2009

EINE RISIKOBASIERTE METHODE FÜR IMPLEMENTIERUNG UND BETRIEB VON GMP KONFORMER IT INFRASTRUKTUR AM BEISPIEL USER- UND IDENTITY MANAGEMENT

Peter Brandstetter
CSC

Barbara Ginda
Intercell

Stefan Tautscher
Intercell

EINE RISIKOBASIERTE METHODE FÜR IMPLEMENTIERUNG UND BETRIEB VON GMP KONFORMER IT INFRASTRUKTUR AM BEISPIEL USER- UND IDENTITY MANAGEMENT

Peter Brandstetter[1], Barbara Ginda, Stefan Tautscher[2]

Kurzfassung
Pharmazeutische Betriebe unterliegen besonderen rechtlichen Vorgaben für das Qualitätsmanagement. Dies gilt sowohl für die Produktion als auch für IT Systeme, die für die Produktion verwendet werden. Die Einhaltung wird von nationalen und internationalen Behörden (FDA, EMEA) überprüft. Der vorliegende Aufsatz beschäftigt sich mit diesen Vorgaben und deren Anwendung auf IT Infrastruktur, wobei ein risikobasiertes Vorgehen im Allgemeinen vorgestellt wird und spezifische Probleme bei der Umsetzung am Beispiel einer zentralen Benutzervergabe diskutiert werden.

1 Vorwort

Pharmaunternehmen unterliegen in ihrer Arbeit strengen behördlichen Auflagen, die darauf abzielen, die Gefährdung der Patienten durch fehlerhafte bzw. qualitativ minderwertige Arzneimittel zu minimieren. Ziel der zuständigen Behörden wie etwa der FDA (Food and Drug Administration, Arzneimittelzulassungsbehörde der Vereinigten Staaten) oder der Europäischen Kommission ist es, durch strenge Vorschriften und regelmäßige Kontrollen, so genannten Inspektionen, sicherzustellen, dass das Pharmaunternehmen ein ausreichend gutes und ausgereiftes Qualitätsmanagementsystem nach den Vorgaben der Guten Herstellungspraxis (Good Manufacturing Practice - GMP[3]) besitzt und dieses bei der Herstellung seiner Produkte auch befolgt.

Ein Bestandteil jedes Qualitätsmanagementsystems das sich an den Richtlinien der guten Herstellpraxis orientiert, ist das Instrumentarium der „Validierung“, also die Prüfung einer These durch Bereitstellung eines objektiven Nachweises. Vereinfacht gesagt, dient der Prozess einer Validierung dazu, sicherzustellen, dass ein Prozess oder eine Methode den vom Benutzer definierten Spezifikationen entspricht.

Ebenfalls zu erwähnen ist in diesem Zusammenhang der Begriff der Qualifizierung von Geräten. Unter Qualifizierung versteht man die Beweisführung, dass Ausrüstungsgegenstände einwandfrei arbeiten und tatsächlich zu den erwarteten Ergebnissen führen.

---

[1] CSC
[2] Intercell
[3] Neben GMP gibt aus es auch noch andere Vorgaben, die im Allgemeinen unter dem Kürzel GxP zusammengefasst werden.

Die im pharmazeutischen Bereich übliche behördliche Definition der Begriffe Validierung bzw. Qualifizierung lässt sich jedoch auch auf den IT Bereich anwenden. Im Allgemeinen wird die dokumentierte Prüfung der Tauglichkeit von Computersystemen als Computervalidierung bezeichnet. Innerhalb der Computervalidierung wiederum unterscheidet man meist zwischen Softwarevalidierung und Hardwarequalifizierung. Bei Softwarevalidierungsprojekten liegt der Fokus auf der Prüfung der Tauglichkeit der Software hinsichtlich ihrer Unterstützung für den abzubildenden Geschäftsprozess. Hardwarequalifizierung dient der Tauglichkeitsprüfung der Geräteteile, die für den Einsatz einer Anwendungssoftware notwendig sind. Um also eine Software validieren zu können, muss zuvor die zugrunde liegende Hardware qualifiziert werden.
In dem hier vorliegenden Aufsatz wird eine Methode für die GMP konforme Implementierung und den Betrieb von IT Infrastruktur vorgestellt. Dabei wird nicht zwischen Software und Hardware unterschieden sondern zwischen Anwendungssoftware (Software, die Geschäftsprozesse unterstützt, wie ERP System, LIMS, etc.) und der dazu notwendigen zugrundeliegenden Infrastruktur.
Der Begriff IT Infrastruktur wird dabei folgendermaßen definiert:
„Gesamtheit aller Computersysteme eines Betriebes bestehend aus der Hardware, Netzwerkkomponenten, Betriebssoftware (jedoch ausgenommen der Geschäftsanwendungen) sowie die zugrunde liegenden Prozesse und Prozeduren, um den Betrieb der Computer Systeme gewährleisten zu können."

Die IT Infrastruktur Komponenten lassen sich in folgende 3 Kernbereiche unterteilen:

- Server: zentralisierte Hardware, das dort installierte Betriebssystem sowie unterstützende Infrastruktur Applikationen (Virenschutz, Datensicherung, etc.).
- Netzwerk: Router, Switches, Verkabelungs-Infrastruktur sowie unterstützende Infrastruktur Applikationen (Netzwerk- Verwaltungsprogramme, Firewalls, etc.)
- Clients: dezentrale Anwender-Hardware, die darauf installierten Betriebssysteme sowie unterstützende Infrastruktur Applikationen (z.B.: lokale Virenschutzprogramme).

Die Planung und Implementierung von IT Infrastruktur ist dem Software-Lebenszyklusmodell ähnlich im Unterschied zur Betriebsführung, wo Infrastruktur sehr häufigen Änderungen unterworfen ist. Der direkte Einfluss von Infrastruktur auf produktrelevante Daten ist jedoch vergleichsweise gering zu dem einer Anwendungssoftware. Daher ist nicht die Funktion einer einzelnen Komponente, sondern das Zusammenspiel und die richtige Konfiguration von entscheidender Bedeutung. Man spricht deshalb bei Infrastruktur nicht von „Validierung" sondern üblicherweise von „Under Compliance" [1] (unter Kontrolle durch Einhaltung von Verhaltensmaßregeln). „Under Compliance" bedeutet in diesem Zusammenhang, dass die Planung, Organisation, Installation, Verwendung und Verwaltung der IT Infrastruktur kontrolliert und dokumentiert wird.

2 Methode der IT Infrastrukturqualifizierung

In diesem Kapitel wird anhand eines Modells versucht eine Abgrenzung zwischen Infrastruktur und Anwendungssoftware zu schaffen, wobei die Infrastruktur in 2 Ebenen eingeteilt wird. Diese an sich künstliche Zweiteilung erfolgt, um für die unterschiedlichen Ebenen entsprechend ihrer Komplexität und daher schlussendlich ihres möglichen Fehlerrisikos andere Qualitätsstandards und –maßnahmen zu setzen.
Dieses hier vorgestellte Modell und die Vorgehensweise hinsichtlich Validierung/Qualifizierung ist das Ergebnis aus verschiedenen Projekte sowohl unterschiedlicher IT Umgebungen als auch unterschiedlich großer IT Abteilungen und basiert auf Industriestandards wie dem GAMP V-Modell [1] und ITIL [5].

Klassische Vorgehensmodelle

2.1.1 V-Modell

In der Computervalidierung gilt das V-Modell wie es auch im GAMP [1] als Basismodell verwendet wird, als quasi Standard. Auf der linken Seite, die als Entwurfsphase betrachtet werden kann unterscheidet man zwischen Anforderungsdefinition (auch Lastenheft oder User Requirements Specification = URS), funktionaler Spezifikation (auch Pflichtenheft oder Functional Specification = FS) und technischem Entwurf (DS = Design Specification).

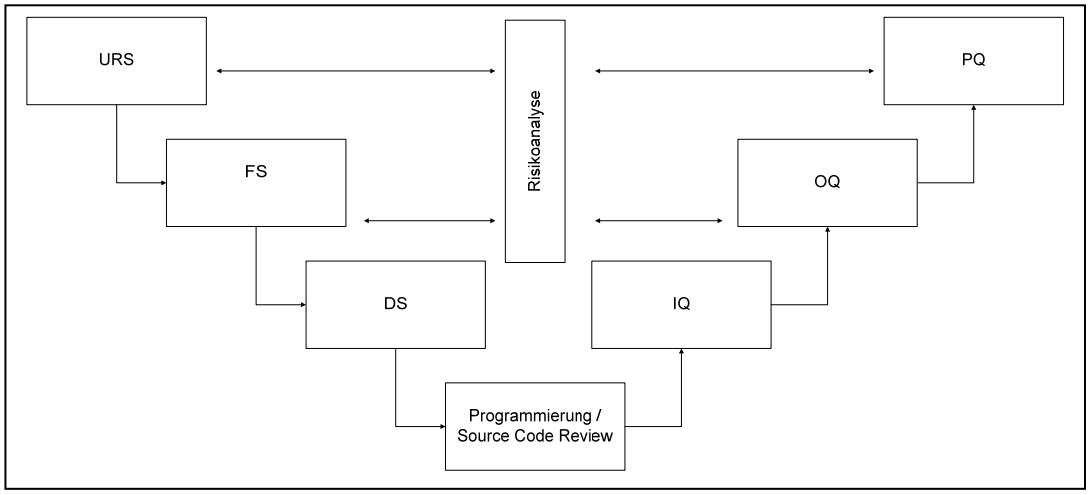

Abbildung 1: V-Modell nach GAMP

Jeder dieser Spezifikationsphasen steht eine Qualifizierungsphase (Testphase) gegenüber. Im Rahmen der Qualifizierung wird die korrekte Installation aller Komponenten (IQ = Installation Qualification), ein detaillierter Funktionstest (OQ = Operational Qualification) und ein Gesamttest des Produktivsystems (PQ = Performance Qualification) durchgeführt. Um den Detaillierungsgrad der Qualifizierungstests zu bestimmen, wird häufig auch eine funktionale Risikoanalyse durchgeführt (siehe auch Kapitel 2.1.3).
Das V-Modell ist ein sehr allgemein gültiger Rahmen, der durchaus auch verschiedenste Softwareentwicklungsmethoden, wie z.B.: Spiralmodell, extreme Programming, etc. zulässt.

2.1.2 ITIL

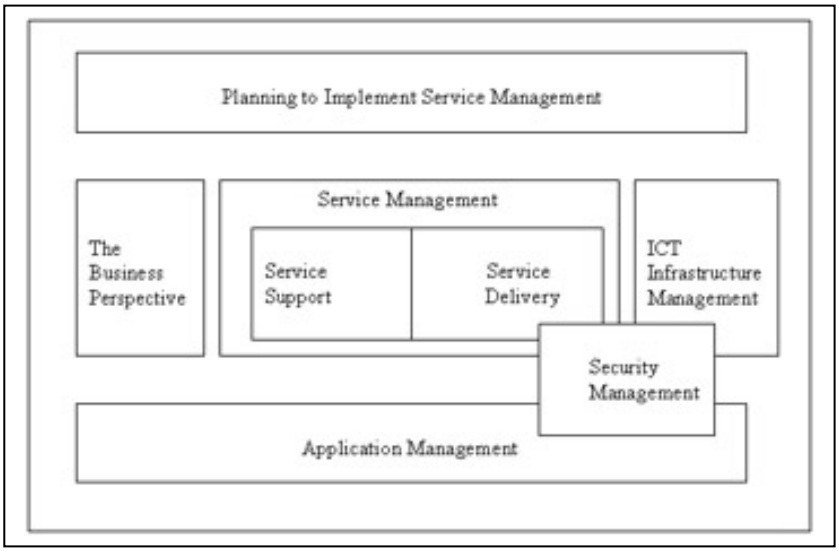

Abbildung 2: Management Strategien nach ITIL V2

Im Bereich Infrastrukturmanagement wird in der Praxis häufig ein an ITIL [5] angelehntes Modell angewendet. In Abbildung 2: Management Strategien nach ITIL V2 eine Übersichtsdarstellung der vom ITIL Modell abgedeckten Prozesse.
Sowohl das V-Modell, als auch die ITIL Prozesse bilden die Basis für die hier vorgestellte Infrastrukturqualifizierung.

Qualifizierung von IT Infrastruktur

2.1.3 Risikobetrachtung – Risiko Management

Da die Validierung von IT einen nicht unerheblichen Aufwand bedeutet, hat sich ein risikobasiertes Verfahren etabliert, wo der Aufwand der Qualitätssicherungsmaßnahmen in Relation zu dem möglichen Einfluss einer Funktion oder einer Komponente auf die Qualität des pharmazeutischen Produktes bzw. das Leben des Patienten gestellt wird. Es gilt also, je mehr eine Funktion bzw. eine Komponente das zu produzierende Arzneimittel beeinflusst, desto besser muss auch dessen korrekte Funktionsweise abgesichert werden.

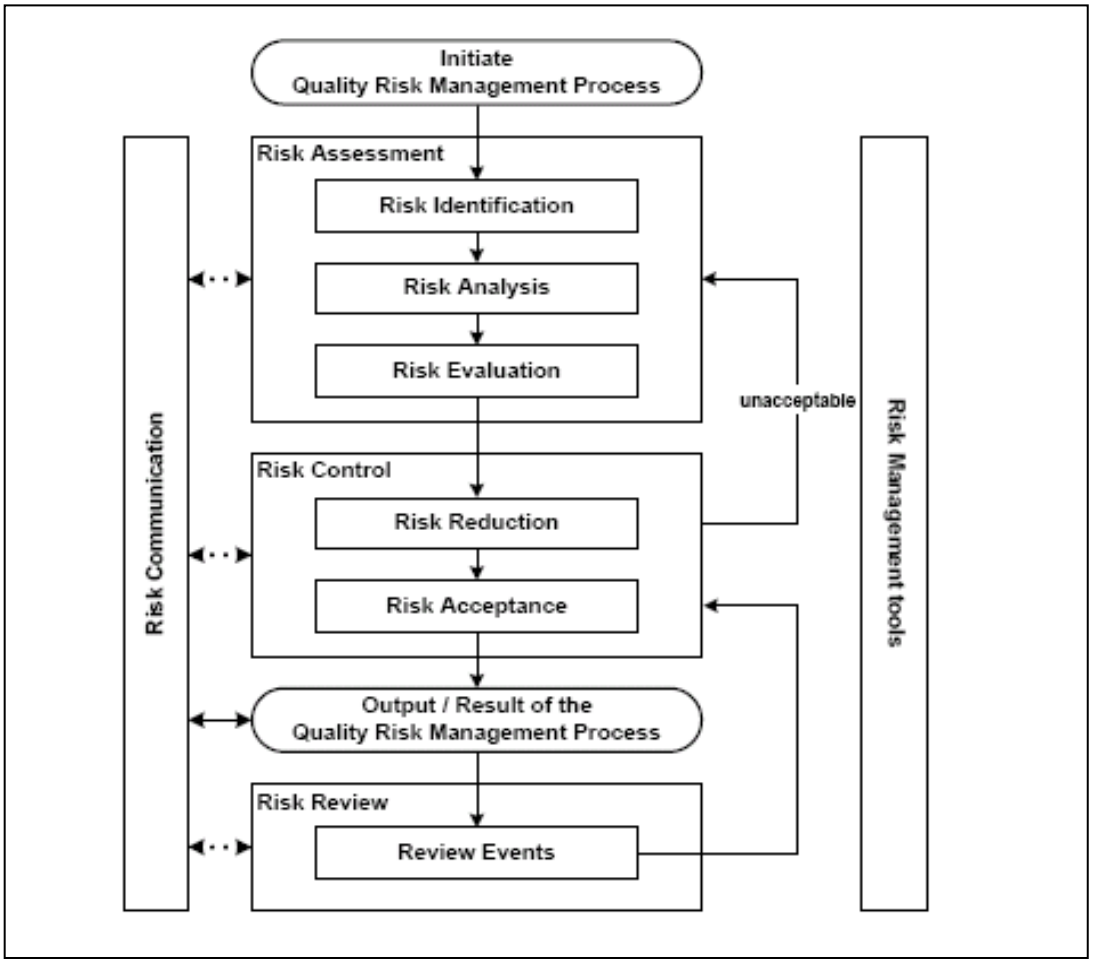

Abbildung 3: Risikomanagement nach ICH Q9

Risk Management ist als ein ständig begleitender Prozess zu sehen. Sowohl in der Entwurfsphase und der Implementierung, als auch im Betrieb werden mögliche Risiken betrachtet und entsprechende Maßnahmen (z.B.: redundante Server oder detaillierte Funktionstests) zur Risikominimierung gesetzt. In Abbildung 3: Risikomanagement nach ICH Q9 [4] ist ein allgemein üblicher Riskomanagement Prozess dargestellt.

2.1.4 Modell einer Infrastrukturqualifizierung

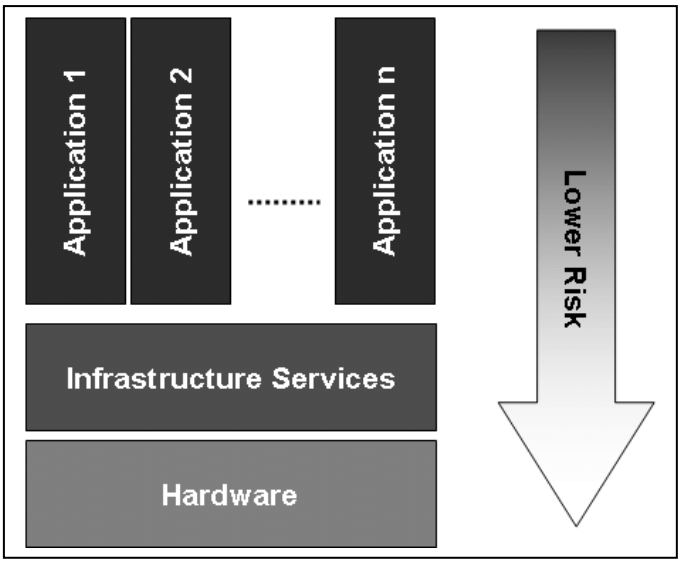

Abbildung 4: Infrastruktur Qualifizierungsmodell

Das wesentliche Ziel der Computervalidierung ist es, zu gewährleisten, dass IT Systeme, welche die Qualität der Medikamentenproduktion und somit die Gesundheit des Patienten gefährden könnten, korrekt funktionieren. Mit Risikomanagement werden die Qualitätssicherungsmaßnahmen auf die Bereiche konzentriert, die höheren Einfluss auf die Qualität des pharmazeutischen oder medizintechnischen Produktes haben.
Betrachtet man nun die unterschiedlichen Komponenten einer typischen IT Landschaft, so ist aus dem Gesichtspunkt der Computervalidierung heraus eine Aufteilung in Applikation und Infrastruktur sinnvoll (siehe Abbildung 4: Infrastruktur Qualifizierungsmodell), da auf Applikationsebene noch sehr deutlich die Kritikalität einer Applikation von einer anderen hinsichtlich der Patientensicherheit unterschieden werden kann, und natürlich auch auf funktionaler Ebene innerhalb einer bestimmten Applikation. Gerade bei Hardware und vor allem zentralen Komponenten, wie Server, virtuelle Server, Netzwerk, SAN, etc, wo eine physische Einheit unterschiedliche Applikationen bedient, ist diese Vorgehensweise nicht mehr möglich. Andererseits ist in dieser Risikobetrachtung auch der Grad an Standardisierung zu berücksichtigen und auch die Fehlertoleranz einer Komponente. Aufgrund von deutlich höherer Standardisierung, die allein durch das mögliche Zusammenspiel von Komponenten unterschiedlicher Hersteller notwendig ist und auch nachdrücklicher verfolgt wird (z.B.: Festplatten unterschiedlichster Hersteller funktionieren in einem PC), kann Hardware weniger fehleranfällig eingestuft werden, als etwa eine individuell erstellte Software. Außerdem besitzen Hardware und auch z.B.: Netzwerkprotokolle üblicherweise sehr robuste Fehlerkorrekturmechanismen, oder zumindest Fehlererkennungsfunktionen, was das mögliche Risiko eines unerkannten Fehlverhaltens noch weiter senkt.
Ähnlich gelagert sind Infrastrukturdienste, die unterschiedlichen Applikationen zur Verfügung stehen, wie z.B.: Dateisystem, Druckdienste, Netzwerkprotokolle, etc. In unserem Qualifizierungsmodell verstehen wir unter dem Begriff Infrastrukturdienste jene Software, die nicht ausschließlich von einer Applikation genutzt wird, sondern vielmehr so gebaut ist, dass viele unterschiedliche Anwendungen sich ihrer Funktionen bedienen. Schon durch diesen Umstand müssen solche Dienste robuste gut definierte Schnittstellen aufweisen, die auch eine Fehlerkorrektur oder -erkennung ermöglichen. Weiters sind in unserer Betrachtung Infrastrukturdienste als Standardkomponenten anzusehen, die sich einer großen Verbreitung erfreuen. Aufgrund des hohen Verbreitungsgrades ist die Wahrscheinlichkeit, dass Fehler schnell

erkannt werden sehr hoch. Bei der Qualifizierung von Infrastrukturdiensten ist jedoch eine gesonderte Risikobetrachtung für jeden Dienst sinnvoll und abhängig davon die Teststrategie festzulegen. Zusätzlich wird die Funktionalität der Hardware und von Infrastrukturdiensten auch bei der Überprüfung der Applikation implizit mitgetestet.
Aus diesen Umständen heraus ist ein detaillierter Funktionstest von Hardware und Infrastrukturdiensten nicht notwendig, vielmehr ist es wichtig, korrekte Installation und Konfiguration sicherzustellen und zwar nicht nur zum Zeitpunkt der Inbetriebnahme, sondern auch über den gesamten Lebenszyklus hinweg (siehe auch 0).
Vor allem wenn IT als einziges Medium für die Aufzeichnung und Archivierung von produktionsrelevanten Daten verwendet wird, ist eine sichere und korrekte Langzeitspeicherung dieser elektronischen Daten zu gewährleisten. Eine gute Backup und Archivierungsstrategie ist daher unumgänglich, wie auch ein Disaster Recovery Konzept (z.B.: in Anlehnung an die IT-Grundschutzkataloge des deutschen Bundesministeriums für Informationssicherheit [3]).
Im Gegensatz zur Sicherung korrekter Funktionalität bei der Validierung von Software ist daher der Fokus bei Qualifizierung von Infrastruktur auf korrekte Installation und Konfiguration und sichere Betriebsführung zu legen.
Um dies zu gewährleisten ist auf Basis eines verkürzten V-Modelles der folgende Prozess sinnvoll (Abbildung 5: Qualifizierungsprozess).

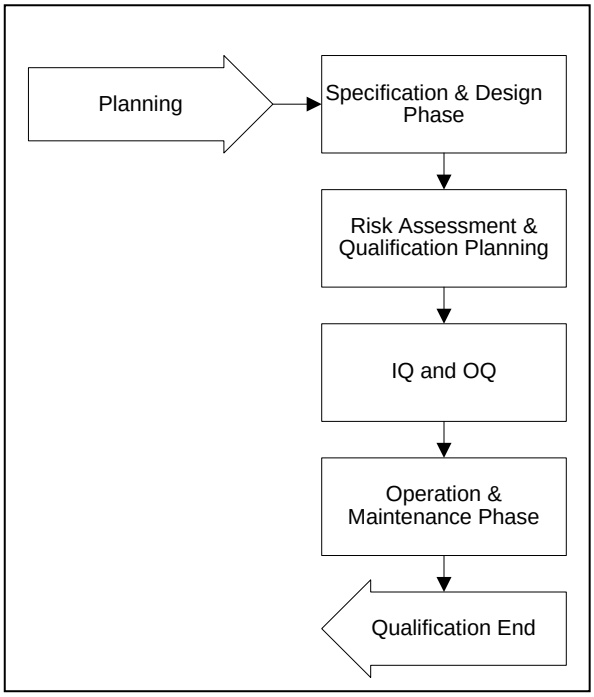

Abbildung 5: Qualifizierungsprozess

2.1.5 Specification & Design Phase

Ähnlich wie bei Geschäftsanwendungen sind die Anforderungen an die Infrastruktur noch systemunabhängig zu definieren. Vor allem Sicherheitsaspekte wie Datensicherheit und Zugriffssicherheit sind dabei zu beachten, aber auch Kapazitative wie Datenmengen, Antwortzeiten, etc.
Ausgehend von den Anforderungen wird dann sowohl die entsprechende Hardware ausgewählt, als auch Konfigurationsparameter für Dienste bestimmt. Dabei ist natürlich auch die vorhandene Infrastruktur mit einzubeziehen. Schon beim Design von Infrastruktur empfiehlt es sich, Risikomanagementwerkzeuge anzuwenden, um wichtige Parameter zu dokumentieren, und sicherzustellen, dass diese auch in der Designphase nicht vergessen werden. Für kritische

Parameter ist eine Festlegung vor der Installation notwendig, denn nur so kann erreicht werden, dass durch die Durchsicht von Dokumenten eine entsprechende fachliche Überprüfung des Designs erfolgt und auch in Form von Testprotokollen die echte Konfiguration der Infrastruktur mit den geplanten Werten übereinstimmt.
Standardisierter Checklisten und Dokumentationsvorlagen für unterschiedliche Komponenten (z.B.: Vorlage für Design eines Windows Servers) erleichtern diese Phase.

2.1.6 Risk Assessment & Qualification Planning

Die Überprüfung bei der Installation und Konfiguration beschränkt sich auf eben die im Design festgelegten kritischen Parameter. Ob eine Konfiguration nur durch Prüfen der Einstellung oder auch durch Testen der entsprechenden Funktion verifiziert wird, hängt von der Komplexität der Einstellungsmöglichkeit und der Kritikalität der Komponente ab und wird über eine Risikoanalyse bestimmt.
Ein weiterer wesentlicher Faktor, der eine reibungslos funktionierende Infrastruktur ermöglicht, ist die richtige Qualifikation der Administratoren. Es ist daher auf entsprechende Ausbildung eigener Mitarbeiter oder Nachweise von Drittfirmen zu achten.

2.1.7 IQ & OQ

Nach Abschuss der Planung der durchzuführenden Tests erfolgt nun die dokumentierte Installation (IQ = Installation Qualification) und die Funktionsüberprüfung (OQ = Operational Qualification). Es muss darauf geachtet werden, dass alle durchgeführten Schritte nachvollziehbar dokumentiert werden, da vor allem diese Dokumentation den Nachweis liefert, der im Rahmen von Behördeninspektionen geprüft wird.

2.1.8 Operation & Maintenance

Nach Abschluss der Tests kann die Infrastruktur verwendet werden. Aus Qualitätssicht sind dabei vor allem Fehler- und Änderungsmanagement wichtig, die im folgenden Unterkapitel beschrieben wird.

2.1.9 Traceability

Dass auch alle im Design festgelegten Vorgaben geprüft werden wird über die sogenannte Rückverfolgbarkeit (Traceability) garantiert. Diese kann entweder in einem eigenen Dokument erfolgen, oder aber auch in allen Phasendokumenten enthalten sein.

Fehler- und Änderungsmanagement

Neben der kontrollierten Installation/Konfiguration von Infrastruktur ist der sichere Betrieb ein wichtiges Qualitätsmerkmal. Industriestandardmodelle wie ITIL bieten sehr detaillierte Methoden für den sicheren Betrieb von Infrastruktur. Hier sollen nur die wichtigsten Aspekte der zwei wesentlichsten Prozesse (Fehler- und Änderungsmanagement) erläutert werden, um den Anforderungen einer qualifizierten Infrastruktur nach FDA und GMP zu genügen.

2.1.10 Fehlermanagement

Um mögliche Fehlfunktionen erstens zu erkennen und zweitens entsprechend der Kritikalität zu beheben, sind folgende Dinge zu beachten:

1. definierter Fehlermeldungsprozess (Helpdesk)
2. Fehlerqualifizierung
3. nachvollziehbare Fehlerbehebung

Um langfristig die Fehlerzahl zu senken, ist präventives Fehlermanagement ein probates Mittel. Dabei werden periodisch durch Analyse der gemeldeten Fehler Präventivmaßnahmen abgeleitet und umgesetzt.

2.1.11 Änderungsmanagement

Im Gegensatz zum Fehlermanagement, geht es bei Änderungsmanagement um die kontrollierte Umsetzung von Änderungen und nicht der Behebung eines Fehlverhaltens. Dabei ist zwar ein ähnlicher Prozess zu durchlaufen, jedoch ist zusätzlich noch eine Genehmigung vor der Durchführung einzuplanen und die bereits bestehende Dokumentation anzupassen.
Konsequentes Änderungsmanagement ist für eine kontrollierte Infrastruktur unumgänglich. Andernfalls wird innerhalb kürzester Zeit aufgrund von nicht qualitätsgesicherten Anpassungen die gesamte Infrastruktur destabilisiert.

Automatisierungswerkzeuge

Durch die bereits erwähnte Häufigkeit der Änderungen bei Infrastruktur entsteht eine Flut an Daten, die sich ohne geeignete Automatisierung der Verwaltung der Daten nicht bewältigen lässt. Der Einsatz von computergestützten Systemen (Tools) zur Verwaltung der Infrastruktur darf jedoch zu keiner Verminderung hinsichtlich der Einhaltung von GxP-Richtlinien führen.
Dies würde bedeuten, dass Software zur Automatisierung von Infrastruktur-Prozessen im selben Ausmaß wie Geschäftsanwendungen validiert werden müssten.
GAMP 5 [1] schlägt jedoch ein anderes Vorgehen vor. Für sogenannte „Infrastruktur Software" (Netzwerküberwachungs-, Anti-Virus- und Konfigurationsverwaltung – Software, etc.) ist keine vollständige Validierung vorgeschrieben. Bei einfachen Tools, die „Out-of-the-Box“ ohne weitere aufwendige Konfiguration eingesetzt werden könnnen, genügt die kontrollierte und dokumentierte Installation (IQ) und ein einfacher Gesamttest der Funktionalität des Systems (PQ).
Begründet wird diese Vorgehensweise mit der Ansicht, dass Infrastruktursoftware keinen direkten Einfluss auf die Sicherheit des Patienten hat, also ein deutlich geringeres Risiko darstellt.

3 Beispiel: Benutzerverwaltung und Authentifizierung

Anhand des Beispieles Benutzerverwaltung und Authentifizierung werden wichtige Problemstellungen aus Sicht der risikobasierten IT Infrastrukturqualifizierung diskutiert, wobei der Schwerpunkt in der Darstellung der Anwendung von Risikomanagement liegt und daher detaillierte Schritte der Qualifizierung (Verification, Traceability, …) nicht explizit gezeigt werden. Das Risiko ist in diesem Fall der unbefugte Zugang zu Anwendungen den es weitestgehend zu verhindern gilt und den Anwendern dabei trotzdem höchstmöglichen Komfort zu gewähren.

Userverwaltung für Qualifizierungsrelevante Infrastruktur: Designüberlegungen

Im regulierten oder sicherheitskritischen Umfeld stellen sich zwei grundsätzliche Überlegungen unter der Betrachtung des oben genannten Risikos:

- Will man den Anwendern ohne zusätzliche gesonderte Authentifizierung Zugriff zu GxP relevanten System geben ?
- Wie kann eine, den Anforderungen hinsichtlich Flexibilität und GxP-Konformität entsprechende Userverwaltung mit einem zentralen Userverzeichnis hergestellt werden?

Diese beiden Fragen zielen auf die prinzipielle Designentscheidung hin: zentrale Authentifizierungsinfrastruktur (= als Infrastrukturdienst) vs. getrennte Systeme für GxP und nicht-GxP relevante Applikationen/Bereiche.

3.1.1 Zentrale Authentifizierung für GxP- und Nicht-GxP-relevante Systeme

Wird ein zentraler Authentifizierungsserver verwendet, der sowohl von GxP- als auch von nicht-GxP Anwendungen verwendet wird, so muss dieser zwangsläufig unter den strengeren GxP-

Richtlinen aufgesetzt und betrieben werden. Sämtliche Änderungen (z.B.: an den Rechten oder den Stammdaten) unterliegen dann dem Änderungsmanagement. Es muss aber auch möglich sein, dass nicht-GxP relevante Applikationen diesen Dienst verwenden können. Steht der Authentifizierungsserver etwa in einem getrennten Netzwerksegment, müssen entsprechende Anfragen zugelassen werden. In einfachen Systemen mag dies eine taugliche Möglichkeit darstellen, bei komplexeren Systemen, wenn beispielsweise auch Server aus einer DMZ Benutzer authentifizieren müssen (z.B.: Mail- oder Proxyserver) ist ein solches System aus sicherheitsrelevanten Aspekten nicht zielführend.

3.1.2 Getrennte Authentifizierungssysteme

Alternativ können für die verschiedenen Sicherheitsbereiche (als solches kann eine GxP-Landschaft betrachtet werden) unterschiedliche Authentifizierungsserver implementiert werden, im vorliegenden Beispiel also ein Directory für nicht-GxP relevante Anwendungen sowie ein eigenes für alle GxP-kritischen Anwendungen. Dieses Setup hat mehrere Vorteile:

- eigenes Login für den GxP-kritischen Bereich schafft Bewusstsein beim Benutzer (z.B.: Einhalten von SOPs erforderlich, …) ohne die grundsätzlichen Vorteile eines SSO (=Single Sign On Lösung) zu vernachlässigen (SSO jeweils innerhalb eines Bereiches),
- höherer Sicherheitsstandard durchsetzbar, da die Anzahl und Art der Applikationen normalerweise kleiner ist,
- keine Kommunikation zwischen GxP-Authentifizierungsserver und nicht-GxP Applikationen notwendig.

Um den letzten Punkt sicherzustellen ist es notwendig, dass die Geschäftsanwendungen nicht am Benutzerclient installiert werden (dieser kann auch in der Regel nicht zwei unterschiedliche Benutzerkonten verwalten). Das kann relativ einfach z.B.: dadurch erreicht werden, indem alle Applikationen auf einem Terminal Server (TS) bereitgestellt werden, welcher sich im GxP-Bereich befindet. Am Client muss nun lediglich sichergestellt werden, dass die Kommunikation zwischen TS-client und dem TS verschlüsselt wird.
Diese Variante hat allerdings einen Nachteil: Zwei verschiedene Server benötigen auch eine doppelte Benutzerverwaltung. Für die Benutzerkonten selbst sowie die reine Rechtevergabe (etwa Mitgliedschaft in verschiedenen Securitygruppen) mag dies kein allzu großer Nachteil sein, bei klassischen Stammdaten (etwa Telefonnummer, Emailadresse, Sozialversicherungsnummer, ...) ist die doppelte Pflege allerdings sehr mühsam und vor allem fehleranfällig.
Zudem müssen oft Applikationen (z.B.: ein ERP-System) auf beide Datenbestände zugreifen (da ja nicht jeder Benutzer zwangsläufig ein login am GxP-System benötigt). Damit existiert aber nun eine Anzahl an Benutzern mit doppeltem Login, was Berichte z.B.: hinsichtlich der tatsächlichen Mitarbeiterzahl (basierend auf dem am System existierenden Accounts) erschwert.

3.1.3 Identitymanagement vs. Accountmanagement

Eine Möglichkeit dem Problem der doppelten Stammdatenwartung beizukommen besteht darin, die unterschiedlichen Login- und Berechtigungsdaten (die Accounts) von den unveränderlichen Stammdaten (der Identity) zu trennen, d.h. man speichert alle personenbezogenen Daten auf einem getrennten System, dem „Identity Service“ und verknüpft lediglich mehrere System Accounts (z.B.: GxP- und nicht-GxP kritische Benutzerdaten) mit denen der physikalischen Person.
Attribute, wie Telefonnummer usw., die nicht mit den Benutzerkonten zusammenhängen werden im Identitymanagement-System gespeichert. Im Directory des Authentifizierungsservers verbleiben lediglich die Login- und Berechtigungsinformationen sowie ein Link zur Person im Identity Directory. Selbst für Systeme mit einem lokalen Authentifizierungsmechanismus kann ein solches Vorgehen genutzt werden wenn die entsprechenden Schnittstellen zur Verfügung stehen.

Je nach Art der Daten und Verwendungszweck muss entschieden werden, ob dieses System GxP-kritische Daten enthält oder nicht, im zweiten Fall kann dies auch von Personen, die nicht notwendigerweise eine Ausbildung im GxP-konformen Arbeiten besitzen (z.B.: die Personalabteilung) gewartet werden.
Speziell bei Internetapplikationen gibt es derzeit schon Ansätze eines zentralen Identitymanagements, welches von verschiedenen Diensten verwendet wird (exemplarisch sei z.B.: die yahoo liveID erwähnt), im Firmenumfeld gibt es zum derzeitigen Zeitpunkt leider noch kein System (zumindest „Out-of-the-box"), welches eine Unterteilung in Account- („usercredentials") und Identityinformationen (Stammdaten) ermöglicht. Dazu kommt, dass das zentrale Directory im Normalfall nicht alle Stammdaten einer Person erfasst (z.B.: Personaldaten), es zwar in den meisten Applikationen, die via zentralem Directory authentifizieren können, eine Verbindung zwischen Account- und Personentabelle gibt, diese im Regelfall jedoch als 1:1 Verbindung ausgeführt wird. Eine notwendige 1:n Verbindung (1 Personendatensatz für mehrere Systemaccounts) muss demnach meistens zusätzlich programmiert werden. Hinsichtlich der Validierung eines solchen Systems muss demnach mit einem größeren Aufwand gerechnet werden.

Fazit

Grundsätzlich können beim Design der Infrastruktur für GxP-relevante Applikationen mehrere Ansätze gewählt werden, wobei im Hinblick auf die Validierung des Gesamtsystems hierbei besonderes Augenmerk auf die Schnittstellen der Infrastruktur und der Systeme gelegt werden muss. Dies gilt im Besonderen für die Passwortauthentifizierung und Benutzerverwaltung: unterliegt die Verwaltung der Benutzerdaten keiner Kontrolle so kann das Gesamtsystem nie „Under Compliance" sein. Weiters unterliegen GxP-relevante Systeme typischerweise höheren Sicherheitsanforderungen, weshalb auch die Schnittstellen der Authentifizierungsserver nach außen hin (in Zonen mit niedrigeren Sicherheitsansprüchen oder -möglichkeiten) möglichst gering gehalten werden müssen. Duplizierung der Authentifizierungsinfrastruktur ermöglicht es hier, die Vorteile eines zentralen Directories elegant mit den Anforderungen diverser Regularien in Einklang zu bringen. Die doppelte Wartung von Stammdaten stellt in diesem Zusammenhang ein Problem dar, einfache und standardisierte Lösungen existieren hierfür noch nicht. Will man dem Mehraufwand einer doppelten Stammdatenwartung durch Schaffung eines Identity Management Systems entgehen ist in jedem Fall Individualprogrammierung vonnöten, die aber wiederum unter dem Risikoaspekt erhöhter Fehleranfälligkeit betrachtet werden muss.

4 Literaturverzeichnis

[1] International Society for Pharmaceutical Engineering (ISPE) (2008): GAMP 5. A risk-based approach to compliant GxP computerized systems

[2] ISPE: GAMP Good Practice Guide: IT Infrastructure Control and Compliance. ISPE (2005)

[3] Deutsches Bundesministerium für Informationssicherheit (2005): IT-Grundschutzkataloge. Standardwerk zur IT-Sicherheit. Köln: Bundesanzeiger-Verlag. BSI-Schriftenreihe.

[4] Food and Drug Administratio (FDA): Guidance for Industry – Q9 – Quality Risk Management. Rockville (June 2006)

[5] LATA, Arora; SHAILA Singh, POONAM Sharma: Managing Infrastructure using ITIL. Skill Soft Press (2007)