role in Computer Validation: Applied Clinical Trials: February 2001
29. Abschlussbericht Systemvalidierung in klinischen Studien, Erstellung eines Validierungspaketes für die KKS und andere Verbünde, Projekt SY-4.5, Hrg.: Ronald Speer, 2003-08-29, TMF 2003.
30. Concept Heidelberg (Herausgeber), Aktuelle Aspekte der Validierung computergestützer Systeme, Editor Cantor Verlag, Aulendorf, 2004.
31. Erreichung und Sicherstellung von Validierungsstandards in den Forschungsverbünden der Telematikplattform für Medizinische Forschungsnetze e.V. (TMF); Projektgruppe Systemvalidierung TMF, GMDS 2006
32. COMPUTER – VALIDIERUNG, Ein Leitfaden für die Validierung computergestützter Systeme bei Blutbanken: Deutschen Gesellschaft für Transfusionsmedizin und Immunhämatologie (DGTI), www.dgti.de, 3. Auflage, Mai 2003

9.2 Abbildungsverzeichnis

9.3 Tabellenverzeichnis

9.4 Glossar

AMG Gesetz über den Verkehr mit Arzneimitteln – Arzneimittelgesetz
ASP Application Service Provider
CAP Corrective Action Plan
CDMS Clinical Datamanagement System
CFR Code of Federal Regulations der USA (www.gpoaccess.gov/cfr)
CMS Content Management System (zumeist Web-basiert)
COTS Commercial-off-the-shelf (Kürzel für kommerzielle Produkte von der Stange)
CRC Clinical Research Coordinator
CRF Case Report Form
CSV Computer System Validation
DGTI Deutschen Gesellschaft für Transfusionsmedizin und Immunhämatologie
DQ Design Qualification
EC European Commission
EDC Electronic Data Capturing
EG Europäische Gemeinschaft
FDA Federal Drug Administration (www.fda.gov)
FV Forschungsverbünde (in der TMF)
GAMP Good Automated Manufacturing Practice, Richtlinien eines technischen Sub-Kommittees der ISPE (www.ispe.org/gamp)
GCP Good Clinical Practice, Regelwerk der ICH
GLP Good Laboratory Practice
GMDS Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (www.gmds.de)
GMP Good Manufacturing Practice, Richtlinien der Weltgesundheitsorganisation (WHO) für die Herstellung und die Sicherung der Qualität von Arzneimitteln
GOST Teststudie mit dem Titel "German Validation Of Studysoftware"
GxP Good [..] Practice - das x ist Platzhalter z.B. für C wie Clinical (s. GCP) oder M wie Manufacturing
iAS interActive Systems (www.interactive-systems.de)
ICH International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (www.ich.org)
IIT Investigator initiated trial
IQ Installation Qualification im Rahmen einer Systemvalidierung
ISPE International Society for Pharmaceutical Engineering (www.ispe.org)
IVT Institute of Validation Technology
KKS Koordinierungszentrum für Klinische Studien (www.kks-netzwerk.de)
KN Kompetenznetz (www.kompetenznetze-medizin.de)
ML KN Maligne Lymphome (www.kompetenznetz-lymphome.de)
OQ Operational Qualification im Rahmen einer Systemvalidierung
PG Projektgruppe
PhOSCo Pharma Open Source Community (www.phosco.org)
PQ Performance Qualification im Rahmen einer Systemvalidierung
QA Quality Assurance
QM Qualitätsmanagement
QS Qualitätssicherung
RDE Remote Data Entry (System)
RTM Requirements Traceability Matrix
SLA Service Level Agreement
SOP Standard Operating Procedure
SVMP Systemvalidierungs-Masterplan
TM Traceability Matrix
TMF Telematikplattform für Medizinische Forschungsnetze e.V. (www.tmf-ev.de)
URS User Requirments Specification
VLC Validation Life Cycle
V-Modell Verpflichtendes Vorgehensmodell für ausgeschriebene IT-Projekte der Bundesbehörden. Im Februar 2005 wurde die Version V-Modell 97 durch V-Modell XT (für eXtreme Tailoring) abgelöst (www.kbst.bund.de/cln_011/nn_836960/Content/Standards/V__Modell/vmodell__node.html)
VMP Validation Master Plan
VP Validierungsplan
WHO World Health Organization (www.who.org)