pharma technologie journal

Aktuelle Aspekte der Validierung computergestützter Systeme

von
Karl-Heinz Menges, Klaus Feuerhelm, Thierry P Dietrich, Martin Wolf, Frederike Gottschalk, Christian Baumgartner, Jürgen-F Hammer, Thomas Metzger, Anke Meyer, Jörg Schwamberger, Michaela Bühler, Sieghard Wagner, Thomas Linz, CONCEPT HEIDELBERG

1. Auflage

Aktuelle Aspekte der Validierung computergestützter Systeme – Menges / Feuerhelm / Dietrich / et al.

schnell und portofrei erhältlich bei beck-shop.de DIE FACHBUCHHANDLUNG

ECV Editio Cantor 2003

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 87193 298 4

Inhaltsverzeichnis: Aktuelle Aspekte der Validierung computergestützter Systeme – Menges / Feuerhelm / Dietrich / et al.

3. Gestaltung eines modernen Risikomanagement-Systems

Die Vision ist klar: Die verantwortliche Person im Pharmaunternehmen möchte ad hoc eine zuverlässige Aussage über den Zustand ihrer Computersysteme hinsichtlich des Grades der Erfüllung der FDA-Anforderungen erhalten. Sie möchte die derzeitigen Schwachstellen sehen, sie möchte erkennen können, welche Arbeiten zur Verbesserung der Konformität gerade im Gange sind und sie möchte das Risiko einschätzen können, was sie mit dem Betrieb der Computersysteme auf sich nimmt. Weiterhin möchte sie diese Informationen den Inspektoren als Grundlage für deren Prüfungstätigkeit zur Verfügung stellen. Damit nicht genug. Vielleicht möchte sie sich sogar ad hoc ein Bild über den Grad der „compliance" der gesamten Produktion verschaffen.

Ziel ist also, jederzeit eine fundierte und qualitative Aussage darüber treffen zu können, wie groß das Risiko ist, daß ein Fehler im Computersystem (bzw. an allen Stellen in der Organisation) Auswirkungen auf die Produktqualität hat.

Wie kann nun ein Risikomanagement helfen, diese Vision zu erreichen? Folgende drei Bausteine sind das Fundament eines funktionierenden Risikomanagement-Systems:

- Die Methode zum Risiko- und Maßnahmenmanagement[4)] bei der Computervalidierung (siehe Kapitel 3.1.)
- Die Tool-Unterstützung des Risiko- und Maßnahmenmanagements (siehe Kapitel 3.2.)
- Die technische und organisatorische Einführung und Umsetzung des Risikomanagement-Systems (siehe Kapitel 3.3.)

3.1. Methode zum Risiko- und Maßnahmenmanagement bei der Computervalidierung

Bei der nachfolgend dargestellten Methode zum Risiko- und Maßnahmenmanagement wird bewußt zwischen Risikomanagement und Maßnahmenmanagement (im Sinne von Management der risikomindernden Maßnahmen) unterschieden. Damit soll – wie oben bereits erwähnt – deutlich werden, daß ausschließlich aus dem Maßnahmenmanagement ein unmittelbarer wirtschaftlicher Nutzen gezogen werden kann (Abb. 3).

Ausgangspunkt dieser Methode sind die üblichen Unterlagen der Computervalidierung. Infrastruktur-Listen, SOPs etc. sowie Gap-Analysen gemäß CPG sollten bereits mehr oder weniger vollständig vorhanden sein. Je vollständiger und detaillierter diese Unterlagen vorliegen, um so einfacher und unaufwendiger kann der erste Schritt – die Identifikation der Risiken – durchgeführt werden.

3.1.1. Identifikation der Risiken

Zur Identifikation der Risiken wird auf einen prozeßorientierten Ansatz zurückgegriffen, weil in der Regel bereits die Prozesse in Form von SOPs sowie weitere Spezifikationen vorliegen. Für jeden relevanten Prozeßabschnitt wird ermittelt, ob und wie er fehlerhaft ablaufen könnte (What could go wrong?). Fehlerhafte Abläufe können dabei ihre Ursache in einzelnen technischen Komponenten eines Computersystems (Hardware, Software, Schnittstellen, Dateien etc.) haben, in einer fehlerhaften Prozeßorganisation oder in den involvierten Mitarbeitern.

[4)] In der Literatur wird das Management der risikomindernden Maßnahmen zumeist als ein Teil des Risikomanagements betrachtet.

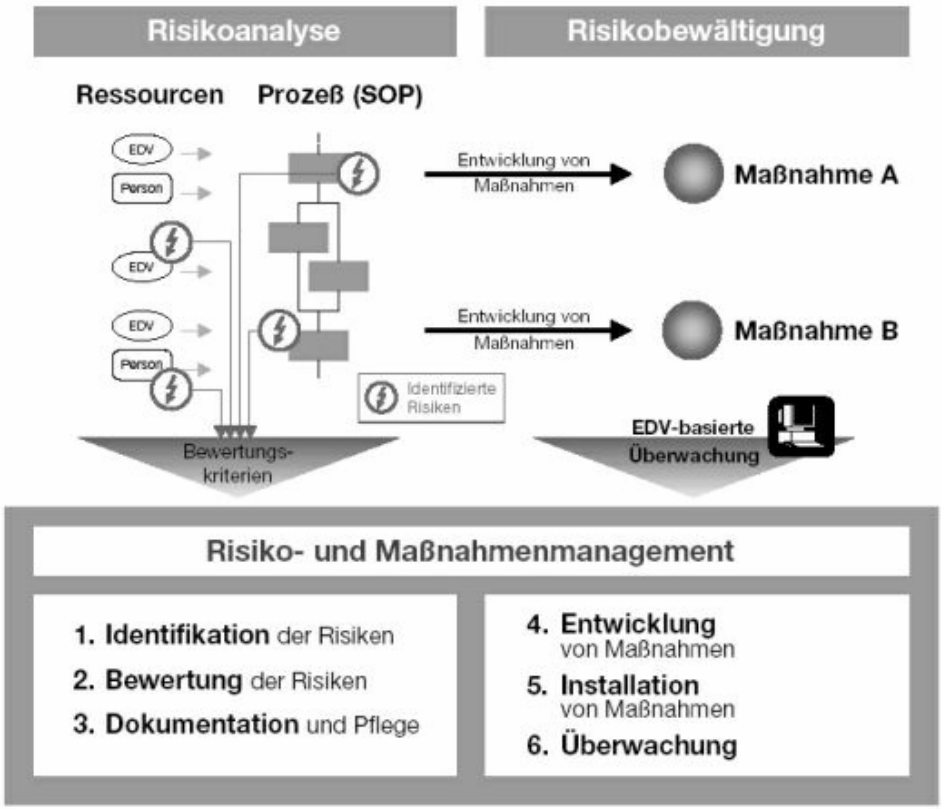

Abb. 3: Risiko- und Kontrollmanagement bei der Computervalidierung.

Wichtig ist, die Risiken in einem geeigneten Detaillierungsgrad zu ermitteln, da auf der einen Seite die potentiellen Auswirkungen eines Risikos relevant sein sollten, und es auf der anderen Seite eine zu benennende Ursache für dieses Risiko geben sollte. Um dies zu gewährleisten, sollte die Identifizierung der Risiken in einer Gruppe und unter methodischer Anleitung durchgeführt werden.

3.1.2. Bewertung der Risiken

Die identifizierten Risiken müssen zunächst gemäß der üblichen Kriterien für Qualität, Sicherheit und Ordnungsmäßigkeit der Computernutzung (Integrität, Zuverlässigkeit, rechtliche Erfordernisse etc. (vgl. z. B. Cobit) (ISACA 2000) klassifiziert werden, um zielbezogen die Vollständigkeit der Risikoliste zu gewährleisten. Die Anforderungen aus 21 CFR Part 11 werden dabei unter dem Kriterium der rechtlichen Erfordernisse abgedeckt. Je nach angestrebtem Schwerpunkt der Risikoanalyse sollten die relevanten Bereiche verstärkt betrachtet werden.

Weiterhin wird in dieser Phase die Eintrittswahrscheinlichkeit (bzw. Eintrittshäufigkeit) eines Risikos eingeschätzt sowie die potentiellen Auswirkungen des Risikos qualitativ oder quantitativ bewertet. Diese Abschätzung bildet nachher die Grundlage, um die erforderlichen Maßnahmen, die die Auswirkungen eines Risikos verringern sollen, priorisieren zu können. Mit der Priorisierung der Risiken wird später der Fokus bei der Risikobewältigung auf die tatsächlich relevanten Risiken gelenkt.

3.1.3. Dokumentation und Pflege der Risiken

Die identifizierten Risiken werden üblicherweise in den CSV-Dokumenten (SOPs, Inventurlisten etc.) dokumentiert. Bei Änderungen der Prozesse oder der Rechner-Infrastruktur werden die Risiken ebenfalls angepaßt. Die Pflege der CSV-Dokumente kann erheblich vereinfacht werden, wenn ein Tool eingesetzt wird, das auf verschiedene Speicherorte der CSV-Dokumente zugreifen und Änderungen der Dokumente sowie Einträge in den Dokumenten überwachen kann. Die Identifikation, Bewertung und Dokumentation der Risiken ist auf diese Weise kein einmaliges Ereignis, sondern ein andauernder Prozeß, durch den die überwachten Risiken ständig auf dem aktuellen Stand gehalten werden können.

3.1.4. Entwicklung von risikomindernden Maßnahmen

Die im Schritt 2 bewerteten Risiken bilden die Grundlage für die Entwicklung von risikomindernden Maßnahmen. Maßnahmen werden zur Reduzierung des Risikos an den Stellen plaziert, wo am ehesten ein Schaden beim Eintreten eines bestimmten Ereignisses vermieden werden soll. Eine risikomindernde Maßnahme kann auch die Einrichtung einer Kontrolle sein, die zur Überwachung des ordnungsgemäßen Betriebes oder zur Überwachung, ob ein bestimmtes Ereignis eingetreten ist, dienen.

Risikomindernde Maßnahmen beziehen sich in der Regel nicht auf nur ein einzelnes Risiko, sondern in der Regel auf Risiken, die an verschiedenen Stellen im Unternehmen mit der selben Ursache auftauchen. Um derartige prozeßübergreifende Abhängigkeiten zu berücksichtigen und Maßnahmen zu entwikkeln, die einen maximalen Nutzungsgrad haben, werden Ursachen-Wirkungsketten gebildet, aus denen derartige Abhängigkeiten deutlich werden.

Bei den entwickelten Maßnahmen kann es sich um alle der in Abb. 2 vorgestellten Risikobewältigungsmöglichkeiten handeln. Sowohl Vermeidung und Verminderung von Risiken, als auch Risikoübertragung sind Risikobewältigungsmöglichkeiten, die im Rahmen der Maßnahmenentwicklung in Betracht gezogen werden sollten.

Gut plazierte Maßnahmen sowie deren ständige Überwachung sind von essenzieller Bedeutung für den ordnungsgemäßen bzw. validen Betrieb der Computersysteme gemäß regulatorischer Anforderungen.

3.1.5. Installation von risikomindernden Maßnahmen

Risikomindernde Maßnahmen können auf technischer, organisatorischer oder personenbezogener Ebene greifen. Eine technische Maßnahme ist beispielsweise die Installation eines elektronischen Überwachungssystems. Bei einer organisatorischen Maßnahme handelt es sich z. B. um eine Vorschrift, in regelmäßigen Intervallen Reports auszuwerten. Ein Beispiel für personenbezogene Maßnahmen ist die Fortbildung von Mitarbeitern. In der Regel sind bei risikomindernden Maßnahmen alle Ebenen einbezogen, allerdings in unterschiedlicher Stärke. So bringt z. B. die Installation einer neuen Software als technische Maßnahme u. U. die Änderung organisatorischer Abläufe sowie Schulungsbedarf mit sich.

Es ist anzunehmen, daß – auch nach der neuen zu erwartenden Guidance der FDA – Maßnahmen (z. B. Installation einer 21 CFR Part 11-konformen Software) nicht unmittelbar umgesetzt werden müssen, sondern daß es reicht, sie nach Risikoaspekten priorisiert im Rahmen eines Umsetzungsplanes zu implementieren. Die Einhaltung dieses Planes ist deshalb aus regulatorischer Sicht unbedingt notwendig, so daß der Kontrolle der Umsetzung des Planes eine besondere Bedeutung zukommt.