Roemer, Sandkühler, Schmitt, Schober, Veit

Computergestützte Systeme im GMP-Umfeld

Hardware und Software
GMP-konform validieren und betreiben

4. Auflage 2025

GMP VERLAG Peithes

GMP-Fachwissen TECHNIK

PDF Download

GMP-BERATER Auszug

Inhaltsverzeichnis

Einführung

Computergestützte Systeme spielen eine zentrale Rolle bei der Herstellung und Prüfung von Arzneimitteln. Dies erklärt auch, warum solche Systeme unter GMP-Gesichtspunkten validiert sein müssen.

Bei der Validierung computergestützter Systeme sind zahlreiche **Anforderungen** zu beachten. Neben den verbindlichen Regularien gibt es zahlreiche Leitlinien mit Empfehlungscharakter, die den Stand der Technik repräsentieren. Hierzu zählt auch der GAMP®5.

Eine wichtige Voraussetzung für die Validierung ist das Verständnis des **System-Lebenszyklus**, der von der Planung bis zur Stilllegung reicht. Für die eigentliche Validierung wird das sogenannte V-Modell zur Darstellung der Spezifikations- und zugehörigen Testphasen herangezogen.

Die **Systemklassifizierung** gemäß GAMP®5 sieht vier Softwareklassen vor, die sich in ihrer Komplexität und dem dazugehörigen Validierungsumfang unterscheiden. Diese Einstufung muss über einen Prozess des **Risikomanagements** weiter verfeinert werden. Ziel ist es, die erkannten Risiken zu bewerten und durch geeignete Maßnahmen zu minimieren.

Die **Validierung** nach dem V-Modell verläuft in 2 Phasen: der Konzeptionsphase und der Projektphase. Die einzelnen Schritte mit den dazugehörigen Aktivitäten und Dokumenten werden ausführlich erläutert. Die Rückverfolgbarkeit aller Validierungsaktivitäten über den gesamten Lebenszyklus eines Systems wird dabei durch eine *Traceability Matrix* sichergestellt. Zum Transfer der Daten und zur Inbetriebnahme des Systems sollte ein *Transition Plan* mit allen wichtigen Prüfpunkten für die Inbetriebnahme erstellt werden.

Für den **Betrieb** eines computergestützten Systems müssen zahlreiche Abläufe definiert, in SOPs beschrieben und geschult werden. Zu den relevanten Themen zählen Zugangsberechtigungen, Datensicherung und Archivierung, Notfallplanung und Datenwiederherstellung, der Umgang mit Änderungen und Fehlern, die periodische Überprüfung und die letztendliche Stilllegung des Systems.

Werden für die Validierung **externe Dienstleister** hinzugezogen, müssen diese vor der Auftragsvergabe qualifiziert werden. Dieses Kapitel enthält einen Fragenkatalog zur Bewertung von Dienstleistern und Lieferanten, mit dem Sie sich auf die Auditierung vorbereiten können. Hilfreiche Tipps zu wichtigen Inhalten des Dienstleistungsvertrags ergänzen die Ausführungen.

Cloud-Anwendungen sind flexibel, schnell und kostengünstig. Aus der Sicht eines GxP-regulierten Unternehmens ergeben sich jedoch viele Fragen bezüglich der Datensicherheit, Datenverfügbarkeit und Datenintegrität. Voraussetzung für eine erfolgreiche Cloud-Nutzung im GxP-Umfeld ist daher ein klares Verständnis der Anforderungen sowie der potenziellen Chancen und Risiken.

Dabei hat die grundlegende Forderung nach **Datenintegrität** einen besonderen Stellenwert eingenommen. In diesem Kapitel finden Sie die wichtigsten Anforderungen an die Datenintegrität, die aus den aktuellen Vorgabedokumenten abgeleitet werden können. Zur Einhaltung der Vorgaben sollten geeignete Überwachungssysteme vorhanden sein. Außerdem sollten regelmäßig Personalschulungen durchgeführt werden. Die Forderung nach Datenintegrität bezieht sich auf den gesamten Lebenszyklus und schließt auch die Archivierung mit ein.

Viele Abbildungen, Beispiele, Tabellen und Checklisten erleichtern die Einarbeitung in das Thema Computergestützte Systeme. Im Kapitel **Informationsquellen** finden Sie ein umfangreiches Verzeichnis von weiterführender Literatur und Regelwerken als Grundlage für eine weitere Vertiefung in die Materie.

Dieses e-book beinhaltet Themen aus dem Bereich Computergestützte Systeme, die in der Wissenssammlung GMP-BERATER enthalten sind. Der GMP-BERATER behandelt alle Themen, die für die GMP-Konformität in der Arzneimittelherstellung von Bedeutung sind.

Schopfheim, Juli 2025

1 Zielsetzung und Bedeutung der Computervalidierung

Markus Roemer

Hier finden Sie Antwort auf folgende Fragen:
- Was ist ein computergestütztes System?
- Was versteht man unter „Computervalidierung“?
- Welche Rolle spielen Qualitätsmanagement und Risikomanagement für die Computervalidierung?
- Welche Bedeutung hat die Qualifizierung der IT-Infrastruktur?
- Wie sind Aufwand und Nutzen der Computervalidierung einzuschätzen?

Was wäre die moderne Arzneimittelherstellung ohne Computer? Von der Bestellung der Ausgangstoffe bis zur Auslieferung des fertigen Arzneimittels gibt es kaum noch einen Arbeitsschritt, der nicht in irgendeiner Weise von der ordnungsgemäßen Funktion eines computergestützten Systems abhängig ist. So gesehen ist es nicht verwunderlich, dass der Validierung computergestützter Systeme eine zentrale Bedeutung zukommt.

In diesem Kapitel erfahren Sie, welche regulatorischen Anforderungen dabei zu beachten sind, und in welchen Leitlinien Sie nützliche Informationen zur Umsetzung in die Praxis finden (siehe Kapitel 2 *Regulatorische Anforderungen an computergestützte Systeme und den Validierungsprozess*). Eine wichtige Voraussetzung für die Validierung ist das Verständnis des System-Lebenszyklus, der in Kapitel 3 *System-Lebenszyklus* vorgestellt wird. Systemklassifizierung und Risikomanagement sind wichtige Elemente, um Umfang und Tiefe der Validierung richtig einzuplanen. Ihre Anwendung wird in Kapitel 4 *Systemklassifizierung und Risikomanagement* erläutert. Die einzelnen Schritte der Validierung werden in Kapitel 5 *Qualifizierung und Validierung computergestützter Systeme* ausführlich beschrieben und anhand von Beispielen veranschaulicht. Welche Aspekte beim Betrieb eines computergestützten Systems aus GMP-Sicht relevant sind, erfahren Sie in Kapitel 6 *Betrieb computergestützter Systeme*. Welche Besonderheiten bei der Zusammenarbeit mit externen Dienstleistern zu beachten sind, erfahren Sie in Kapitel 7 *Externe Dienstleister*. Auch auf spezielle Fragestellungen wie Rohdatenmanagement oder Cloud-Lösungen soll eingegangen werden (siehe Kapitel 8 *GXP-relevante Daten in der Cloud*).

Zentrales Thema dieses Kapitels ist die Validierung von computergestützten Systemen, die im allgemeinen Sprachgebrauch häufig als **Computervalidierung** bezeichnet wird. Der Begriff *computergestütztes System* ist dabei historisch geprägt, wird hier thematisch aber breiter aufgestellt, um die heutige Komplexität, den Stand der Technik und deren Zusammenhänge richtig darzustellen.

Vom computergestützten System zur Informationstechnologie

Mit dem Aufkommen von Computern in der Industrie in den 80er Jahren des letzten Jahrhunderts wurde auch damit begonnen, die Qualität solcher Systeme mit regulatorischen Forderungen zu belegen. Ein bekanntes Beispiel ist das *Blue Book* („Guide to Inspection of Computerised Systems“) der FDA aus dem Jahre 1983. Hier wurde z. B. schematisch eine Zentrale Recheneinheit (CPU) über zwei Kabel an eine analoge Signalquelle verbunden dargestellt, oder über die Möglichkeit von Netzwerken (z. B. über Satelliten) zwischen zwei verschiedenen Standorten geschrieben. Dies wirkt aus heutiger Sicht zwar amüsant, aber die Grundprinzipien der Validierung aus dem o.g. *Blue Book* sind interessanterweise heute noch zutreffend. Heutige Systeme oder Applikationen fallen dabei eher in den weiteren Bereich der *Informationstechnologie* (kurz: IT) und repräsentieren damit den sogenannten Stand der Technik, welcher grundlegend sehr verschieden geartet sein kann.

Die Validierung von computergestützten Systemen ist eine *interdisziplinäre* Aufgabe, die u.a. folgende **Elemente** beinhalten kann:

- Prozessanalyse
- Anforderungsmanagement
- Projektmanagement und -methoden
- Risikomanagement-Methoden
- Spezifikationen / Systembeschreibungen
- Software-Entwicklungsstandards
- Test-Management und Automatisierung
- IT-Management und Services
- Gute Dokumentationspraxis / Qualitätsmanagement

Eine Beteiligung von ausgewiesenen Fachexperten in diesen verschiedenen Aufgaben, die im Englischen *Subject Matter Experts* (SME) genannt werden, kann damit erforderlich sein.

Risikobasierte Validierung und skalierbare Modelle

Im Folgenden wird bewusst die Validierung ohne die traditionelle Darstellung eines V-Modells oder die herkömmlichen Phasen (DQ, IQ, OQ, PQ) beschrieben. Stattdessen werden skalierbare Validierungsmodelle dargestellt, sowie die dazugehörigen Kriterien zur Auswahl des geeigneten Modells.

Diese Kriterien führen zu einem sogenannten risikobasierten Validierungsansatz, der die Prozesse und Systemeigenschaften berücksichtigt. Daher wird eine mögliche Kategorisierung von Systemen vorgestellt. Generell gibt es eine Vielfalt von verschiedenen Validierungsobjekten wie z.B. IT-Systeme, Applikationen, Tabellenkalkulationsprogramme, Prozessanlagen oder Laborsysteme, für die der geeignete und passende Validierungsansatz bestimmt werden muss. Dieser ist auch abhängig von der (GMP-) Kritikalität der Daten, die im Speziellen auf einem dieser Systeme verarbeitet oder gespeichert werden.

Qualitätssysteme

Die Validierung computergestützter Systeme ist ein wichtiger Bestandteil eines *Pharmazeutischen Qualitätssystems* (PQS) bzw. eines *Qualitätsmanagementsystems* (QMS) von Lieferanten und Dienstleistern. Die Validierung muss in dieses System integriert sein, zum Beispiel für die Dokumentenverwaltung der Validierungsaufzeichnungen oder die Regelung von Verantwortlichkeiten. Grundsätzlich sind IT-Projekte immer kommerziell oder vertraglich verbunden über einen Auftraggeber (z.B. pharmazeutischer Betreiber; Lastenheft) und einen Auftragnehmer (Lieferant, Dienstleister; Pflichtenheft). Beide Parteien müssen über ein entsprechendes, nachweisbares PQS bzw. QMS verfügen. Dies gilt auch, wenn der Auftragnehmer firmenintern für die Umsetzung verantwortlich wäre (z.B. IT-Abteilung). Je nach Bewertung und Komplexität eines IT-Projekts sollte eine Lieferantenbewertung über verschiedene Methoden einer Qualifizierung (z.B. Auditierung) erfolgen. Neben der qualitätsrelevanten Bewertung von Auftragnehmern können oftmals auch vertragliche Aspekte hinzu kommen, die in Qualitätsvereinbarungen (*Quality Agreements*) festgelegt sein müssen (z.B. Outsourcing, Gewährleistung, Antwortzeiten, etc.).

Eine wichtige Basis des Qualitätsmanagements ist das *Risikomanagement*, das auch für die Validierung in verschiedenen Phasen und Ausprägungen angewendet werden soll. Hieraus entstehen diverse qualitätsrelevante und nachvollziehbare Entscheidungen (*Quality Decisions*), die ebenso dokumentiert und nachweisbar sein müssen und im Validierungsansatz enthalten sind.

IT-Service-Management und Anwendungen

Viele Systeme werden im IT-Netzwerk und nicht als Einzelplatzlösung betrieben, was thematisch zur **Qualifizierung der IT-Infrastruktur** führt. Ferner werden im Rahmen von Prozessoptimierungen auch Systeme über Schnittstellen für den (bi-direktionalen) Datenaustausch miteinander verbunden. Solche Schnittstellen und die daraus resultierende, routinemäßige Datenübertragung müssen in die Überlegungen für die Validierung ebenso eingehen. Selbst die Festlegung, wo exakt die Systemgrenzen zu ziehen sind, ist nicht leicht zu treffen. Oft wird auch über IT-Lösungen gesprochen, die wiederum aus einzelnen IT-Systemen (von verschiedenen Herstellern) bestehen können.

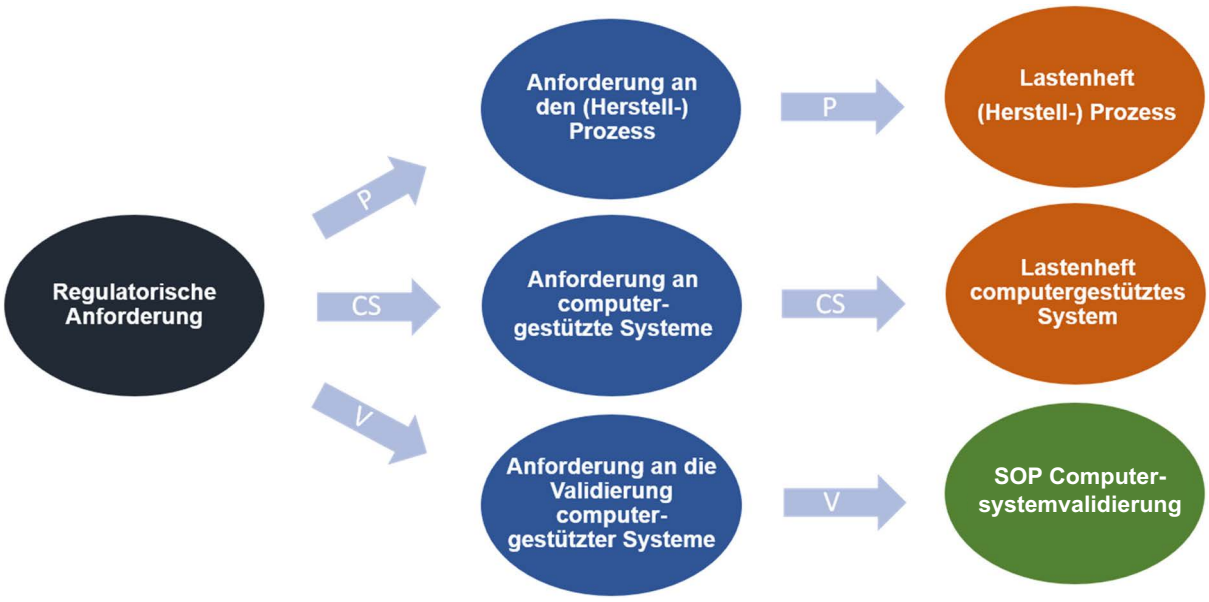
Zu den heutigen Validierungsaufgaben gehört oftmals auch die Ablösung von bestehenden, im Betrieb befindlichen Systemen durch neue Systeme. Dabei kann zusätzlich die Anforderung

Bei der Betrachtung der Anforderungen lassen sich daher drei wesentliche Arten von Anforderungen unterscheiden:

1. Spezielle Anforderungen an den Prozess
   - Beispiel: Eingaben in Aufzeichnungen sollen unmittelbar nach der Durchführung einer Tätigkeit vorgenommen werden. Die Eintragungen sollen unauslöschlich sein und die eintragende Person eindeutig identifizieren. (EU-GMP-Leitfaden Teil II – Abschnitt Dokumentation und Protokolle)
2. Allgemeine Anforderungen an computergestützte Systeme
   - Beispiel: Elektronisch gespeicherte Daten müssen gegen Verlust und Manipulation geschützt werden. Bei computergestützter Datenverarbeitung ist anstatt der händischen Unterschrift der eindeutige Name der Person anzugeben. Zudem muss sichergestellt werden, dass nur autorisierte Personen elektronische Eingaben und Bestätigung über die Ausführung der jeweiligen Tätigkeiten vornehmen können. (AMWHV Abschnitt 2 § 10 Allgemeine Dokumentation)
3. Anforderungen an die Validierung computergestützter Systeme
   - Beispiel: Die Einführung eines computergestützten Systems soll geplant erfolgen. Dabei muss der gesamte Lebenszyklus risikobasiert betrachtet werden und eine vollständige, nachvollziehbare Validierungsdokumentation muss vor der produktiven Nutzung genehmigt sein. (EU-GMP-Leitfaden Anhang 11)

Diese unterschiedlichen regulatorischen Anforderungen finden Eingang in unterschiedliche Dokumente, wie Abbildung 2-1 veranschaulichen soll.

Abbildung 2-1 Unterteilung der regulatorischen Anforderungen an Prozesse, computergestützte Systeme und Validierung mit den zugehörigen Dokumenten



Anforderungen an computergestützte Systeme müssen für die digitalisierten Prozesse umgesetzt werden. Die regulatorischen Anforderungen an den Validierungsprozess müssen im pharmazeutischen Unternehmen in eine Verfahrensanweisung überführt werden.

2.3 Analyse der Anforderungen

Zur Unterstützung der Leser bei der Erarbeitung regulatorischer Anforderungen an Computersysteme und die Validierung computergestützter Systeme wurden die folgenden Regularien einer inhaltlichen Schlagwortanalyse unterzogen und die gefundenen Textstellen analysiert:

- Arzneimittelgesetz (AMG)
- Arzneimittel- und Wirkstoffherstellungsverordnung (AMWHV)
- EU-GMP-Leitfaden Teil I – (für Arzneimittel)
- EU-GMP-Leitfaden Teil II – (für Wirkstoffe)
- EU-GMP-Leitfaden Anhang 11
- 21 Code of Federal Regulations (CFR) Part 11

3 System-Lebenszyklus

Markus Roemer, Dr. Siegfried Schmitt

Hier finden Sie Antwort auf folgende Fragen:
- Was ist ein (Computer-)System?
- Welche Phasen beinhaltet der System-Lebenszyklus?
- Was versteht man unter dem „V-Modell“?
- Was ist bei der Softwareentwicklung zu beachten?
- Was versteht man unter Konfiguration und Anpassung?

3.1 Was ist ein Computersystem?

Der ISPE®GAMP 5 Guide beschreibt ein (Computer-)System folgendermaßen:
„Ein (Computer-)System besteht aus der Hardware, der Software und den Netzwerkkomponenten, sowie den gesteuerten Funktionen und der zugehörigen Dokumentation.“

3.2 Welche Phasen beinhaltet der System-Lebenszyklus?

Bevor das Thema Validierung von computergestützten Systemen weiter vertieft wird, soll zunächst der gesamte **Lebenszyklus** eines Systems betrachtet werden. Dieser ist in Abbildung 3-1 schematisch dargestellt und setzt sich aus den nachfolgend beschriebenen Elementen zusammen.

Abbildung 3-1 Lebenszyklus computergestützter Systeme

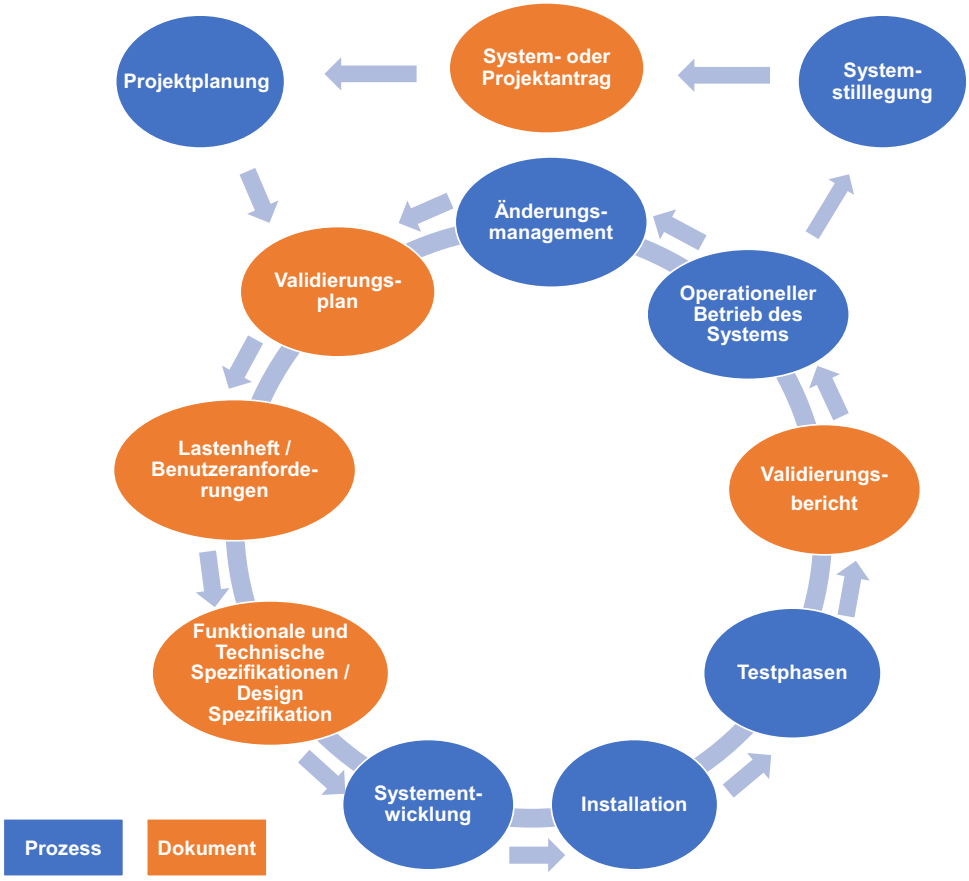


Abbildung 4-3 Anwendungsfälle für Risikobeurteilungen im Rahmen der Validierung computergestützter Systeme

Mögliche Risikobeurteilungen im Rahmen einer Validierung computergestützter Systeme

- Bestimmung/Abgrenzung der GMP-Relevanz des Systems
- Ablösung einer manuellen Tätigkeit durch ein computergestütztes System
- Auswahl von Lieferanten oder Dienstleistern (Hinweis: IT-Abteilung sollte als Dienstleister behandelt werden)
- Auswahl einer Technologie
- Verwendung einer elektronischen Signatur
- Festlegung der Testtiefe für verschiedene Funktionen
- Migration und Aufbewahrung von Daten bei Ablösung/Stilllegung eines Systems
- Planung von Systemänderungen (z. B. Systemupdate, Änderung der Infrastruktur)
- Bewertung der Abweichungen aus der Lieferantenbewertung
- Auswahl und Änderungen des IT-Sicherheitskonzepts (z. B. Backup und Restore)
- Änderungen der Projektorganisation
- Änderung am operationellen Betrieb des Systems (z. B. Vergabe von Berechtigungen)
- Akzeptanzkriterien für „go live“ und „Status validiert“

Alternativer Ansatz zur Risikobewertung

Auf Grundlage der prozessbezogenen Anforderungen im Lastenheft ist gemäß ISPE GAMP®5 eine **Prozessrisikoanalyse** vorgesehen, um Risiken bezüglich Patientensicherheit, Produktqualität, Datenintegrität und Compliance-Anforderungen festzustellen. Ziel ist es, eine Aussage darüber zu bekommen, welches Risiko eine Anforderung mit sich bringt und ob weitere risikominimierende Maßnahmen erforderlich sind.

Aus der Anwendung der Methode des *Golden Circle* ergeben sich folgende Aufgaben, um das Ziel der Risikobewertung computergestützter Systeme zu erreichen:

1. Lastenheft mit allen regulatorischen und Prozess-Anforderungen erstellen
2. unerwünschte Wirkungen identifizieren und die erforderlichen risikominimierenden Maßnahmen als Anforderungen im Lastenheft ergänzen
3. Software- und Hardware-Kategorie gemäß ISPE GAMP®5-Definition den Anforderungen im Lastenheft zuordnen
4. für jede Anforderung die GxP-Relevanz bestimmen
5. Risikoprioritätszahl bestimmen
6. Risikoprioritätszahl bewerten

Die **Schritte 1–3** sind bereits in Kapitel 4.1 *Systemklassifizierung nach ISPE GAMP®5* und Kapitel 5 *Qualifizierung und Validierung computergestützter Systeme* beschrieben und werden daher hier nur kurz zusammengefasst. Die Bestimmung der GxP-Relevanz, die Berechnung der Risikoprioritätszahl sowie deren mögliche Bewertung (Schritte 4-6) werden nachfolgend erläutert.

In der Regel sind computergestützte Systeme aus Modulen, Komponenten und Funktionen aufgebaut, denen verschiedene Softwarekategorien gemäß ISPE GAMP®5 zur Erfüllung einer Anforderung zugeordnet werden können (siehe Kapitel 4.1 *Systemklassifizierung nach ISPE GAMP®5*). So wird beispielsweise eine individuell programmierte Schnittstelle der Softwarekategorie 5 zugeordnet, während ein Standard-Monitoring-System ohne Konfiguration der Softwarekategorie 3 entspricht. Für die Risikobewertung kann daher jede Anforderung einzeln betrachtet und bewertet werden.

Durch die Anwendung von Risikoanalysemethoden können potentiell unerwünschte Wirkungen oder fehlende Anforderungen aufgezeigt werden. Die Ergebnisse sollten iterativ als Anforderung im Lastenheft ergänzt und ebenso einer Risikobeurteilung unterzogen werden.

Schritt 4: Bestimmung der GxP-Relevanz

Der ISPE GAMP®5 gibt einige Beispiele zur Risikobeurteilung, wird jedoch bei Angaben zur Risikopriorität respektive Auswirkung unerwünschter Wirkungen auf Patientensicherheit, Produktqualität und Datenintegrität eines computergestützten Systems nicht konkret. Der ISPE GAMP®5 folgt damit letztlich nur der Formulierung der ICH Q9, quantitative Beschreibungen wie zum Beispiel „high“, „medium“ oder „low“ so detailliert wie möglich zu definieren. Entsprechende Zitate sind in Abbildung 4-4 wiedergegeben.

Abbildung 5-17 Inhalte eines Migrationsplans (Forts.)

Punkte im Migrationsplan	Beschreibung
verwendete Programme zum Datentransfer bzw. zur Datenkonvertierung	Beschreibung der verwendeten Programme und deren Zusammenwirken
Datenprüfung (im alten System)	Die Datenbestände sollten auf Fehler geprüft und bei Bedarf vor der weiteren Verarbeitung korrigiert werden.
Datenaufbereitung (Vorbereitung für die Migration, z. B. Datenformate)	Datenbestände können i.d.R. nicht direkt übernommen werden. Eine Aufbereitung der Daten bzw. das Festlegen von Transformationsregeln sind daher notwendig. Es bietet sich an, Transformationsregeln (alter Wert ➜ neuer Wert) im alten System zu pflegen, da die Benutzer dabei nicht auf ein weiteres System geschult werden müssen. Auch bietet diese Bearbeitung die Möglichkeit, Datenbestände zu harmonisieren.
Datentransformation	Beschreibung der Datentransformation unter Verwendung der aufbereiteten Daten und der verwendeten Programme.
Datenverifizierungsstrategie und Akzeptanzkriterien (Migrationstest)	Beschreibung der Datenverifizierungsstrategie (qualitative und quantitative Prüfung) und Akzeptanzkriterien (Testumfang) und Umgang mit Abweichungen.
Durchführung und Dokumentation der Aktivitäten	Durchführung der Migrationsaktivitäten und Dokumentation in Migrationsprotokollen. Aufnahme von Beobachtungen während der Durchführung.

System- und Akzeptanztest planen, durchführen und abschließen

Bereits im Kapitel 3.3 *Das „V-Modell“* wird auf die unterschiedlichen Testphasen hingewiesen:

- Modul- und Integrationstests erfolgen beim Lieferanten. Damit wird sichergestellt, dass das System gemäß der Spezifikation entwickelt wurde.
- Mit System- und Akzeptanztests auf der Seite der Benutzer wird geprüft, ob das richtige computergestützte System für den spezifizierten Zweck im operativen Geschäft unter den spezifizierten Bedingungen arbeitet.

Auszug Kapitel 3.3 *Das „V-Modell“*

Beim **Systemtest** (*Functional Test*) wird das Programm gegen die Funktionale Spezifikation (Systemspezifikation) geprüft. Dabei wird das System als Ganzes durch den Systementwickler oder durch Fachpersonen, die sich mit dem System sehr gut auskennen, geprüft.

- Beispiel: Ist der Passwortschutz modal? Falsche Eingaben, Abbruch der Funktion, weitere Funktionsprüfungen.
- Beispiel: die Prüfung der korrekten Funktionsweise eines Chromatographiedatenmanagementsystems nach Installation durch die Lieferfirma beim Kunden.

Im **Akzeptanztest** (*Requirements Test*) wird das System durch die Benutzer gegen die Benutzeranforderungen geprüft. Das kann man auch als „Black-Box-Test“ bezeichnen, denn der Benutzer kennt in den allermeisten Fällen den Quellcode nicht. Es ist hier unbedingt zu betonen, dass diese Prüfung nur durch die Benutzer und nicht durch Lieferanten oder sonstige externe Spezialisten durchzuführen ist. Wie kann ansonsten sichergestellt werden, dass die Benutzer mit dem System zufrieden sind?

- Beispiel: Ist der Passwortschutz vorhanden?

Art und Umfang des System- und Akzeptanztests erfolgen entsprechend der Maßnahmen der Risikobewertung. Die Tests haben zwar unterschiedliche Fragestellungen (s.o.), können aber in einem Testpaket kombiniert werden.

Die Dokumentation des System- und Akzeptanztests kann über nachfolgende Dokumentenstruktur erfolgen:

- Testplan
- Testspezifikation
- Testprotokolle
- Testbericht

auftritt. Ein längeres RPO akzeptiert größere Datenverluste, was in manchen Fällen tolerierbar ist, aber in anderen Fällen (z. B. bei kritischen Produktionsdaten) nicht akzeptabel wäre.

In validierten computergestützten Systemen ist die RPO besonders wichtig, da Datenverluste die Datenintegrität und Compliance beeinträchtigen können. Die Backups müssen so geplant werden, dass alle kritischen Daten gesichert sind und potenziell verlorene Daten (im Falle eines Ausfalls) minimiert werden.

Beispiel:
Ein RPO von 1 Stunde bedeutet, dass im schlimmsten Fall Daten von maximal einer Stunde verloren gehen können. Um dies zu erreichen, müssten stündliche Backups oder kontinuierliche Datensicherungen durchgeführt werden oder redundante System vorgehalten werden.

Bedeutung für validierte Systeme

RTO und RPO müssen im pharmazeutischen Umfeld besonders sorgfältig festgelegt werden, da die Wiederherstellungszeiten und der Datenverlust direkte Auswirkungen auf die Produktqualität, die Patientensicherheit, die Datenintegrität und die Einhaltung regulatorischer Anforderungen haben. Abbildung 6-3 vergleicht die unterschiedlichen Aspekte von RTO und RPO.

Kurze RTO und kurze RPO-Werte sind bei GMP-relevanten Systemen oft notwendig, da ein längerer Ausfall oder Datenverlust kritische Auswirkungen auf die Dokumentation und Produktionsprozesse haben könnte. Der Disaster Recovery Plan (DRP) sollte klare Vorgaben für die Backup- und Wiederherstellungsstrategien enthalten, um sicherzustellen, dass die festgelegten RTO- und RPO-Ziele erreicht werden.

Abbildung 6-3 Vergleich von RTO und RPO

Aspekt	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)
Definition	Maximale Zeitspanne, in der ein System nach einem Ausfall wiederhergestellt werden muss.	Maximale Zeitspanne, die seit dem letzten Backup vergangen sein darf. Tolerierter Datenverlust.
Fokus	Zeit, die für die Wiederherstellung eines Systems benötigt wird.	Datenverlust, der im Falle eines Systemausfalls akzeptabel ist.
Geschäftsbezug	Betriebsunterbrechung und Downtime.	Datenverlust und Backup-Häufigkeit.
Ziel	Minimierung der Ausfallzeit.	Minimierung des Datenverlusts.
Auswirkung auf Planung	Bestimmt, wie schnell ein Backup oder eine Wiederherstellung durchgeführt werden muss, um ungeplante Ausfallzeiten zu reduzieren.	Bestimmt, wie oft Backups durchgeführt werden müssen, um den maximal tolerierbaren Datenverlust zu minimieren.

Beide Kennzahlen sind entscheidend, um den Backup- und Wiederherstellungsprozess effektiv zu planen und zu implementieren, insbesondere in Bereichen, in denen Datenintegrität und Compliance höchste Priorität haben.

6.3.4 Systemüberwachung

Die Überwachung von GMP-relevanten computergestützten Systemen ist gemäß ISPE GAMP® 5 2nd Edition und seinen Appendizes ein zentraler Bestandteil des systematischen Lebenszyklus-Managements. Die Überwachungsmaßnahmen dienen dazu, die kontinuierliche Konformität, Integrität und Zuverlässigkeit der Systeme sicherzustellen und sicherheitsrelevante Abweichungen frühzeitig zu erkennen. Die 2nd Edition verstärkt dabei den risikobasierten Ansatz und bietet detaillierte Vorgehensweisen zur Implementierung effektiver Überwachungsstrategien.

Der ISPE GAMP® 5 2nd Edition stellt heraus, dass GMP-relevante computergestützte Systeme über den gesamten Lebenszyklus hinweg überwacht werden müssen, um die Einhaltung regulatorischer Anforderungen sicherzustellen. Die Überwachungsanforderungen gelten für alle Phasen des System-Lebenszyklus, von der Implementierung bis zur Stilllegung, und sollen sicher-

11 Autoren

Markus Roemer
markus.roemer@comes-services.com

Dipl. Ing., Berater
comes compliance services, Ravensburg

Markus Roemer arbeitet als unabhängiger Berater bei comes compliance services in Ravensburg. Sein Themenspektrum ist vielseitig und umfasst u. a. die Validierung computergestützter Systeme, Auditing, Qualitätsmanagement, Projektmanagement und Compliance Management. Seit 2008 engagiert er sich als Botschafter für das Chapter Deutschland, Österreich und Schweiz bei der ISPE.

Nach dem Ingenieurstudium hat Herr Roemer seine berufliche Laufbahn als Teammitglied der Computervalidierung bei der Vetter Pharma-Fertigung in Ravensburg begonnen. Nach einem Wechsel zum MES-Systemanbieter Propack Data GmbH in Karlsruhe war er dort als Quality Manager für EBR-Projekte tätig.

2003 wechselte Herr Roemer als Senior Validation Consultant zu Invensys Validation Technologies in Montreal, Kanada und begleitete globale IT- und Validierungsprojekte im Ausland. Bei der Firma Systec & Services konnte er anschließend seine globalen Kunden- und Lieferantenerfahrungen als Leiter des Compliance Services und Qualitätsmanagements einbringen.

Dr. Dennis Sandkühler
Dennis.Sandkuehler@digital-ls.de

Ingenieur, Informatiker
Digital Life Sciences GmbH, Gescher

Dr. Dennis Sandkühler verantwortet das Qualitätsmanagement bei der Digital Life Sciences GmbH. Er ist zuständig für die Einführung von GxP-relevanten Softwarelösungen und die Computersystemvalidierung in Kundenprojekten. Zuvor war er in der Entwicklung und Zulassung von Medizinprodukten tätig. Herr Dr. Sandkühler ist Mitglied der ISPE D/A/CH und Autor zahlreicher Fachpublikationen.

Während des Ingenieurstudiums der Medizintechnik und Promotion in Angewandter Mathematik und Informatik begann Herr Sandkühler seine berufliche Laufbahn mit der Entwicklung von Software für medizinische Bildgebungsverfahren. In seiner weiteren beruflichen Laufbahn entwickelte er marktreife Medizinprodukte und war durch die Qualifizierung als *Manager Regulatory Affairs International* für die Zulassung im internationalen Markt mitverantwortlich.

Herr Sandkühler hat durch seine Zertifizierung als *Project Management Professional (PMI)* eine hohe Projektkompetenz, die er in seine aktuelle Tätigkeit bei der Digital Life Sciences GmbH einbringt. Schwerpunkte der Digital Life Sciences GmbH sind Softwarelösungen für die produktionsbegleitende Dokumentation der Herstellung und des Qualitätsmanagements.

Herr Sandkühler hat zahlreiche internationale Projekte zur Einführung von Softwaresystemen in der Medizintechnikbranche, in Laboreinrichtungen und der pharmazeutischen Industrie geleitet und berät und unterstützt Unternehmen bei der Computersystemvalidierung.

Dr. Siegfried Schmitt
Siegfried.Schmitt@parexel.com

Chemiker
Vice President Technical, PAREXEL Consulting

Dr. Siegfried Schmitt berät Hersteller von Medizinprodukten und die pharmazeutische Industrie zu allen Aspekten der Regelkonformität, insbesondere in den Bereichen Gestaltung und Implementierung von Qualitätsmanagementsystemen und wettbewerbsorientierter Compliance. Sein erklärtes Interesse gilt zuverlässigen, wirksamen und effizienten Qualitätssystemen zum Sicherstellen der Compliance und nicht zuletzt der Datenintegrität.

Seine Karriere begann Dr. Schmitt 1989 in der Schweiz bei Roche in Basel als leitender Produktionschemiker. Danach folgten Stationen bei Raytheon als Validierungsmanager, bei ABB als leitender Hauptberater und bei GE Healthcare als globaler Direktor Qualität, ehe er zu PAREXEL stieß.

Dr. Schmitt ist erfolgreicher Autor und Herausgeber. Er ist Mitglied im Redaktionsbeirat von BioProcess International, Pharmaceutical Technology und RAPS Focus.

Für die PDA engagiert sich Dr. Schmitt als Mitglied im wissenschaftlichen Beirat und als Präsident des PDA Chapters in Großbritannien. Er ist außerdem aktives Mitglied in weiteren Industrieverbänden und Fellow der Königlichen Gesellschaft für Chemie.

Dr. Peter Schober
peter.schober@gempex.com

Diplom-Chemiker
Gempex GmbH, Mannheim

Herr Dr. Schober ist Principal Consultant bei der gempex GmbH und berät Kunden der Life Science Industrie in den Bereichen IT-Compliance, Computersystem-Validierung und Organisation.

Nach der Promotion im Fach Chemie 1997 und einem Forschungsaufenthalt in den USA begann Herr Dr. Schober seine Berufslaufbahn in einer mittelständischen IT-Unternehmensberatung. Neben der Y2K-Umstellung war sein Arbeitsgebiet die Applikationsentwicklung für die Bereiche Controlling, Logistik, CRM und Klinikinformationssysteme bei einem großen Life-Science-Konzern.

Ab 2005 arbeitete er als Produktmanager und Validierungsbeauftragter für einen LIMS-Hersteller. Es folgten Tätigkeiten als Leiter der Qualitätssicherung beim Aufbau eines In-vitro-Diagnostika Start-up und als Senior Consultant für CSV-Projekte bei Pharma- und Medizinprodukte-Herstellern, Organisation, Prozessmanagement und IT-Lieferanten-Auditierung.

Herr Dr. Schober ist zertifizierter Auditor für Medizingeräte-Software und als Autor und Referent tätig.

Er ist stellvertretender Leiter der GAMP-DACH Special Interest Group „*GAMP for Medical Devices*“.

Dr. Markus Veit
m.veit@alphatopics.de

Apotheker
Alphatopics GmbH, Kaufering

Prof. Dr. Markus Veit ist Gründer und Geschäftsführer der ALPHATOPICS GmbH in Kaufering. Außerdem ist er Mitglied im Ausschuss Pharmazeutische Chemie der deutschen Arzneibuchkommission. Im Rahmen seiner akademischen Lehrtätigkeit hält er Vorlesungen an den Universitäten Frankfurt und Berlin.

Nach dem Studium der Pharmazie in Frankfurt promovierte Herr Veit bis 1990 an der Julius-Maximilians-Universität in Würzburg und habilitierte dort 1997. Er ist Fachapotheker für Pharmazeutische Analytik. In den vergangenen 30 Jahren war er als Geschäftsführer in Dienstleistungsunternehmen für die Pharmazeutische Industrie mit den Schwerpunkten Arzneimittelentwicklung, -herstellung, -prüfung und -zulassung tätig. Gleichzeitig konzipierte und leitete er zahlreiche Fort- und Weiterbildungsveranstaltungen für Mitarbeitende der Arzneimittel- und Medizinprodukteindustrie.

Bibliographische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie, detaillierte bibliographische Daten sind online über die Website der Deutschen Nationalbibliothek abrufbar.

ISBN: 978-3-95807-315-9

4. Auflage 2025

Der Inhalt ist ein Auszug aus dem GMP-BERATER, dem größten GMP-Wissensportal weltweit.

GMP-Verlag Peither AG
Karlstraße 2
79650 Schopfheim
Deutschland

Telefon +49 7622 66686-70
E-Mail: service@gmp-verlag.de
www.gmp-verlag.de

UStID-Nr. DE 251226929
HRB 700572 Amtsgericht Freiburg im Breisgau
Vorstand: Barbara Peither, Michael Lammel
Aufsichtsrat: Thomas Peither (Vorsitz)

Herausgeben von: Barbara Peither, GMP-Verlag Peither AG
Redaktion: redaktion@gmp-verlag.de
Umschlaggestaltung: Diana Sutter, GMP-Verlag Peither AG
Titelfoto: Bildagentur Fotolia
Satz: Computrain Marcus Bollenbach, Staufen