



OS | ECM
Version 6

**Compliance und
Mehrsprachigkeit mit**

across 
act across the border

Dr. Olaf Holst, Köln, März 2009

In den nächsten Minuten wollen wir gemeinsam die folgenden Dinge erarbeiten:

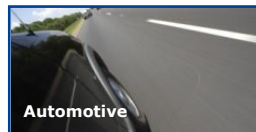
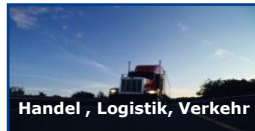
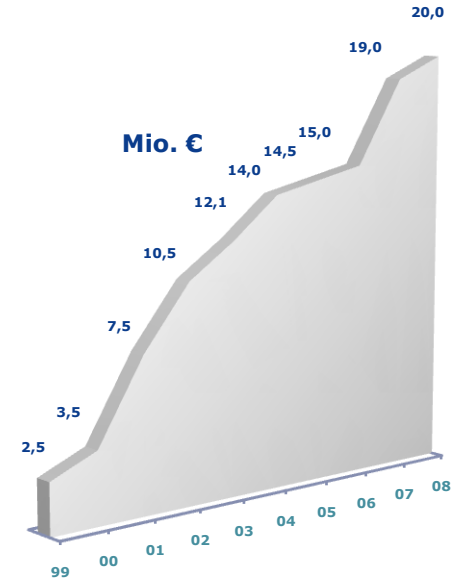
- > kurze Vorstellung OPTIMAL SYSTEMS
- > Mythen und Wahrheiten zu Compliance
- > was bedeutet „Compliance“
- > Muss ich mich damit auseinandersetzen?
- > wie funktioniert's?
- > ist da noch mehr?



Firmengründung: 1991
Geschäftsform: GmbH
Hauptsitz: Berlin
Mitarbeiter: 200
Umsatz (2008): 20 Mio.
Kunden: 700
Partner: >30

Tochtergesellschaften:
 Berlin, Konstanz, Hannover,
 Bielefeld, München, Hüfingen

Standorte europ. Partner:
 Österreich, Schweiz, Polen,
 Lettland, Ungarn



100 % ECM - Zertifizierungen



Mythen und Wahrheiten

Kein Gesetz sagt etwas zur Technologie, mit der es umgesetzt werden muss, z.B. Daten MÜSSEN elektronisch archiviert werden!

Grundsätzlich gibt es zu Gesetzen (fast) immer Durchführungsverordnungen (HGB -> AO -> GDPdU) die u.U. vom Gesetzgeber Hinweise auf zu verwendende Technologien enthalten (§14 UStG -> Elektronische Signatur bei Vorsteuerabzug)

Es gibt keine „Rechtssicherheit“ aber zum Beispiel sog. „Revisionssicherheit“! Der Gesetzgeber definiert einen Entscheidungsrahmen (GoB, GoBS) in dem die Richter interpretativ entscheiden dürfen (jede Entscheidung kann anders aussehen)

Keine Vorschrift gilt immer! Vorschriften unterscheiden sich massiv je nach juristischem Kontext (FDA gilt nicht, wenn ich nicht in den USA tätig bin oder dorthin liefere!)

Im Zweifel gilt Deutsches Recht (z.B. Persönlichkeitsrechte) vor internationalem Recht (z.B. SOX)

Wie bewahren Sie ihr Geld auf?



Wie Oma oder ...



sicher?

Wie sichern Sie sich persönlich ab?



Auf Risiko oder ... mit Krankenversicherung?

Compliance = Sicherheit ?

- **Compliance**

kein Modebegriff, sondern Übereinstimmung mit rechtlichen und regulativen Vorgaben

- **Regularien**

euroSOX, Produkthaftung, Basel II usw.

- **Dokumentationspflicht**

Archivierung des gesamten geschäftsrelevanten Schriftverkehrs für die gesetzlich vorgeschriebenen Zeiten (6, 10, 30 Jahre)

Sicherheit bedeutet den Schutz vor einer nachteiligen Veränderung des normativen Zustandes, also den Schutz vor ungewollten Ereignissen wie:

- › Unfällen (Arbeitssicherheit, Sicherheit im Straßenverkehr, ...)
- › Delikten (Verbrechensprävention, Diebstahlschutz)
- › Anschlägen (Staatssicherheit)
- › Krankheit (Schadensminderung z.B. durch eine Krankenversicherung)
- › Verlusten (Ausfallversicherung des Unternehmens)

Aber auch die Erfüllung von gesetzlichen Auflagen, auf „neudeutsch“ Compliance conformity oder Rechtssicherheit

Welche Anforderungen betreffen uns?

Was tun wir um die Gefahren zu mindern?

(Auswahl)

- Elektronische Dokumente besitzen eine identische rechtliche Bedeutung wie die Papierform
- Die Aufbewahrung von Dokumenten ist Teil des Risikomanagements
- Die Komplexität der rechtlichen Anforderungen nimmt zu
 - › Vorstände und Geschäftsführer haften im Rahmen ihrer Risikovorsorgepflicht persönlich (§ 91, 93 AktG)
 - › Mangelhafte Dokumenten-Aufbewahrung führt zur Verletzung der handelsrechtlichen und steuerrechtlichen Buchhaltungspflicht und kann bestraft werden (§ 162, 238 AO)
 - › Unzureichende oder gar manipulative Aufbewahrung von Dokumenten stellt eine Straftat dar (§ 283 ff. StGB)

- Zum Nachweis der Compliance ist Geschäftsleitung zur Dokumentation verpflichtet
- Im Rahmen der freien richterlichen Beweiswürdigung sind elektronische Dokumente bei gerichtlichen Streitigkeiten von hoher Bedeutung
- Wegen fehlerhafter E-Mail-Archivierung wurde z.B. 2002 gegen die Deutsche Bank eine Strafe von 1,65 Mio. \$ verhängt
- Nach einem Urteil des OLG Karlsruhe (2005) erfüllt z.B. das Löschen und Ausfiltern von E-Mails den Tatbestand des Unterdrückens gemäß § 206 StGB
- Alle elektronischen Dokumente sind demnach zu archivieren



- **Zugriffschutz für bereitgestellte Ressourcen**
 - › „Wer darf was?“
- **Quellensicherheit**
 - › Sind Daten vertrauenswürdig?
- **Schutz vertraulicher / persönlicher Informationen**
 - › Wer kann/darf welche Informationen lesen?
- **Schutz vor Angriffen von außen**
 - › Wie bleibt mein Netz sicher?

- **Einbruch, Datenmanipulation, -zerstörung,**
- **Informationsdiebstahl:**
Diebstahl und Missbrauch von Informationen - entweder durch Einbruch (Datenbank) oder durch Abhören (unverschlüsselte Übermittlung)
- **Identitätsdiebstahl:**
Benutzung der Identität mit betrügerischer Absicht -
Personendaten, logins
- **Distributed Denial of Service Attacks:**
durch Erzeugung unsinnigen Verkehrs wird ein Netzwerk/Server zum Erliegen gebracht
- **Web Graffiti / Defacement:**
Vandalismus, Look-and-Feel Veränderung
- u.V.m.

- **Sorgloser Umgang mit Dokumenten kann bedeuten:**
 - › Ungewissheit zu gültigen Dokumente
 - › Schaden durch unterschiedliche Versionen / Sprachen
 - › Erweiterte Haftung
- **Sorgloser Umgang bei externem Mailverkehr kann bedeuten:**
 - › Geschäftsschädigung durch Ausspähen des Unternehmens
 - › Aktivierung von Viren, Trojanischen Pferden
- **Falsch verstandene Bequemlichkeit am PC-Arbeitsplatz kann auslösen:**
 - › Unberechtigten Zugriff durch fehlenden Passwortschutz
 - › Download und verbreitung jeglicher Schadenssoftware

GDPdU– Richtlinie (Bundesfinanzministerium)

- GDPdU = Grundsätze zum Datenzugriff und zur Prüfbarkeit von digitalen Unterlagen
- ...das Datenverarbeitungssystem muss die Unveränderbarkeit der Daten gewährleisten....

Signaturgesetz (SigG)

- ...die elektronische Signatur ist der herkömmlichen „gleichgestellt“...
- Das Signaturgesetz trägt in seiner geltenden Fassung diesen Besonderheiten umfassend Rechnung, in dem es Rahmenbedingungen schafft, unter denen elektronische Signaturen als sicher gelten können.

Sarbanes-Oxley Act (SOX)/ Euro SOX

- Regelt die Haftung der verantwortlichen Manager für die Jahresabschlüsse börsennotierter Unternehmen (Euro SOX Kapitalgesellschaften)
- SOX gilt als amerikanische Regelung aber auch für international tätige Konzerne mit Schnittstellen in die USA.
- Im Rahmen der 8. EU-Direktive trat 2008 auch in Europa eine vergleichbare Verordnung in Kraft.

Basel II

- Die unter BASEL II zusammengefassten Eigenkapitalrichtlinien für Banken regeln (ab 01/06) die Voraussetzungen für die Kreditvergabe
- Die Kreditnehmer müssen in Systeme und Prozesse investieren, welche die Verfügbarkeit aller rating-relevanten Informationen sicherstellt

Handelsgesetzbuch (HGB): §§ 238, 239 und §§ 258-261

Steuerrecht (GDPdU, AO § 147, EStG, GewStG) und GoB/GoBS

- Aufbewahrungsfristen, Wiedergabemöglichkeit, Revisionsicherheit, Haltbarkeit

Zivilrecht (ZPO, BGB): Anerkennung als Beweismittel

- § 371 a Auf private elektronische Dokumente, die mit einer qualifizierten elektronischen Signatur versehen sind, finden die Vorschriften über die Beweiskraft privater Urkunden entsprechende Anwendung. Der Anschein der Echtheit einer in elektronischer Form vorliegenden Erklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung vom Signaturschlüssel-Inhaber abgegeben worden ist.
- EG-BGB nF §126 ff Ersatz der Schriftform durch die elektronische Form mit qualifizierter elektronischer Signatur

Weitere gesetzliche Rahmenbedingungen z.B.

- Produkthaftungsgesetz
- HGB § 289 „Risikomanagement“
- Fernmeldegesetz (Postgesetz, Artikel 10, Ab. 1 GG, auch z.B. §99 StPO)
- Sozialgesetzbuch für Sozialversicherungsträger
- Kreditwesen Gesetz (KWG)
- Pharmazeutische Industrie (FDA, eCTD, CFR 21, GxP Anforderungen)
- Allgemeine Deutsche Spediteurbedingungen (ADSp)
- Güterkraftverkehrsgesetz (GüKG)
- Zollbestimmungen (z.B Akkreditiv Handhabung, Exportbestimmungen)

Bundesdatenschutzgesetz

- Auswertung personenbezogener Daten (§9 BSG)
- Speicherung und Benachrichtigung (§33 BSG)
- Anspruch auf Löschung personenbezogener Daten (§35 BSG)

Betriebsverfassungsgesetz

- Unterrichtsrecht für Betriebsrat
- Mitbestimmungsrecht

Prüfsysteme und Risiko Management

Der entsprechende, gesetzliche Kontext verpflichtet Kapitalgesellschaften unter Androhung von Bußgeld (§334 HGB) zur Bewertung von Risiken oder das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“, kurz KonTraG, z.B.:

Marktrisiken und –chancen wie

- > Volkswirtschaftliche und politische Entwicklung
- > Wettbewerber, Kunden, Lieferanten, Rohstoffe
- > Neue Produkte und Ersatzprodukte bzw. Dienstleistungen

Finanzrisiken und –chancen wie

- > Zinsänderungen
- > Wechselkursänderungen, ...

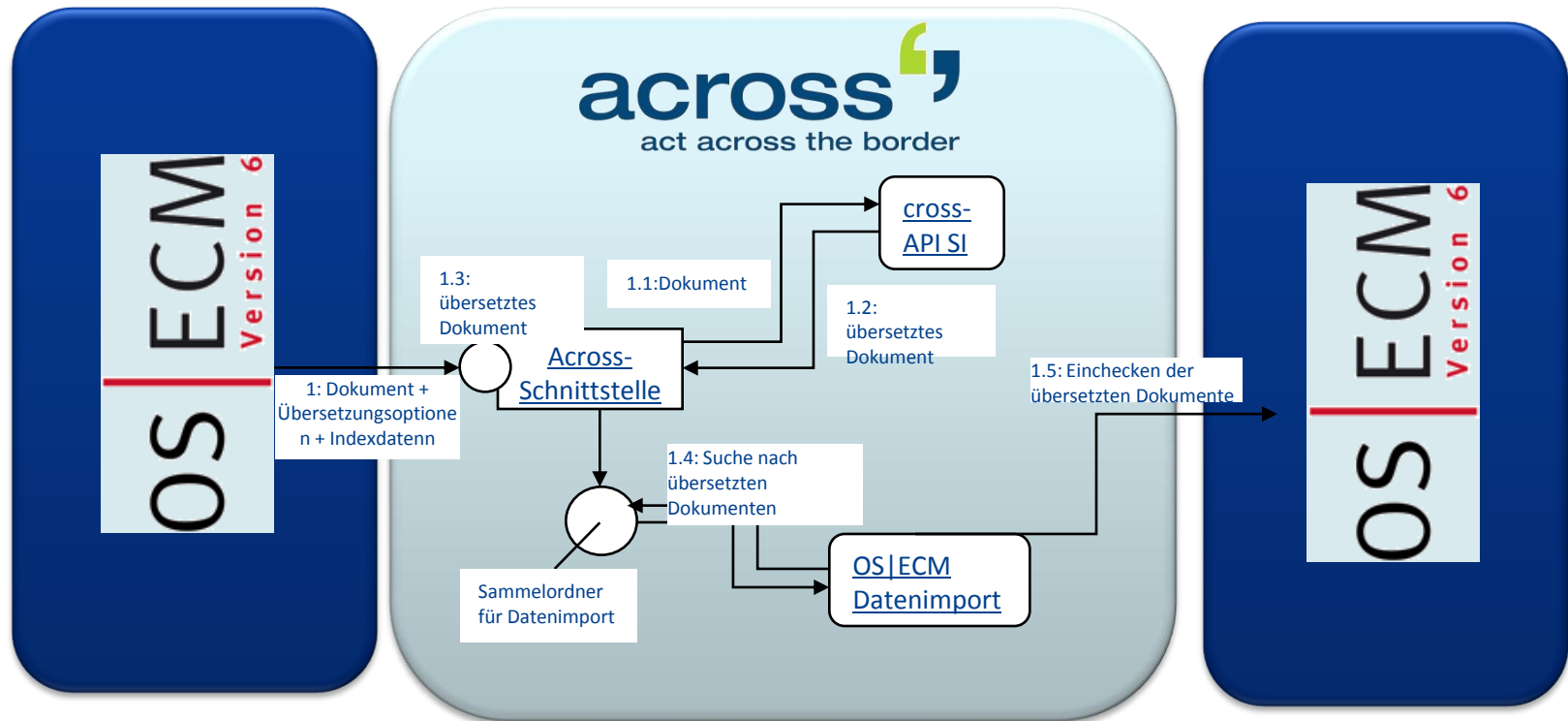
Rechtsrisiken- und Chancen wie

- > Bestehende Gesetze, Verordnungen sowie Rechtsentwicklung in Zielgebieten
- > **Produkthaftung**
- > Gerichtliche Prozesse
- > **Lizenzen, Patente, Genehmigungen, Erlaubnisse**
- > Risiken durch Betrug, Erpressung und andere Delikte, ...

Sonstige interne Risiken und Chancen wie

- > Organisation
- > Personal
- > F & E, ...

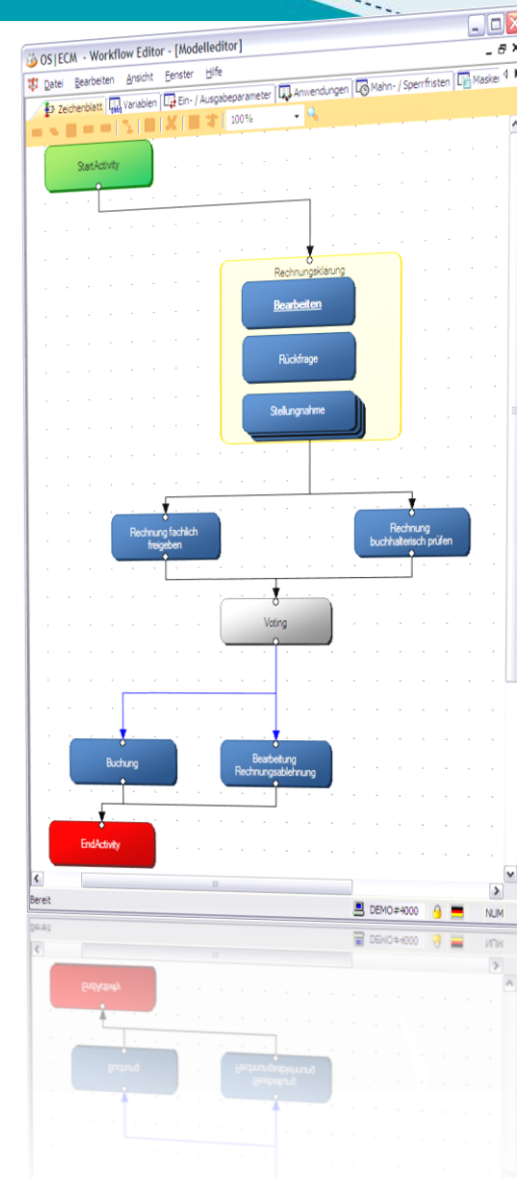
Aufbau der Lösung



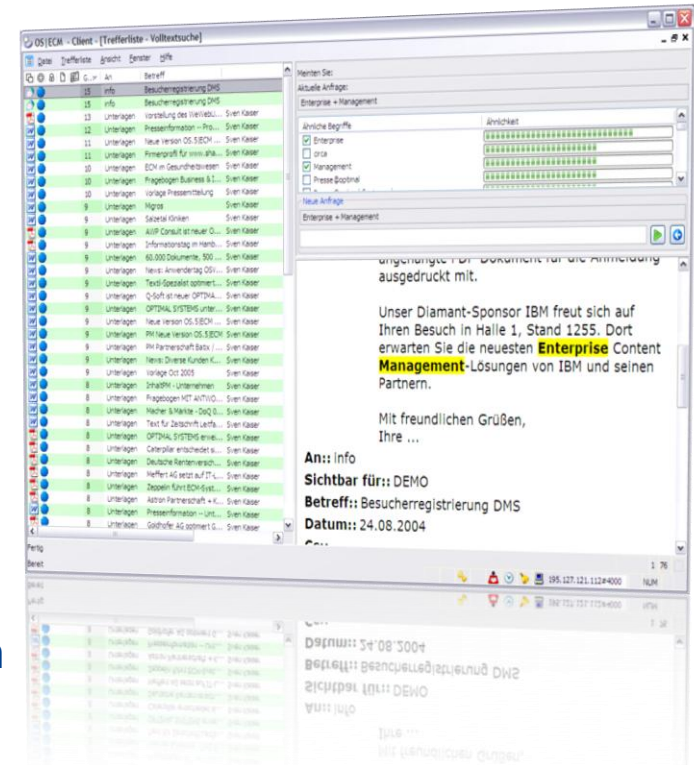
Mehrwerte durch die Kopplung

- › **Ad-hoc-Bereiche** innerhalb strukturierter Workflows
Abbildung spontaner Prozesse
Reaktionsfähigkeit auf variable Anforderungen
- › Erstellung von **Lauflisten**
Auswahl von Empfängern, Aktivitäten und Fristen
- › Einbindung von **Vorlagen** und **Favoriten**

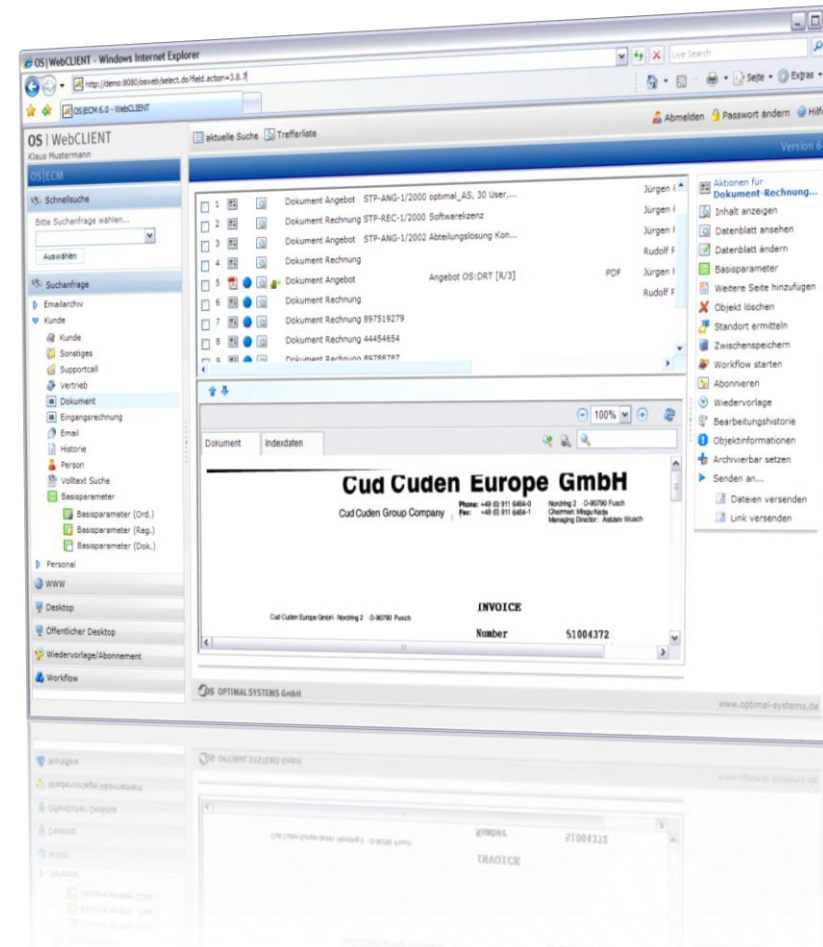
Beispiel: Ein Übersetzer kann seinen Arbeitsvorrat an besser geeignete Kollegen abgeben, Informationen einholen und Freigaben erbitten.



- › Verwendung verschiedener Volltext-Engines (Microsoft Search, Apache Lucene)
- › **Contentmining:** Treffergüte und Hervorheben der Suchbegriffe im Contentviewer
- › **Intelligente Suchverfahren:**
 - › Semantisch-assoziative Suche von „Ähnlichen Begriffen“
 - › Automatische Klassifikation von Texten
 - › „Unschärfe“ Suchmethoden zur Erkennung von fehlerhaften Zeichenfolgen
 - › Volltextrecherche auch in gescannten und sonstigen Bilddokumenten durch Einbindung der serverseitigen OCR für die Schrift-Erkennung
 - › Einbindung von Thesauri



- › **Dynamisch** erzeugte HTML-Seiten und Cascading Style Sheets Technologie (CSS)
- › Moderne und funktionale Benutzeroberfläche
- › **Mehrsprachigkeit**
- › **Recherche** über den gesamten Datenbestand
- › **Ein- und Auschecken** von Dokumenten
- › Hinzufügen neuer Dokumente per **Drag & Drop**
- › Zugriff auf die **Variantenverwaltung**
- › **OS|ECM-Contentviewer** integriert
- › **Abonnement** und **Wiedervorlage**
- › **Workflow** „im Web“
- › Vorlagen für Office-Programme
- › **Scannen** direkt über den Browser



Einbindung von Office-Programmen

Rendition



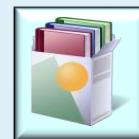
Wiedervorlage
Abonnement

Volltext



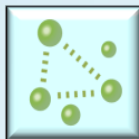
Erfassung
Klassifizierung

Versionierung



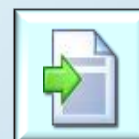
Compound Documents

Datenaustausch
und Integration



E-Mail und Fax

Digitale Signatur



Dokumente aus
vorhandenen Daten

Dokumenten
management



Archiv



Workflow-Management

OS | ECM
Version 6

Fazit

Risikoabschätzung

- Bewertung der materiellen u. immateriellen Vermögen und Betriebsmittel
- Schwachstellen ermitteln
- Bedrohung der Unversehrtheit, Vertraulichkeit, Verfügbarkeit

Sicherheitskonzept

Schutzmaßnahmen

- physikalische Sicherung
 - Zugangsschutz, Brandschutz, USV, Cluster, etc.
- Revisionssicher Archivierung
- Dokumentenmanagement
- Freigabeprozesse
- Identity Management
- Business Continuity Concept

Notfallkonzept

- > Prüfen Sie immer welche Vorschriften tatsächlich für Sie gelten
- > Binden Sie möglichst früh die Behörden ein, die für die Prüfung zuständig sind
- > Es gibt die Chance sich maximale Sicherheit zu verschaffen, in dem man versucht möglichst viele Vorschriften zu erfüllen, z.B. „revisionssichere Ablage“
- > Schaffen Sie einfache Lösungen! Nur einfache Lösungen werden auch gelebt
- > Wenn Sie unsicher sind, holen sie sich fachliche Hilfe und ...

- > nutzen Sie Technologien wie  und 

OPTIMAL SYSTEMS

Gesellschaft für innovative Computertechnologien mbH

Cicerostraße 26

10709 Berlin

Tel.: 030 – 8 95 70 80

Fax: 030 – 8 95 70 88 88