TMF – Technologie- und Methodenplattform
für die vernetzte medizinische Forschung e.V.

Systembetrieb (Aufrechterhalten des validierten Zustandes)

Validierungsschulung (Modul 6)

Version: V03

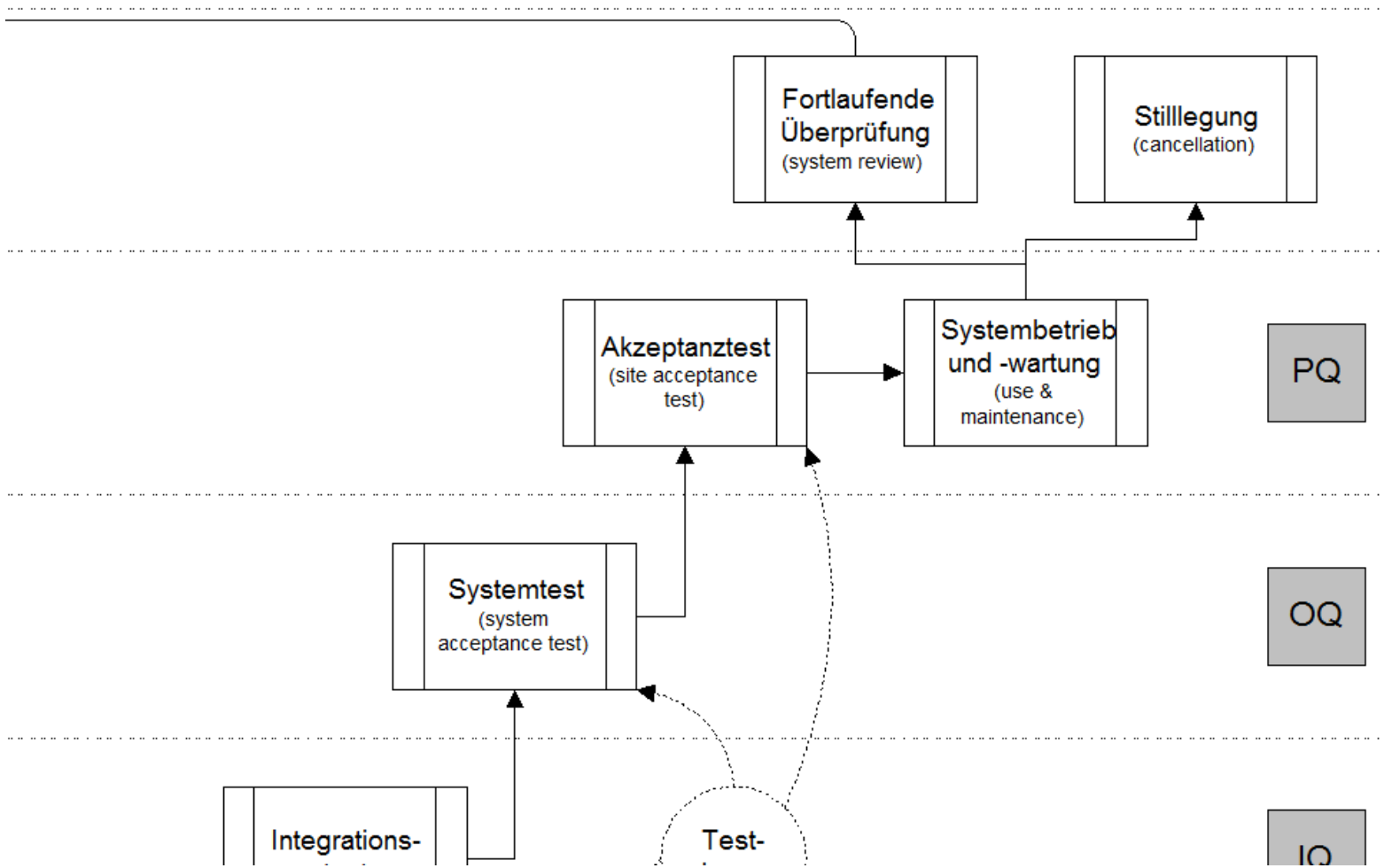
Ronald Speer

LIFE Leipzig

Inhalt

- Systembetrieb und Änderungen
- Change Control: Prinzipien
- Fehler- & Konfigurationsmanagement
- Change Control Verfahren
- Änderungsantrag
- Klassifizierung von Änderungen
- Erhaltung des validen Systemzustandes
- internes Audit
- Revalidierung
- Störungen und Wartung
- Support
- Sicherheitsmanagement

Phase im Lebenszyklus (V-Modell): Systembetrieb



Anforderungen an den Systembetrieb nach GAMP

Bausteine von Betrieb & Wartung (lt. GAMP5):

- Fortlaufende Überprüfung (Review)
- Risikoanalyse
- System und Prozess-Audits
- Änderungskontrolle und Konfigurationsmanagement
- Schulung der Anwender und Systembetreuer

Was kann sich ändern? – Beispiele:

- Neue Software-Versionen, Releases, Patches, Builds
- Änderung der Datenstruktur, z.B. nach Datenmigration oder Bereinigung
- Änderungen von Teilen der Systemumgebung nach einem Disaster Recovery
- Änderungen am unterstützten Prozess (Konfiguration, Customization) und der Dokumentation SOPs
- Anbindung anderer Module oder Software-Pakete
- Erweiterung des Systems (Sizing)

Blockade-Taktik

„Never touch a running system?“

- Stand einfrieren
- Lernen mit Fehlern zu leben, ggf. SOPs schreiben

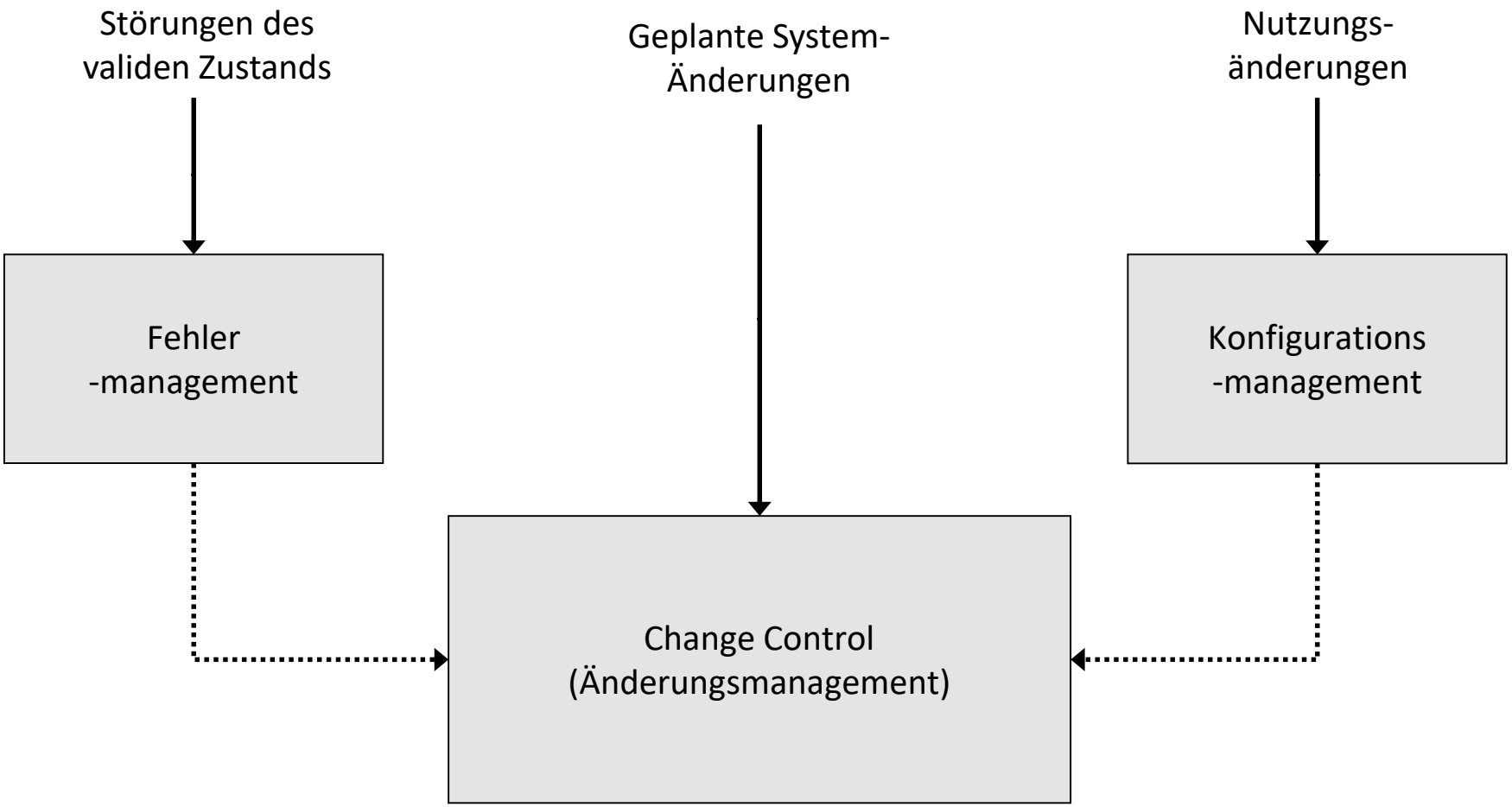
Empfehlung:

- Lassen Sie keine Benutzer an das System!
- Schliessen Sie alle Computer weg!

Change Control: die Prinzipien

- Durch ein funktionierendes Change Control-Management werden Änderungen der Software systematisch erfasst und über die Notwendigkeit einer begleitenden Validierung entschieden
- Werden Fehler festgestellt, müssen diese mit einem Fehlerprotokoll an den entsprechenden Verantwortlichen gemeldet werden
- Mit jeder wesentlichen Änderung des Systems oder der Installation einer neuen Komponente oder eines Upgrades muß eine IQ durchgeführt und dokumentiert werden
- Change Control betrifft neben der Software, auch Änderungen der Hardware, Netzwerkänderungen, Änderungen der Dokumentation (z.B. Benutzerhandbuch) und Schulungen
- Change Control bezieht sich nicht nur auf Fehler, sondern auch auf Verbesserungsvorschläge

Change Control: Abgrenzung

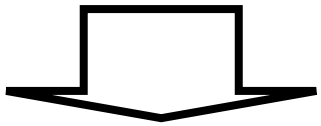


Fehlermanagement

Jeder FEHLER,
der nicht in den Validierungsdokumenten erwähnt wird,

- ist eine Störung des validierten Zustandes!

- Fehlerbehebung = Änderung



Change Control

Konfigurationsmanagement: Elemente

Hardware:

- Systemkomponenten spezifizieren
- Aufzeichnung (Logs) der Einstellungen und Modifikationen von Komponenten
- Kontrolle von Zustand/Status, Vollständigkeit, Konsistenz und Korrektheit/Kompatibilität von Komponenten

Software:

- Module / Komponenten, deren Funktionsumfang von Administratoren über Systemparameter einstellbar ist
- Bausteine (Programme), deren Funktionsweise von Administratoren oder Anwendern über Vorgabewerte (Basis-/ Stamm-/ Grunddaten) gesteuert werden kann

Konfigurationsmanagement: Richtlinien

- Ziel: Alle Änderungen an der Konfiguration sollen koordiniert und kontrolliert werden
  - Konfigurationsstatus
  - Versionskontrolle
  - Spezifizierung
  - Konfigurationsbeurteilung
  - Freigabe

- Im Rahmen der Validierung werden
  - die Systemteile definiert, die dem Konfigurationsmanagement unterliegen sollen, und
  - mögliche alternative Konfigurationen geprüft und freigegeben (Konfigurationsrahmen)

- Änderungen außerhalb des Konfigurationsrahmens unterliegen dem Änderungsmanagement (Change Control)

Erhaltung des validen Zustandes durch Change Control

Das Change Control-Verfahren stellt sicher:

1. alle planbaren Änderungen werden kontrolliert umgesetzt
2. das Lebenszyklusmodell wird gemäß dem system-spezifischen Projekt-/ Validierungsplan angewendet
3. jede Änderung unterliegt einem Genehmigungsprozess
4. jede Änderung wird bezüglich ihrer Auswirkung auf das Gesamtsystem bewertet (Risikoanalyse),
5. aus der Bewertung werden nachvollziehbare Maßnahmen abgeleitet

Change Control: Überblick

1. **Beschreiben**
2. **Bewerten**
3. **Genehmigen**
4. **Durchführen**
5. **Freigeben**

Praxis:

Wahrscheinlichste Änderungen vordenken und regeln (=SOP)

Mit jeder neuen Änderung erweitern

Beispiel für einen Änderungsantrag (Change Request) - Beschreibung

Änderungsantrag EDV

Änderungsantrag-Nr. (wird vom Change Control Team vergeben)	
Systembeschreibung:	

Änderungsgrund:

☐ Änderungswunsch ☐ Fehler (entspr. Fehlerdokumentation in Kopie beifügen)

Detaillierte Beschreibung der gewünschten / benötigten Änderung:
(Beschreibung, Begründung, Ziel, Auswirkung und Nutzen)

Change Control: Änderungsanträge

- Änderungsanträge bei geplanten Änderungen am System
- Jeder Nutzer des Systems kann eine Änderung beantragen
- Der Systembetreuer (oder das Change-Control-Team) erhält den Antrag und bewertet die Änderung
- Durch den Systembesitzer und die QA-Abteilung erfolgt die Genehmigung oder Ablehnung
- Jede Änderung muss dokumentiert werden und von der Person, die die Änderung durchgeführt hat, und der QA-Abteilung unterzeichnet werden
- Testung der Änderung
- Systemfreigabe durch die Unterschrift des Systembesitzers

Beispiel für einen Änderungsantrag (Change Request) - Bewertung

Änderungsbewertung (wird vom Change Control Team ausgefüllt)		
Auswirkungen / Änderungsumfang	**Klassifizierung**	**Massnahme(n)**

Klassifizierung von Änderungen

Änderung	Klassifizierung	Mögliche Maßnahme(n)
Austausch einfacher Standard-Komponenten, z.B. Drucker, Endbenutzergerät	gering	Nachweis der Eignung des Gerätes. Funktionstest und Dokumentation des Austausches.
Hardwareerweiterung (Hauptspeicher, Platten-kapazität, weitere Drucker)	gering	Nachweis der Eignung des/ der Elemente. Funktionstest und Doku-mentation des Austausches.
Erhöhung der Benutzeranzahl für Betriebssystem, Applikation, Datenbank	mittel	Belastungstest mit max. Anzahl User erneut durchführen. Dokumen-tation der Tests
Wesentliche Änderungen von Datenvolumina (Grenzwerte der Datenbank werden erreicht)	hoch	Hoch:Upgrade oder Installation einer neuen DB. Abwicklung über Lebenszyklus, ab Anforderungs-spezifikation. Mittel:Erweiterung der Daten-bankfunktionalität (User / Volumen) mit mindestens Verfahrens-qualifizierung.

Change Control baut auf dem Validierungsprozess auf

Die Systemvalidierung erleichtert das Change Control

- Bei der Bewertung von Änderungen und der Definition von Maßnahmen sind hilfreich:
  - Validation Master Plan und SOPs
  - Liste aller Systeme inkl. Bewertung der GCP-Relevanz
  - Risikoanalyse des betreffenden Systems / Moduls
  - Datensicherheits- und –sicherungskonzept
  - (erste) Erfahrungen im Umgang mit Änderungen während der Systemeinführung
  - qualifizierte Mitarbeiter, die das System oder den Prozess kennen

Change Control ist die logische Fortsetzung der Computer System Validierung

Sicherheit & Nachvollziehbarkeit
im laufenden Betrieb

Maßnahmen zur Erhaltung des validen Systemzustandes (Überblick)

- Maßnahmen zur Änderungskontrolle müssen gewährleisten, dass Systemänderungen nur risikobewertet und dokumentiert durchgeführt werden (Jede Änderung = Risiko den validen Zustand zu verlieren)
- Maßnahmen zur Systemsicherheit dienen der Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen
- Maßnahmen zur Leistungsüberwachung dienen der Überprüfung, ob die von einem Computersystem durchzuführenden Prozesse in den für sie geforderten Zeiten bearbeitet werden können
- Ein zuverlässiger Support ist eine unbedingte Voraussetzung für den kontrollierten Betrieb eines Computersystems
- Der valide Systemzustand sollte über interne und externe Audits regelmäßig überprüft werden

Konzept für internes Audit

- die interne Überprüfung des Validierungsstandes in den Verbünden
- Überprüfung einer regelrechten und adäquaten Computer-System-Validierung

Internes Audit: Aufgaben

- Festlegung der Verantwortung: Systemeigner und QS
- Festlegung der Zeit- und Ablaufplanung
- Festlegung der Prüfperiode
- Festlegung des Entscheidungsvorgangs
- Durchführung des Audits

Ziel und Aufbau des internen Audits

- Das interne Audit hat das Ziel festzustellen, ob sich das System in einem validierten Zustand befindet und in Übereinstimmung mit den GCP-Vorschriften und den Grundsätzen des Verbundes betrieben wird
- Teile des Audits:
  - Validierung
  - Betrieb
  - Konfigurationsänderungen
  - Offenstehende Aktionen des Validierungsberichtes
  - frühere Auditberichte
  - Belege für Instabilitäten oder Unsicherheiten im Betrieb
  - Änderungen der Umgebung, Anforderungen oder Praxis
  - Betriebsanweisungen (SOPs)
  - Personal (Schulung, Qualifikation)
  - Systeminstandhaltung
  - Datensicherung

Revalidierung

- Die Notwendigkeit für erneute Validierung des Systems (Revalidierung) kann sich nach größeren Änderungen an der Hard- und Software eines Computersystems ergeben

Störungen und Systemwartung

- Sowohl für routinemäßige vorbeugende Wartungsarbeiten als auch zur Behebung von Störungen sollen dokumentierte Verfahren vorhanden sein
- Diese Verfahren sollen die Aufgaben und Verantwortlichkeiten des dazu eingesetzten Personals beschreiben
- Wenn derartige Wartungsarbeiten Änderungen der Hardware und/oder der Software erforderlich machen, kann es nötig werden, das System erneut zu validieren.
- Über alle Probleme oder bemerkten Unregelmäßigkeiten, die während des täglichen Betriebs des Systems aufgetreten sind, sowie über die daraufhin durchgeführten Maßnahmen, sind Aufzeichnungen anzufertigen und aufzubewahren

Businesskontinuitätsplanung

- Kontinuitätspläne (Kontingenzplänen) sollen für Katastrophen-situationen erarbeitet werden
- Unter Kontingenzplänen versteht man eher die technischen Vorgehensweisen und unter Kontinuitätsplanung die Vorkehrungen, die aus Verbundsicht notwendig sind
- Es ist sinnvoll hier mit Szenarien zu arbeiten, die auf Katastrophenplänen basieren, die festlegen, in welcher Weise auf das Auftreten bestimmter Bedrohungen reagiert werden soll
- Im Bereich der Softwaresysteme betrifft dies z.B. Feuer, Wassereinbruch oder Diebstahl im Rechenzentren / Serverraum

Service Level Agreement (ASP)

- im Bereich der Bereitstellung von Studiensoftware (Hosting, ASP) gibt es verschiedenen Dienstleistungen zwischen einem Softwareprovider und einem Verbund
- Hierbei kann ein Verbund auch als Softwareprovider (z.B. EDC-System, Pseudonymisierungsdienst, SAE-Management) für einen anderen Verbund auftreten
- Diese Beziehungen werden durch SLA-Verträge geregelt
- Hierbei werden die Dienstleistungen im Detail geregelt
- Die TMF besitzt einen Muster-SLA-Vertrag für Verträge zwischen zwei Verbünden

Aufbau eines Muster-SLA‘s

1 Service Level Agreements
2 Rechenzentrumsdienstleistungen
- 2.1 Remote Hands Service
- 2.2 Organisatorische Abwicklung und allgemeine Leistungen
  - 2.2.1 Projektleitung, Service-Manager
  - 2.2.2 <Hostinganbieter> User-Help-Desk und Service- Desk Leistungen
  - 2.2.3 Security-Management (Plan - Do - Check – Act)
  - 2.2.4 Service Requests
  - 2.2.5 Change-Management
  - 2.2.6 Emergency Changes
  - 2.2.7 Wartungsfenster
  - 2.2.8 Erweitertes Wartungsfenster
  - 2.2.9 Notfallhandbuch
  - 2.2.10 Ticket-System – Dokumentation von Betriebsereignissen
  - 2.2.11 Reporting/Berichtswesen
- 2.3 Service-Level-Agreements
  - 2.3.1 Verfügbarkeiten
  - 2.3.2 Für Service-Level relevante Definitionen

3 Dezentrale Produkte
- 3.1 Hardware
- 3.2 Software
- 3.3 Störungsannahme
- 3.4 (Optional) Ticket-System
- 3.5 Reaktionszeiten

4 Mitwirkungspflichten des Kunden

Support für den Systembetrieb: Arten von Support

- Ein zuverlässiger Support ist eine unbedingte Voraussetzung für den kontrollierten Betrieb eines Computersystems
- Arten von Support:
  - **First Level-Support:** (auch „User Help Desk“) ist die erste Anlaufstelle für alle eingehende Unterstützungsfragen. Ziel ist das schnelle Lösen einer möglichst großen Anzahl von Problemen.
  - **Second-Level Support**: unterstützt den First-Level-Support, sowohl durch Weiterbildung am Arbeitsplatz als auch durch Übernahme komplexerer Anfragen.
  - **Third-Level Support:** setzt sich aus Spezialisten bzw. Mitarbeiter des Herstellers des Systems zusammen

IT-Sicherheit: Bestandteile

- Etablierung von IT-Sicherheitsprozesse im Verbund
- Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit (Verantwortlichkeiten, Rollen)
- Erstellung einer Übersicht über vorhandene IT-Systeme, mit Risikoabschätzung für Sicherheit
- Erstellung eines IT-Sicherheitskonzepts
- Umsetzung des IT-Sicherheitskonzepts nach einem Realisierungsplan
- Erstellung eines Schulungskonzepts für IT-Sicherheit
- Sensibilisierung der Mitarbeiter für IT-Sicherheit
- Aufrechterhaltung der IT-Sicherheit
- Erstellung von Managementreports zur IT-Sicherheit

Sicherheitsmanagement: notwendige Dokumente

- Datenbestandsübersicht
- Datensicherungsplan
- Datensicherungsarchiv
- Benachrichtigungen
- Mitarbeiterverpflichtungen
- Restaurierungsvorgehen

Wichtig:

- Backup von Daten
- Datensicherungsplan

Sicherheitsmaßnahmen

- Festlegung von Verantwortlichkeiten
- Datenträgerverwaltung
- Regelungen für Wartungs- und Reparaturarbeiten
- Vergabe von Zutrittsberechtigungen
- Vergabe von Zugriffsrechten
- Überprüfung des Software-Bestandes (Nutzungsverbot nicht freigegebener Software)
- Regelung des Passwortgebrauchs
- Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln (Datenvernichtung)
- Prinzip: "Der aufgeräumte Arbeitsplatz"
- Reaktion auf Verletzungen der Sicherheitspolitik
- Datenschutzaspekte bei der Protokollierung
- Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen

IT-Sicherheit: Notfallvorsorge

- Zur Vorbeugung beim Eintreten eines Notfalles (z.B. Brand, Wasserschaden, usw.), welcher die Verfügbarkeit von Daten und Technik beeinträchtigt, sind zusätzliche Maßnahmen erforderlich:
  - Verfügbarkeitsanforderungen
  - Notfallhandbuch
  - Notfallübungen
  - Verträge, Versicherungen
  - Ersatzbeschaffungsplan
  - Siehe: Kontingenzplan, Wiederanlaufplan

IT-Sicherheit: Systemausfall

- Der Ausfall eines Computersystems bedeutet, das ein Computersystems längere Zeit nicht genutzt werden kann
- Zum Zugriff auf Datenbestände während dieser Zeit ist ein Ersatzsystem, oder ein alternatives Verfahren zur Datenrepräsentation, bereitzuhalten
- Auch für das Ersatzsystem sind Anforderungen an: Verfügbarkeit, Angemessenheit, Praktikabilität, Verlässlichkeit und Vollständigkeit zu stellen
- es sollte ein Verfahren festgelegt werden, um das Computersystem wieder in seinen funktionsfähigen Grundzustand zu bringen
- Systemfehler sollten im laufenden Betrieb vermieden werden
- Kontrollmaßnahmen zum frühzeitigen Erkennen von Systemausfällen sollten etabliert werden

Vielen Dank für Ihre Aufmerksamkeit!

Mehr Information:

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