IT-Anforderungen an Biobanken

Ronald Speer
Koordinierungszentrum für Klinische Studien Leipzig

TMF-Symposium Biomaterialbanken
Berlin, 27.04.2006

Gliederung

- Ausgangssituation
- Generelle Anforderungen
- Validierung und Qualitätssicherung
- Sicherheitsmanagement
- Integration

Ausgangslage

- Ziel: Daten klinischer Studien mit Ergebnissen von Biomaterialbanken zusammenzuführen und auszuwerten

- im Bereich klinischer Studien und Biomaterialbanken werden zunehmend computerunterstützte Verfahren zur Erfassung, Management und Auswertung der Daten eingesetzt

- Systeme unterliegen Richtlinien:
  - Datensicherheit
  - Datenschutz
  - Qualitätssicherung
  - ICH-Richtlinie für Good Clinical Practise

Rechtsgrundlagen, Normen, Standards

- **AMG, PharmBetrV**
- EG–GMP-Richtlinie und -Leitfaden
- Ergänzende Leitlinie computergestützte Systeme (Annex 11)
- GAMP-Guide und APV Interpretation des Annex 11
- PIC Empfehlungen für die Validierung
- PIC Guideline für computergestützte Systeme
- US-FDA – Guide to Inspection of Computerized Systems in Drug Processing (Blue Book)
- US-FDA - Guide to Inspection of Sponsors, CROs and Monitors
- **US-FDA – Guidance for Industry "Computerized Systems used in Clinical Trials"**
- **US-FDA - 21 CFR Part 11 (Electronic Records; Electronic Signatures)**
- GCP, GLP, ...

Generelle Anforderungen

Audit Trail als Grundbedingung für Nachvollziehbarkeit:

- Alle Änderungen an Daten und Dokumenten sind mit Datum, Uhrzeit und Name nachvollziehbar
- Über die gesamte Lebensdauer der Aufzeichnung;

Datensicherheit als Schutz vor Manipulationen:

- Rollen-basierte Zugriffsregelungen
- Verfügbarkeit von Trainingsdaten
- Aktuelle und praktikable Arbeitsanweisungen (SOPs)

Electronic Signatures (closed systems):

- Wird eineindeutig einer Person zugeordnet; nicht wieder verwendbar
- Höhere Anforderungen in „offenen Systemen“ (PKI, Verschlüsselung)

Validiertes System

Ziel der Validierung

- Erhöhung des Prozessverständnisses durch ein besseres Systemverständnis
- Erhöhung des Vertrauens in das computergestützte System
- Minimierung des Risikos von Fehlfunktionen
- Senkung der Kosten des laufenden Systembetriebs
- Senkung der Kosten bei Weiterentwicklungen des Systems

- zur Erfüllung gesetzlicher Anforderungen

Was ist Systemvalidierung

„Validierung ist die Erbringung eines **Nachweises**, dass ein Prozess mit hoher Wahrscheinlichkeit dauerhaft ein spezifikations- und qualitätsgerechtes Produkt erzeugt.“

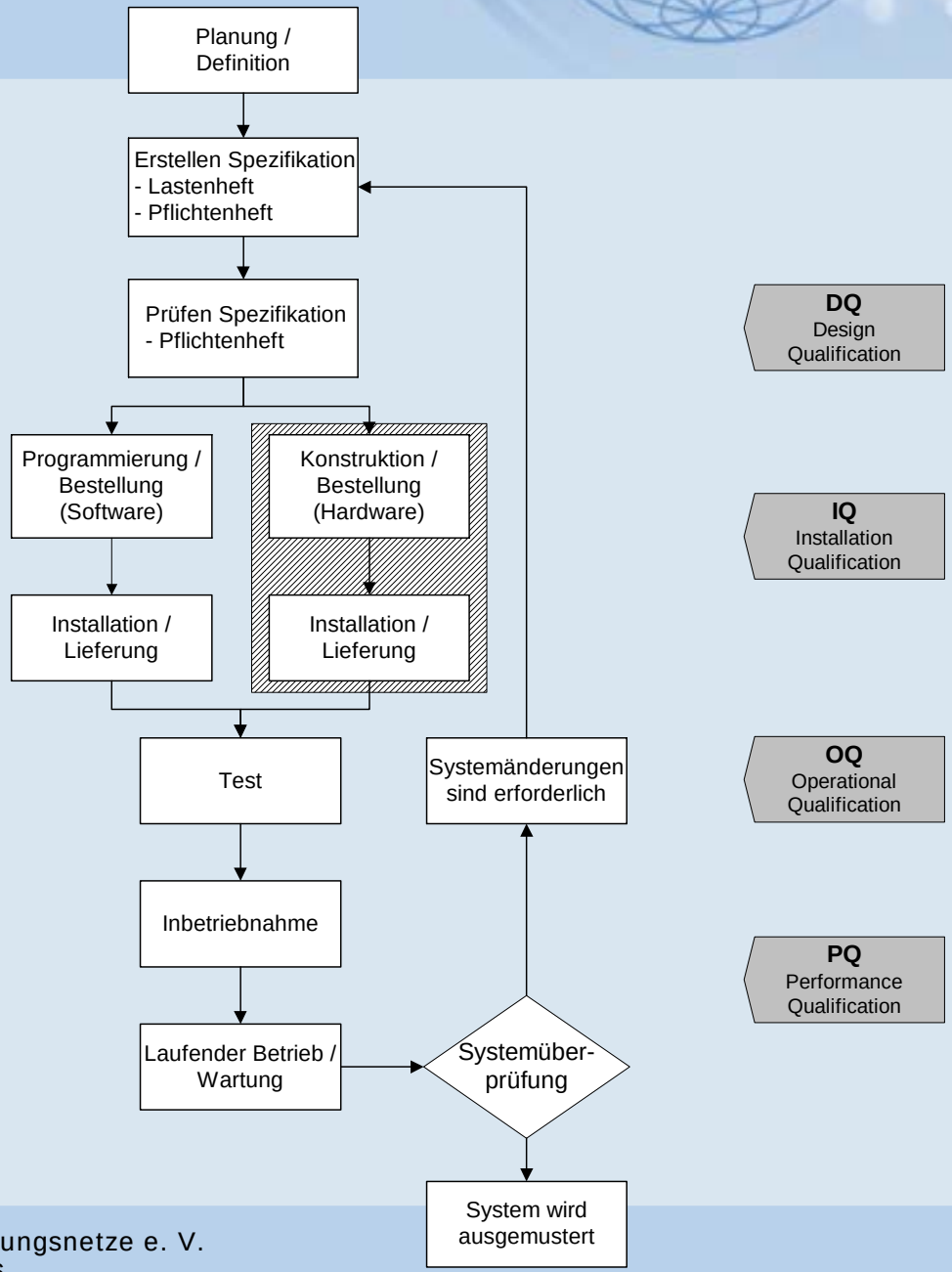
FDA Guidelines on General Principles of Process Validation

„Wenn ein **computergestütztes System** an die Stelle eines manuellen Vorgangs tritt, dürfen weder die Qualität der Produkte noch die Qualitätssicherung beeinträchtigt sein.“

Annex 11 zum EU-Leitfaden

„Validierung eines **computergestütztes Systems** ist der dokumentierte **Nachweis**, dass das System den regulatorischen Anforderungen genügt und so arbeitet und in Zukunft arbeiten wird, wie es dies laut Spezifikation tun soll.“

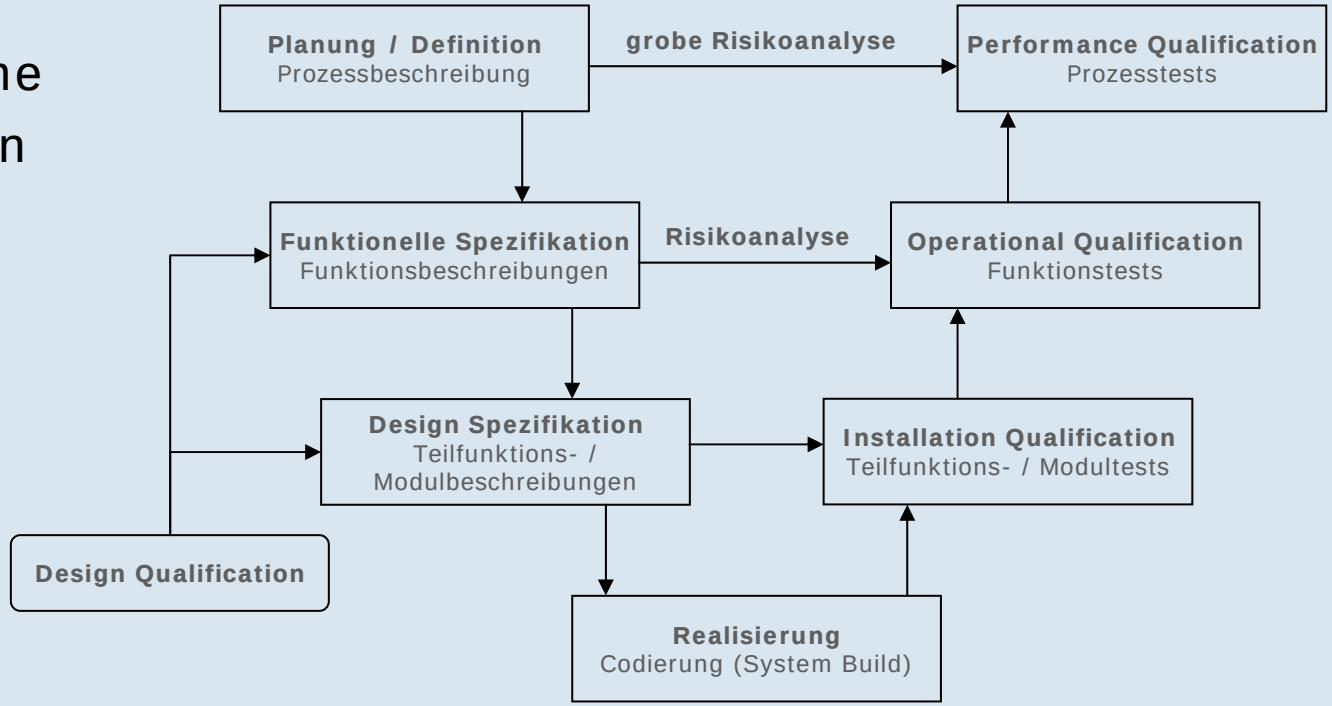
Life Cycle


Planung / Definition
Erstellen Spezifikation - Lastenheft - Pflichtenheft
Prüfen Spezifikation - Pflichtenheft
Programmierung / Bestellung (Software)
Konstruktion / Bestellung (Hardware)
Installation / Lieferung
Installation / Lieferung
Test
Systemänderungen sind erforderlich
Inbetriebnahme
Laufender Betrieb / Wartung
Systemüber-prüfung
System wird ausgemustert
DQ Design Qualification
IQ Installation Qualification
OQ Operational Qualification
PQ Performance Qualification

Validierungsprozess

Prozess der Validierung erstreckt sich über den gesamten life cycle:

- Planung
- Spezifizierung
- Programmierung
- Prüfung
- Inbetriebnahme
- Dokumentation
- Betrieb
- Kontrolle
- Änderung



Risikofaktor Systeme: Kategorien nach GAMP

Kat. 1: Systemsoftware / Betriebssysteme
Produkt- & Versionsmanagement

Kat. 2: Firmware (Barcodeleser, Scanner, Treiber, ...)
Produkt- & Versionsmanagement, Einstellungen

Kat. 3: Standardsoftware (Office, Datenbanken, ...)
Produkt- & Versionsmanagement
Beschreibung und Test des Anwendungsbereiches

Kat. 4: Konfigurierbare Standardpakete
Produkt- & Versionsmanagement
Spezifikation und Test der individuellen Konfiguration
Lieferantenbewertung

Kat. 5: Individualsoftware, Anpassungen, Schnittstellen
Full Life Cycle Dokumentation
Ggf. Lieferantenbewertung

VH

Risikofaktor: Anwender

- mangelndes Training
- „öffentliche“ Passwörter
- unklare Verantwortlichkeiten
- Work-arounds sind bequemer
- Nicht praktikable oder zu allgemeine Anweisungen
- Fehlende Plausibilitätsprüfungen
- Fehlende Sicherheitsabfragen

- Bedenke: Vorsätzliche Manipulation lässt sich nicht vermeiden

***p**roblem*
***e**xists*
***b**etween*
***k**eyboard*
***a**nd*
***c**hair*

Standard Operating Procedures

- Standard Operating Procedures (SOP) dienen in erster Linie der Dokumentation und der Qualitätssicherung
- sie sind ein notwendiges und bindendes Regelwerk für Vorgehensweisen innerhalb eines Forschungsverbundes.
- Sie besitzen ein festes, einheitliches Format, eine fortlaufende Nummerierung und unterliegen einer Versionisierung, d.h. eine bestehende SOP-Version ist nicht mehr änderbar, sondern wird regelmäßig auf ihre Aktualität überprüft, gegebenenfalls überarbeitet und als neue Version verabschiedet.
- Folgende Bereiche werden zum Beispiel von SOPs abgedeckt :
  1. Datenerfassung und –verarbeitung
  2. Systemwartung
  3. Backup, Recovery, Notfallplan
  4. Sicherheit
  5. Änderungskontrolle/Change Management

Wann ist ein System validiert ?

- Das Systemumfeld ist beschrieben.
- Eine Risikobetrachtung wurde durchgeführt
- Die Systemdokumentation ist vorhanden und von den verantwortlichen Personen (Herstellungsleiter und Kontrolleiter) 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.

Wie bleibt ein System validiert ?

- 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

Need-to-have

Alle Beteiligten müssen hinreichend **qualifiziert** sein
→ Trainingsplan; Vereinbarungen mit Externen

Die **Dokumentation** muss vollständig sein
→ Regelwerk (QM-Handbuch, SOPs)

Das System muss hinreichend **getestet** werden
→ Testplan

Die **Zugriffe** müssen geregelt sein
→ Berechtigungskonzept

Änderungen müssen kontrolliert werden
→ Change Control Verfahren

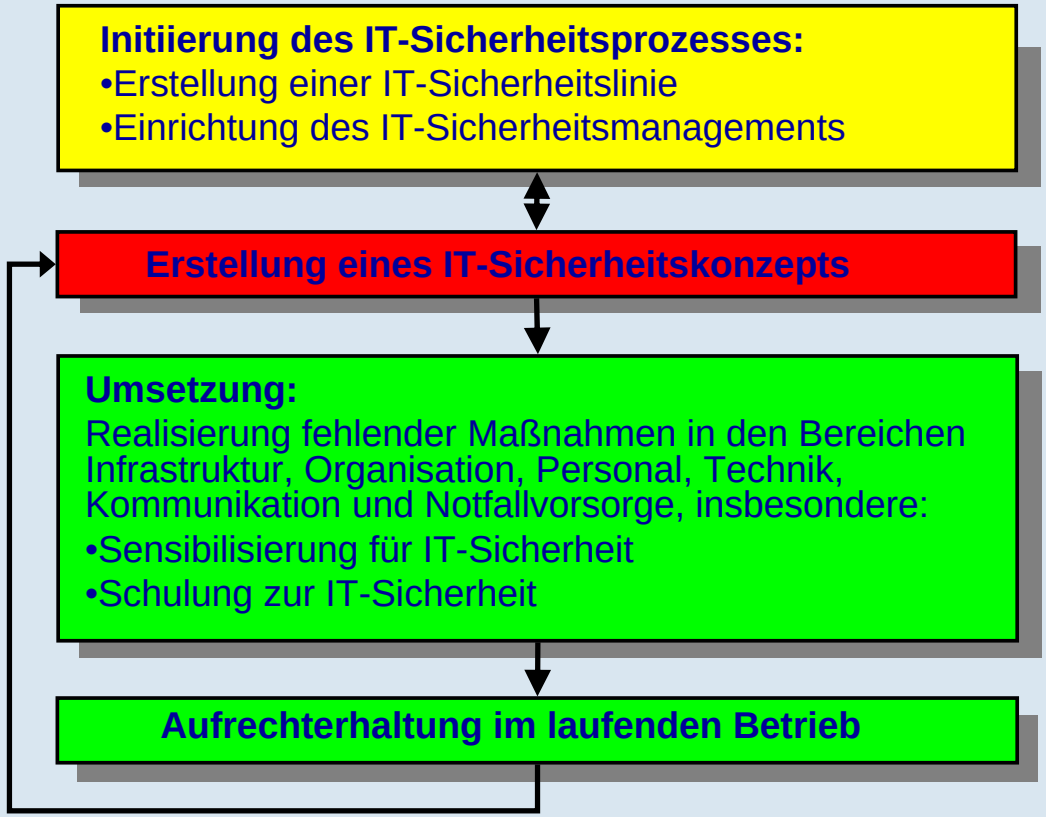
Das System muss die regulatorischen Anforderungen funktional unterstützen
→ **Spezifikationen** (Requirements Tracking)

Der **Betrieb** des Systems muss geregelt werden
→ Datensicherheitskonzept (Disaster Recovery)

Motivation

- Sicherheitskonzepte bilden eine wesentliche Grundlage für die sichere Erfassung, Verarbeitung und Speicherung von kritischen Daten
- besonders bei der für Forschungsverbünden typischen verteilten Verarbeitung von Patienten- und Studiendaten
- Forderung durch Regularien und Gesetze (ICH-GCP, FDA, AMG) über Nachweis der Maßnahmen und Prozesse in klinischen Studien

IT Sicherheitsprozess



Sicherheitsmanagement

Organisation 1

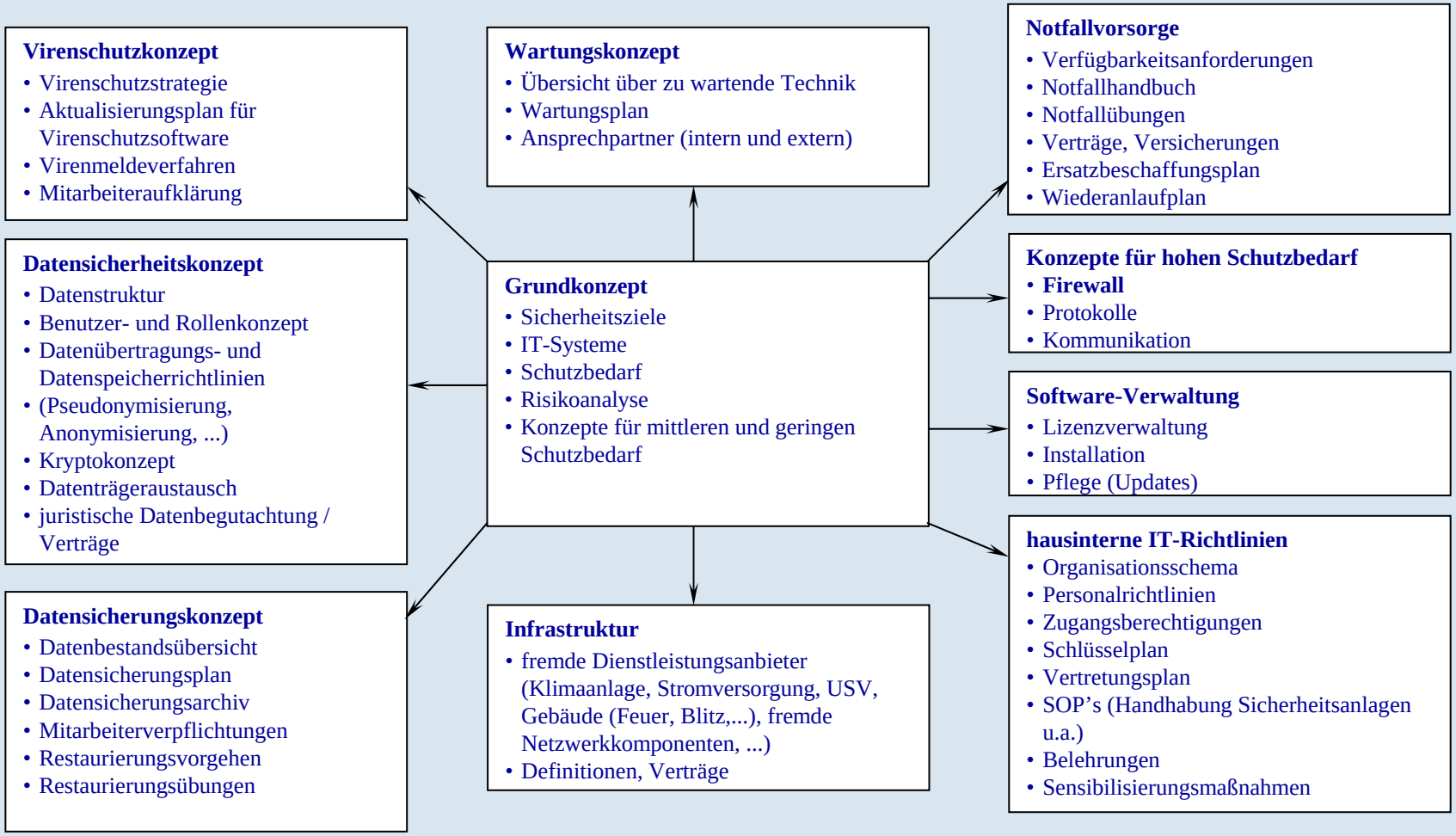
- Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz
- Datenträgerverwaltung
- Regelungen für Wartungs- und Reparaturarbeiten
- Vergabe von Zutrittsberechtigungen
- Vergabe von Zugangsberechtigungen
- Vergabe von Zugriffsrechten
- Regelung des Passwortgebrauchs

Sicherheitsmanagement

Organisation 2

- Nutzungsverbot nicht freigegebener Software
- Überprüfung des Software-Bestandes
- Betreuung und Beratung von IT-Benutzern (optional)
- Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln
- Schlüsselverwaltung
- "Der aufgeräumte Arbeitsplatz"
- Reaktion auf Verletzungen der Sicherheitspolitik
- Datenschutzaspekte bei der Protokollierung
- Sicheres Löschen von Datenträgern
- Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen

Module des Sicherheitskonzeptes



Sicherheitsmanagement

Need-to-have 1

Personal

- Geregelte Einarbeitung/Einweisung neuer Mitarbeiter
- Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Vertretungsregelungen
- Schulung vor Programmnutzung
- Schulung zu IT-Sicherheitsmaßnahmen
- Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern

Virenschutz

- Virenschutzstrategie
- Aktualisierungsplan für Antiviren-Software
- Virenmeldeverfahren

Zugangskonzept

- Anlegen Benutzeraccount
- Wahl der Passworte
- Rechtevergabe

Sicherheitsmanagement

Need-to-have 2

Datensicherung
- Datenbestandsübersicht
- Datensicherungsplan
- Mitarbeiterverpflichtungen
- Restaurierungsvorgehen
- Restaurierungsübungen

Wartung
- Wartungsplan
- Technische Wartung / Reparaturen
- Fehlermeldungsweg
- Wartungsverträge
- Ansprechpartner / Serviceleister

Notfallvorsorge
- Verfügbarkeitsanforderungen
- Notfallhandbuch
- Notfallübungen
- Verträge, Versicherungen
- Ersatzbeschaffungsplan
- Wiederanlaufplan

Was tun?

Ressourcen sind begrenzt!

Umgang mit Altsystemen?

- Risikobetrachtungen durchführen
- auf das Wesentliche beschränken
- Service Level Agreements abschließen

Aber!

- Prozessverständnis kann Kosten minimieren
- Qualität kann Akzeptanz bei Partnern und ‚Kunden' steigern

Integration

- Standards nutzen (XML, SQL, etc.)
- umfassende Systemkonzeption
  (Mit **wem** soll **was** ausgetauscht werden?)
- Schnittstellen definieren und beschreiben
- Standardlösungen nutzen (Validierung!)

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen:

http://www.tmf-ev.de/