Gegenstand und Auswirkungen der BSI-Richtlinie „TR Resiscan“

Dipl. Wirtsch.-Ing. Lothar Leger

B&L Management Consulting GmbH

Anbieter- und produktneutrale Beratung – seit über 20 Jahren

Kompetenzen

- **Business Process Management**
- **Rechnungsprozesse**
- **Dokumenten-Management**
- **Archivierung**
- **ECM-/DMS-Infrastruktur**

Beratungsleistungen

- **Strategie**
- **Potenzialanalyse**
- **Fachkonzept**
- **Fachkonzept**
- **Anbieter- und Produktauswahl**
- **Projektmanagement**
- **Verfahrensdokumentation**
- **Migrationskonzept**

Zitat von der Webseite www.bsi.bund.de zur BSI TR 03138

……. im Zuge der fortschreitenden Digitalisierung (werden) zunehmend elektronische Dokumentenmanagement- und Vorgangsbearbeitungssysteme eingesetzt. Zur Umsetzung des elektronischen Rechts- und Geschäftsverkehrs mehren sich Rechtsvorschriften, die die elektronische Aktenführung zulassen oder vorschreiben. …….

Die Aufbewahrung der Papieroriginale stellt eine hohe finanzielle und organisatorische Belastung der betroffenen Stellen dar. In rechtlicher Hinsicht bestehen – neben der in verschiedenen Rechtsgebieten sehr unterschiedlichen Regelungen zur Zulässigkeit des ersetzenden Scannens – Unsicherheiten aufgrund uneinheitlich ausgestalteter technisch-organisatorischer Anforderungen. …….

Die TR RESISCAN hat zum Ziel, diese Lücke zwischen abstrakten und uneinheitlichen rechtlichen Anforderungen sowie der zuverlässigen technischen Realisierung des Scannens zu schließen.

Mit der TR 03138 Ersetzendes Scannen möchte man folgendes erreichen:

- Anwender im privaten und behördlichen Bereich soll die Auswahl von Scan-Lösungen erleichtert werden (Vereinheitlichung von Anforderungen und Sicherheitsmaßnahmen)
- Hersteller und Dienstleister erhalten Spezifikationen, um ihre Leistungen, Lösungen und Produkte „TR-konform" gestalten und anbieten zu können.
- Beides zusammen bildet die Basis dafür, dass ein (anerkannter) Nachweis zur Einhaltung der Vorgaben für ein „ersetzendes Scannen" erbracht werden kann.
- Die Beweiskraft gescannter Dokumente wird durch die Etablierung eines abgestimmten Verfahrens verbessert (die Vernichtung von Originaldokumenten führt stets zu einer Reduzierung des Beweiswerts).

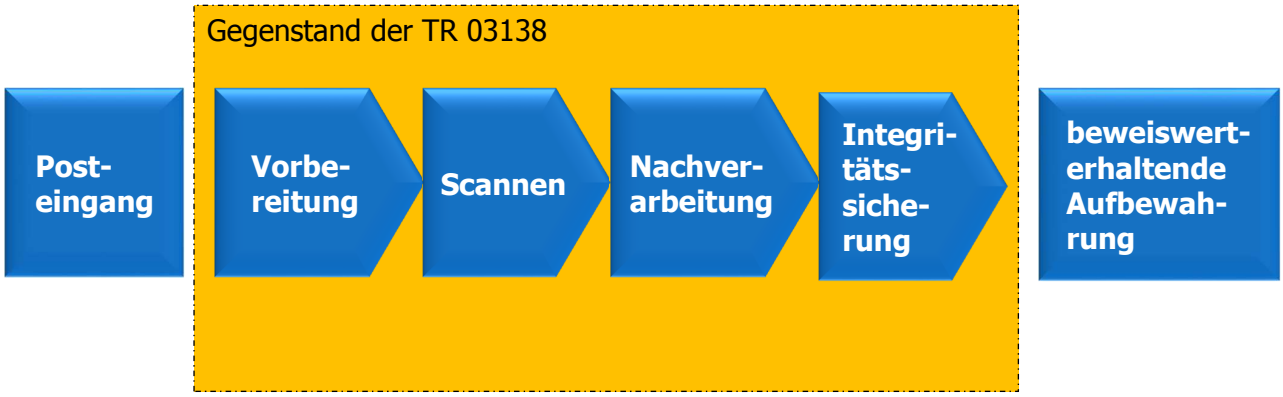
Wozu braucht man die TR 03138 Ersetzendes Scannen, wenn doch schon seit Jahren in vielen Bereichen Papierdokumente digitalisiert und anschließend vernichtet werden?

- Im kaufmännischen und im steuerlich relevanten Umfeld existieren mit Abgabenordung, Handelsgesetz und darauf aufbauend GoBS / GDPdU (resp. jetzt GoBD) ausreichend Vorgaben und Regelungen, nach denen ersetzend gescannt werden kann.
- In anderen Einsatzgebieten fehlen diese Regelungen.

Die Technische Richtlinie besteht aus einem Hauptteil und mehreren Anlagen

Hauptdokument	Maßnahmen, Prüfspezifikationen, Testfälle für Konformitätsprüfung
Informative Anlagen	Anlage A (Ergebnis der Risikoanalyse) Anlage R (unverbindliche rechtliche Hinweise) [nicht Gegenstand der Zertifizierung, nicht für TR-konformen Scanprozess erforderlich]
Anlage V	Exemplarische Verfahrensdokumentation [Musterverfahrensdoku als Orientierungshilfe]
Anlage P	Prüfspezifikation [Muss / Soll / Kann – Kriterien für die Prüfungen]

Die TR 03138 bezieht sich auf den Prozess des ersetzenden Scannens.



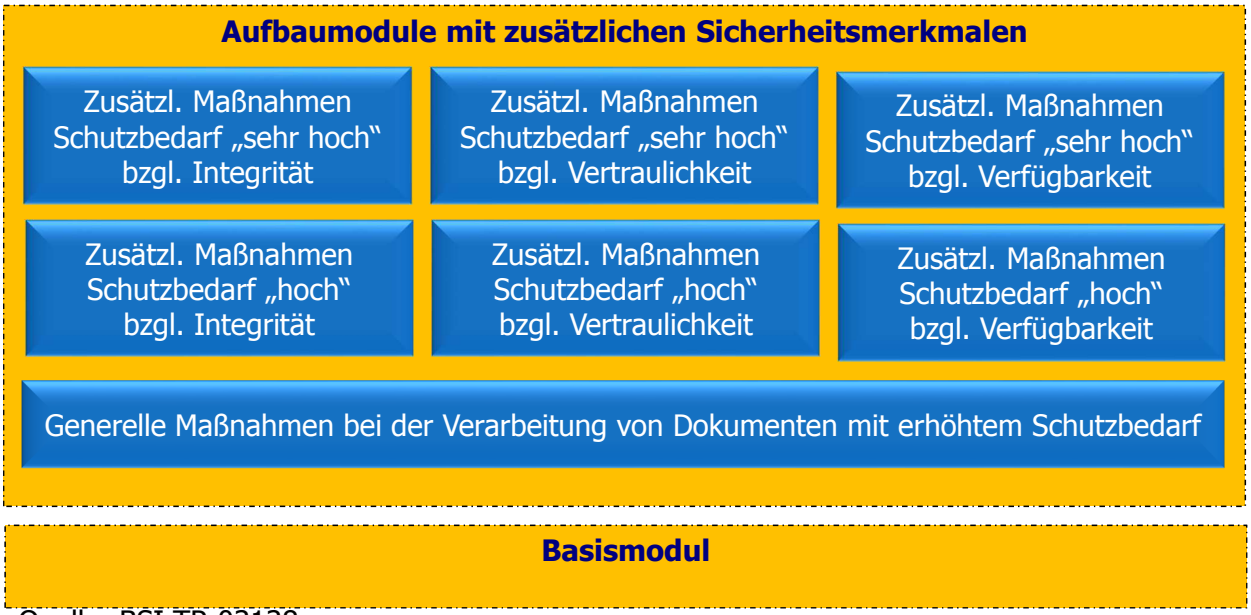
Quelle: BSI TR 03138

Sie bezieht sich NICHT auf bestimmte Hard- oder Softwarekomponenten (Produktneutralität).
Sie umfasst NICHT die Schritte der Sachbearbeitung oder Zwischenspeicherung.

In Abhängigkeit von den Schutzbedarfsanforderungen unterscheidet die TR 03138 zwischen einem Basismodul und Aufbaumodulen.

Quelle: BSI TR 03138

In den Aufbaumodulen wird einerseits zwischen Integrität, Vertraulichkeit und Verfügbarkeit und andererseits zwischen „sehr hoch" und „hoch" unterschieden.



Quelle: BSI TR 03138

Basismodul

Grundlegende Anforderungen* im Basismodul sind

- Verfahrensdokumentation
  - Eine Verfahrensdokumentation MUSS existieren
  - Sie enthält u.a. Informationen zu Abgrenzung, Verantwortlichkeiten, Abläufen, Anforderungen an den Scanprozess, Aussagen zu Administration und Wartung
- Schutzbedarfsanalyse
  - Eine sorgfältig begründete Schutzbedarfsanalyse hinsichtlich der Grundwerte der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) und bezogen auf die zu verarbeitenden Dokumente MUSS durchgeführt werden.
  - Sie bestimmt die Schutzbedarfsklasse („normal", „hoch", sehr hoch"), woraus sich ableitet, welche Module anzuwenden sind (-> Sicherheitsmaßnahmen)

*Vorab ist zusätzlich eine Strukturanalyse durchzuführen

- Identifizierung der relevanten IT-Systeme, Netze, Anwendungen und Datenobjekte

Basismodul

Organisatorische Maßnahmen

- Festlegung von Verantwortlichkeiten, Abläufen und Aufgaben im Scanprozess
- Regelungen für Wartungs- und Reparaturarbeiten
- Abnahme- und Freigabe-Verfahren für Hardware und Software
- Aufrechterhaltung der Informationssicherheit
- Anforderungen beim Outsourcing des Scanprozesses

Basismodul

Anforderungen beim Outsourcing des Scanprozesses

- Die organisatorischen und technischen Schnittstellen zwischen Auftraggeber und Auftragnehmer (Übertragungswege, Datenablageorte, beteiligte Akteure, Rückfallverfahren, Maßnahmen zur Integritäts- und Vollständigkeitskontrolle etc.) MÜSSEN in der Verfahrensdokumentation explizit dargestellt werden.
- Der Auftragnehmer MUSS zur Einhaltung der vom Auftraggeber definierten Sicherheitsmaßnahmen verpflichtet werden.
- Es SOLL eine Analyse der durch die Aufgabenteilung zusätzlich entstehenden Risiken erfolgen.
- Zusätzlich zur regelmäßigen Auditierung SOLLEN unangemeldete Stichprobenprüfungen durchgeführt werden.

Aufbaumodule

Die Aufbaumodule bringen unter anderem folgende Änderungen mit

- Der Zugriff auf sensible Dokumente wird beschränkt
  - Räumliche Zugangsbeschränkung
  - Zusätzliche Verpflichtung der Mitarbeiter zur sorgfältigen Handhabung der Dokumente
- Es besteht eine Pflicht zur Protokollierung beim Scannen.
- Es besteht eine Pflicht zur regelmäßigen Auditierung.
- Einige „SOLL"- oder „KANN"-Kriterien werden zu „MUSS"-Kriterien
- Kryptographische Verfahren, qualifizierte Signaturen und Zeitstempel werden eingesetzt.

* Strukturanalyse, Schutzbedarfsanalyse, Verfahrensdokumentation (Anlage V), Konformitätsprüfung (Anlage P)

- Die Konformitätsprüfung erfolgt durch einen zertifizierten IT-Grundschutz-Auditor
- Das Zertifikat hat eine Gültigkeit von 3 Jahren
- Kosten (Angaben mit Vorbehalt):
  - Zertifizierungsgebühren: ca. 3.000,-€
  - Kosten Konformitätsprüfung: abh. Vom Zertifizierungsgegenstand
- Alternativ zur Zertifizierung durch BSI:
  - Auditoren-Testat
  - Konformitätserklärung

Zusammenfassung TR 03138

Die TR 03138 bringt mehr Beweissicherheit für digitalisierte Dokumente (beim ersetzenden Scannen).

Sie bringt ganz klar auch mehr Aufwand für alle Seiten mit sich.

Sie ist vor allem für die Öffentliche Verwaltung von Bedeutung.

Eine Zertifizierung nach TR 03138 ist möglich.

Es ist aber auch eine Eigenerklärung möglich.

Diskussion pro und kontra Zertifizierung

Welche Zertifizierungen haben Sie?

1. TR 03138 (Ersetzendes Scannen)
2. ISO 9001 (Prozesssicherheit)
3. EfbV (Entsorgungsfachbetrieb)
4. DIN 66399 (Datenvernichtung)
5. Datenschutzgütesiegel-verordnung (DSGSVO) für Datenträgervernichtung
6. Andere:

Warum haben Sie diese Zertifikate?

1. unsere Kunden verlangen das
2. aus Marketinggründen (wir werben mit dem Siegel)
3. als Alleinstellungsmerkmal
4. Für uns selbst (um effiziente und sichere Prozesse etablieren und erhalten zu können)

Zertifizierte Produkte - Ersetzendes Scannen aus 2016

Enteos GmbH

Ersetzendes Scannen für Scan-Dienstleistung

DMI GmbH & Co. KG

Scandienstleistung am Produktionsstandort Leisnig und der DMI Servicestelle am Standort Braunschweig der Städtisches Klinikum Braunschweig gGmbH

Universal Investment GmbH

Prozess des "Ersetzenden Scannens" der Verträge, Dokumente und Belege nach den Vorgaben der TR Resiscan unter Einbeziehung eines Dienstleisters mit TR-RESISCAN konformem Capturing-System CROSSCAP Enterprise Server

Deutschen Telekom AG

Scanprozess im De-Mail Accountmanagement

Satz-Rechen-Zentrum Hartmann + Heenemann GmbH & Co. KG (SRZ-Berlin)

Ersetzendes Scannen nach TR-RESISCAN

Zertifizierungen aus 2014 / 2015:

DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, DATEV eG, Vivento Customer Services GmbH, Mentana Claimsoft GmbH

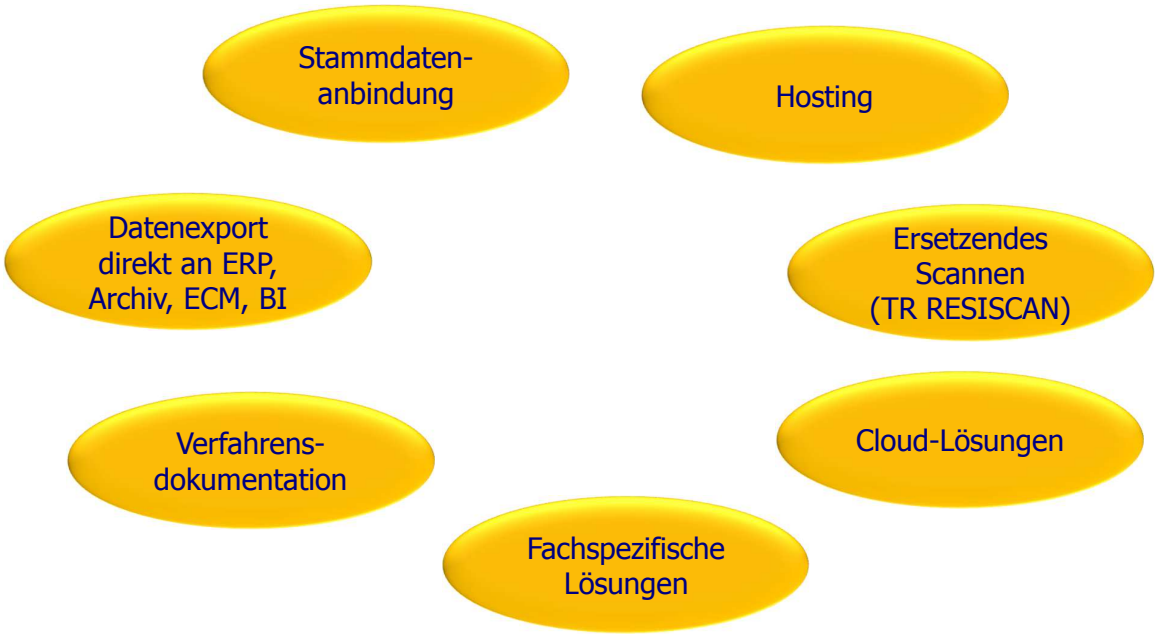
Pause

Rückblick (Vortrag 2016): Auswirkungen auf Dienstleister

Full Service Lösungen sind gefragt. Dienstleister sollten ihre „Werkbank" verlängern.

Rückblick (Vortrag 2016): Auswirkungen auf Dienstleister

Mehrwertdienste sind gefragt. Scannen alleine ist häufig nicht ausreichend.



Rückblick (Vortrag 2016): Auswirkungen auf Dienstleister

Gefragt sind Lösungen für spezielle Einsatzfelder, die ganze Prozesse oder größere Teile der Prozesse abdecken.

Automatisierte Posteingangs-lösung

Papier, E-Mail, Fax --- Scannen / Umwandlung --- Klassifizierung --- Attributierung --- Verteilung / Weiterleitung ---

Rechnungs-bearbeitung

Paper, E-Mail, Fax --- Scannen / Umwandlung --- ZUGFeRD --- Datenanreicherung --- rechtskonforme Behandlung (GoB IT, GDPdU) --- SaaS

weitere:

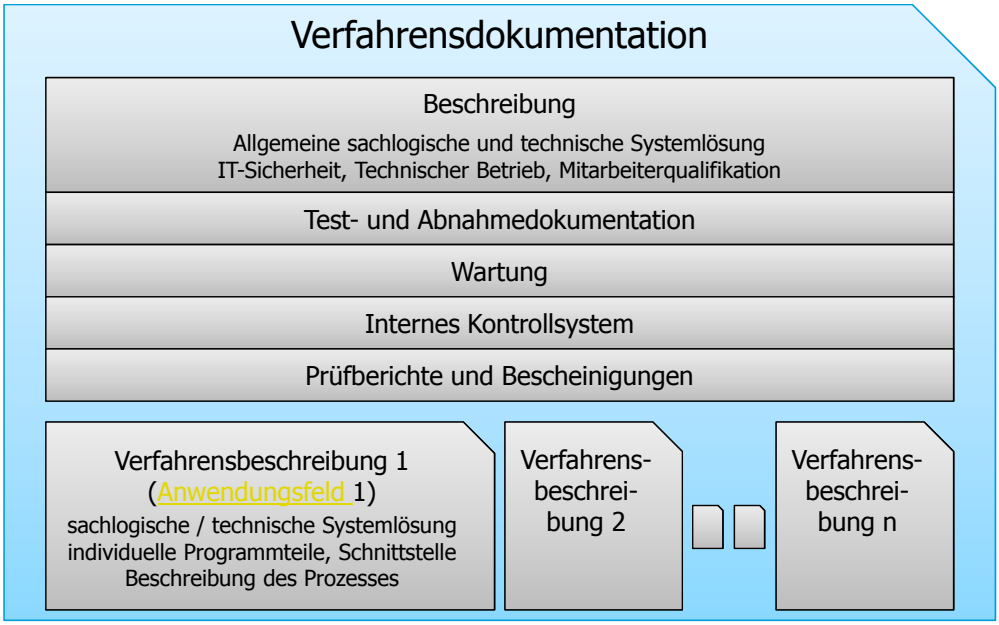
Vertragsakten / Vertragsarchiv

Personalakten

Aufbau einer VFD: Grundsätzlicher Aufbau I

Grundsätzlich erfolgt eine Aufgliederung in zwei Teile:

1. Verfahrensdokumentation (globaler Teil)
2. Verfahrensbeschreibungen Prozess 1 bis n



Aufbau einer VFD: Grundsätzlicher Aufbau II

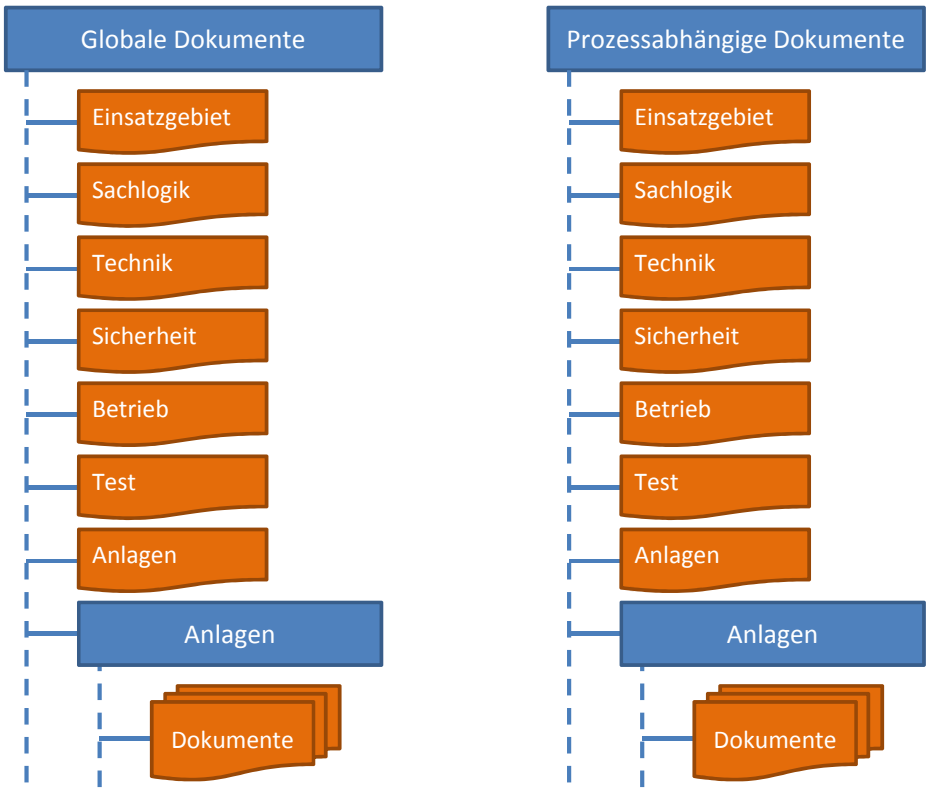
Der globale Teil beinhaltet alle Informationen, die das gesamte Unternehmen betreffen. Dazu gehören z.B.:

- Technische Voraussetzungen wie Server und Netzanbindung
- Internes Kontrollsystem (IKS)
- Brand- und Einbruchsschutzvorkehrungen
- Informationen bzw. Verantwortungen zu IT-Sicherheit und Datenschutz
- Verantwortungen für Pflege und Aktualisierung der VFD

Die Verfahrensbeschreibungen enthalten alle Informationen, die ausschließlich den beschriebenen Prozess betreffen. Dazu gehören z.B.:

- Technische Dokumentation der jeweiligen Lösung
- Sachlogischer Prozessablauf
- Verwendete Schnittstellen

Aufbau einer VFD: Kapitelübersicht

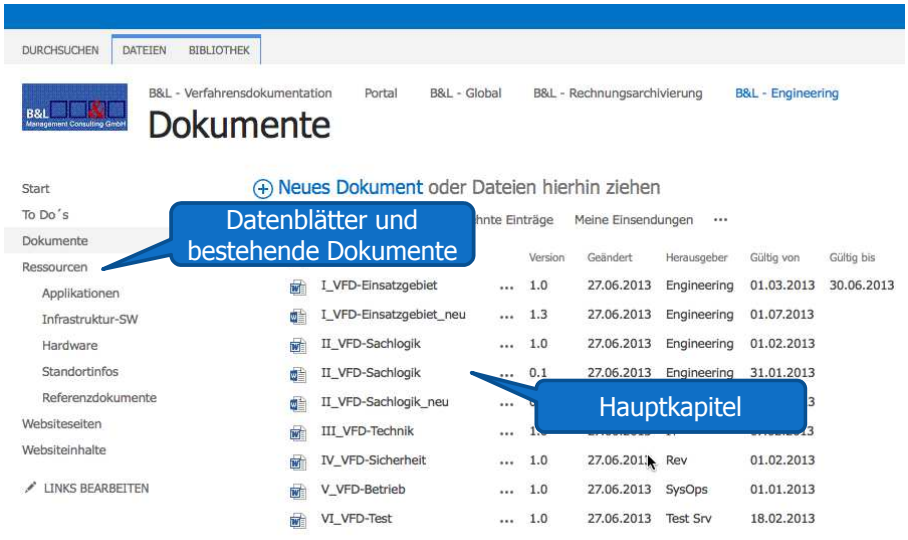


Vorgehensweise: Lösungsansatz

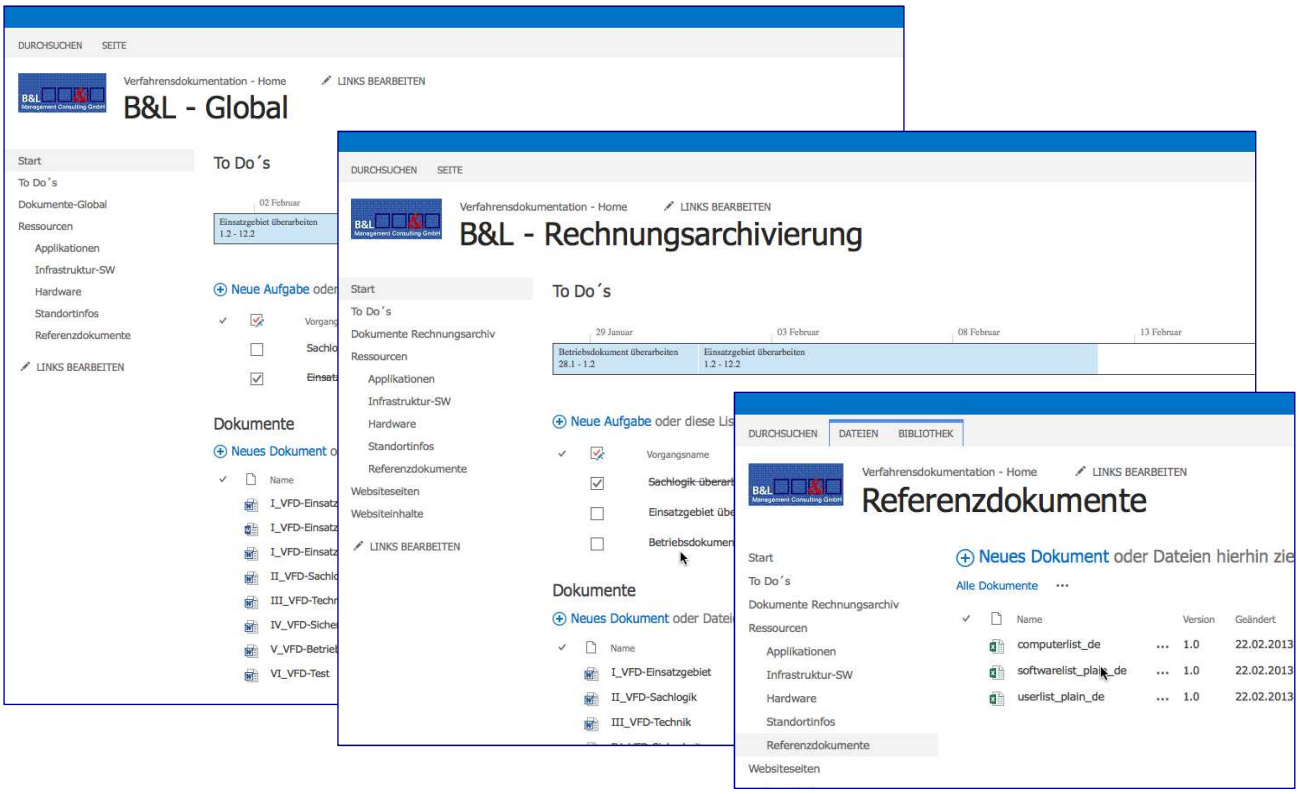
- Aufteilen
  - Verantwortung, Änderungshäufigkeit, Gültigkeit
- Am Prozess orientieren
  - Übergreifende und verfahrensspezifische Prozesse
- Strukturieren
  - Rahmendokumente, Metadaten, Tabellen, Referenzen
- Automatisieren
  - Systemdaten, System- & User-Directories, Rechte
- Zeitbezug herstellen
  - Gültig von, bis
- Zusammenführen
  - Dokumente fusionieren & archivieren

Vorgehensweise: Aufteilen

- Verteilung der inhaltlichen Verantwortung für Erstellung & Pflege auf zuständige Organisationseinheiten
- Infos bzw. Dokumente mit häufigen Änderungen in Anhänge auslagern
- Referenzierung auf bestehende Dokumente bzw. Ablagen

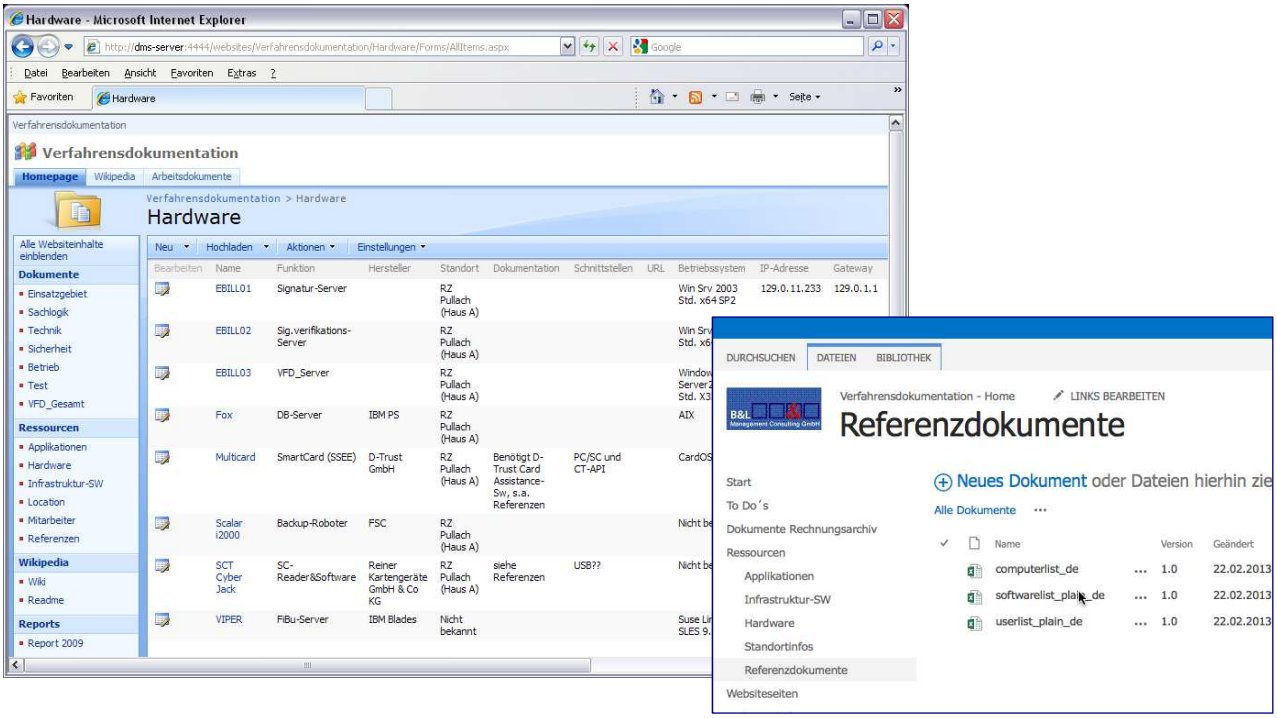


Vorgehensweise: Am Prozess orientieren



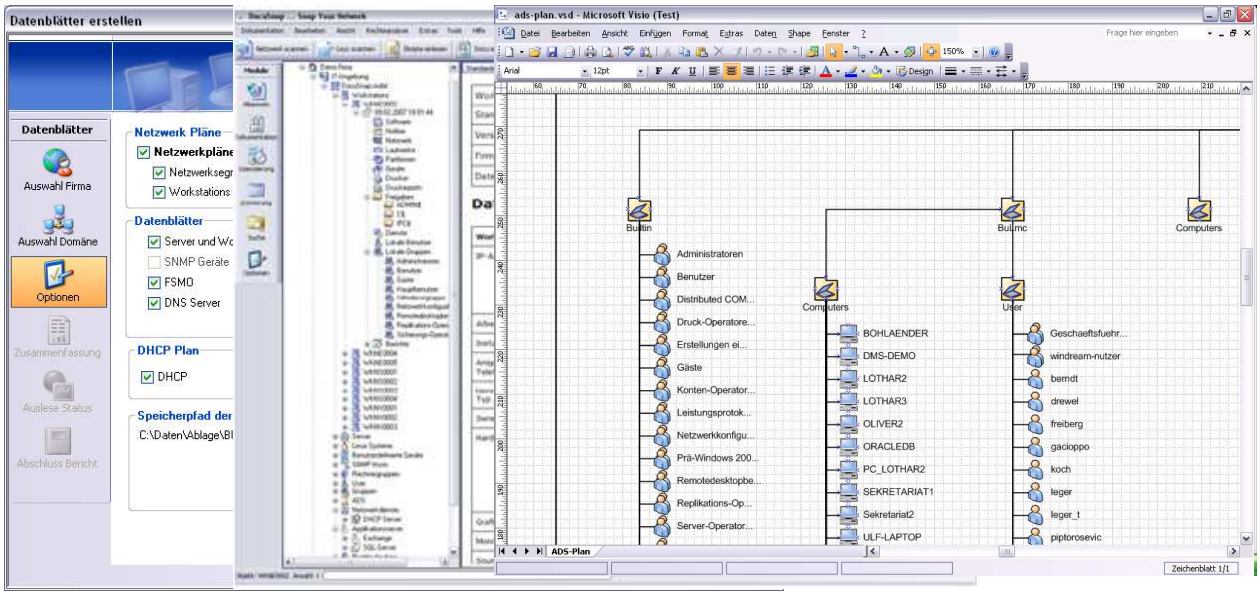
Vorgehensweise: Strukturieren

- Rahmendokumente, Metadaten, Tabellen, Referenzen



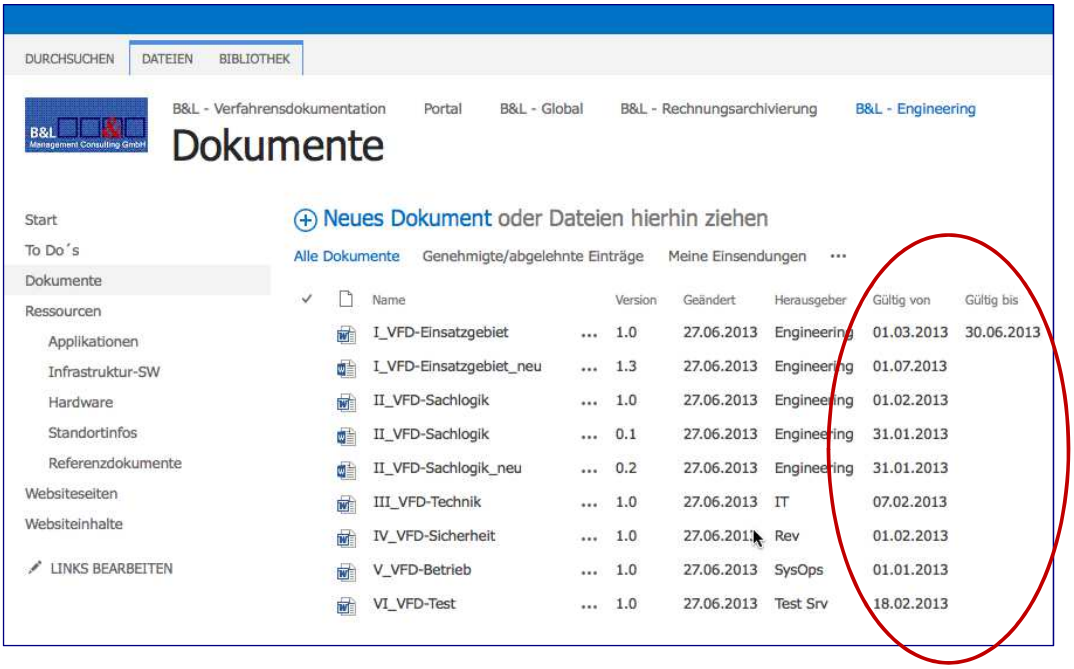
Vorgehensweise : Automatisieren

- Technische Dokumente lassen sich über entsprechende Tools (z.B. DocuSnap) automatisiert erstellen.



Vorgehensweise: Zeit- und Mandantenbezug herstellen

- Freigegebene Versionen müssen mit einer entsprechenden Gültigkeit versehen werden.



Vorgehensweise: Zusammenführen und Archivieren

- Umwandlung der Dokumente in PDF/A und idealerweise Ablage in einem Archivsystem.
- Optional: Erzeugung einer Gesamt-PDF aus den Einzeldokumenten.

Zusammenfassung

Die Verfahrensdokumentation wird verstärkt als Voraussetzung für ein Ordnungsmäßigkeit gesehen (gilt für GoBD, wie auch für TR 03138).

Die Verfahrensdokumentation ist ein gutes Mittel, um Rechtssicherheit zu verbessern oder überhaupt erst zu erlangen.

Wie bei der Zulassung von Technik (Beispiel Kfz) bezieht sich ein Zertifikat immer nur auf den individuellen Einzelfall (= auftragsbezogener Prozess), alles andere ist nur eine „Allgemeine Betriebserlaubnis".

Eine Verfahrensdokumentation unterliegt Änderungen, ein Zertifikat hat nur eine zeitlich begrenzte Gültigkeit.

Eine Verfahrensdokumentation sollte nicht nur erstellt werden, um rechtliche Vorschriften zu erfüllen. Vielmehr sollten die Mehrwerte (Qualität, Marketing / Vertrieb) ausgeschöpft werden.

Kontakt: **Lothar Leger**
B&L Management Consulting GmbH
Frankfurt / Rosenheim
Tel.: 069-133093-0 / 08031-2212374
E-Mail: leger@bul-consulting.de
Internet: www.bul-consulting.de