

SAP Governance, Risk & Compliance bei

LEDERUNDSCHUH INTERNATIONAL AG^{LS}

DI Hubert Petz, CPIO

SAP World Tour, 18.9.2008, Linz

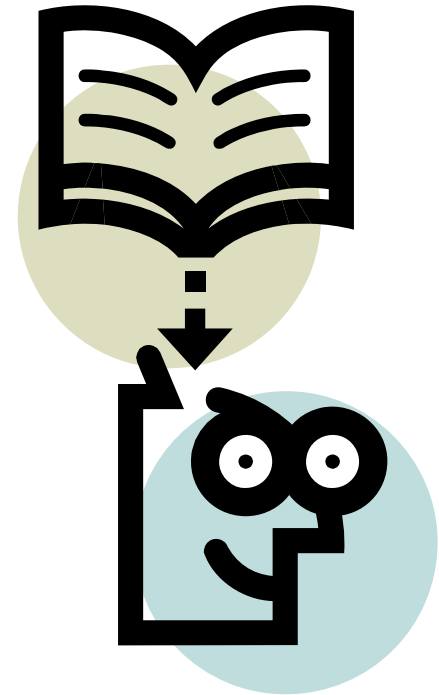
CORTI DOMINICI HUMANIC



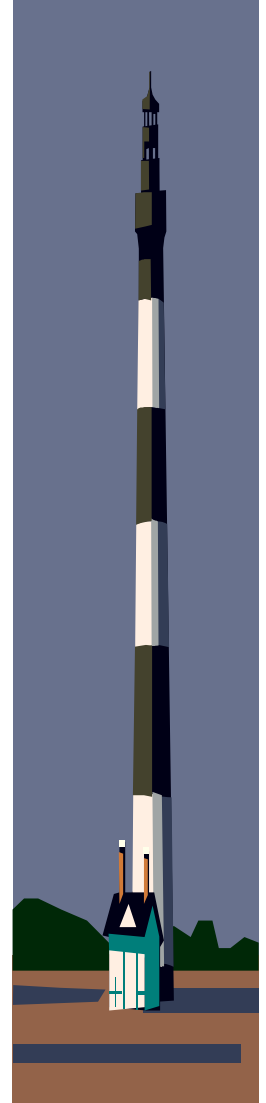
... ein Projekt für das Sie
- von wenigen
- ein wenig Lob ernten werden.
So what!



- **Ursachenforschung**
- **Entscheidungen bei LS**
- **Umsetzung Berechtigungsmanagement**
- **Learnings**
- **Die LS International AG**



- Firmenpleiten (Enron, Worldcom u.a.) durch Laschheit und Betrug
- Reaktion 1: Angst
- Reaktion 2: Gesetze
- Reaktion 3: Methoden und Mittel zur Gesetzesüberwachung
- Reaktion 4: Wir benötigen Systeme dazu!



- Einfaches Gesamtsicherheitskonzept nach BS 7799/ISO 17799 mit Vorstand

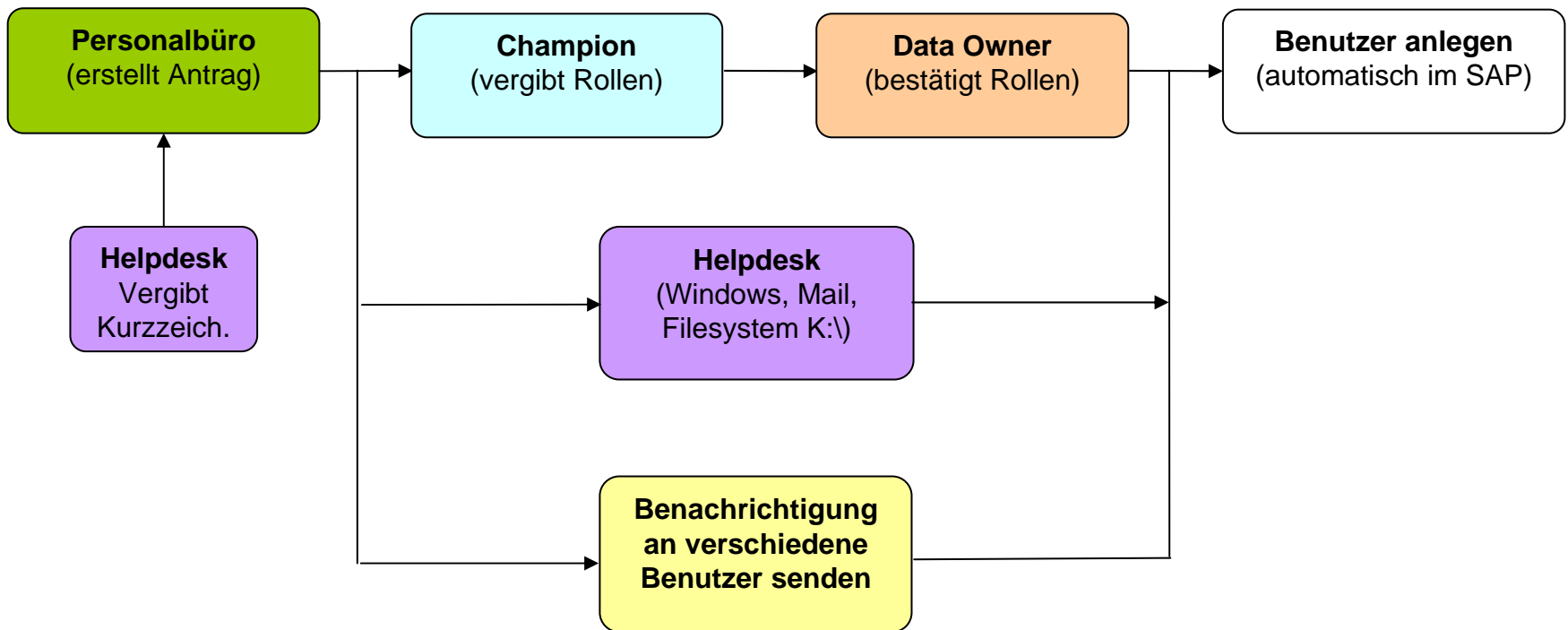


- **Aufsplittung in Verantwortungsbereiche**
- **IT-Grundschutz: Ehrliche Bewertung und Risikoermittlung**
 - Organisation und physische Sicherheit
 - Netze, Server, Clients, Datenbanken, Viren, Intrusionprevention, Spam, ...
 - Sicherung, Backup
- **Berechtigungssysteme: 1. Priorität SAP**
 - Standardisierung
 - Automatisierung (Neu, Änderungen, Doku)
 - Den EU-Gesetzen vorauseilende Realisierung

- **Lösungssuche**
 - Selber machen (Excel-Monster, ...)
 - CA eTrust, CheckAud, ...
 - SAP GRC Suite
- **Entscheidung 12/06 für SAP GRC Suite**
 - **Compliance Calibrator (CC)**: Analyse, Erkennung und Sanierung von Risiken bei Zugriffsrechten
 - **Access Enforcer (AE)**: Regelkonforme Vergabe von Benutzerrechten
 - **Firefighter (FF)**: Kontrolle von Superusern
 - **Role Expert (RE)**: Definition/Verwaltung von Rollen

- **Beraterauswahl**: PwC
 - Externe Moderation der Workshops
 - Fachwissen zu IKS
 - Deckung durch Prüferzertifizierung
- **Implementierung CC, AE, FF**
 - Verzögerungen bei GRC-Release 5.2
 - Kick Off 5/07 durch Vorstand + sämtliche Verantwortliche + IT
 - Workshops + paralleler Aufbau durch IT/PwC
 - Techn. Projektabschluss 1/08
 - Danach: Aufräumarbeiten (Änderungen, Neuaufbau Rollen) bis 5/08
 - RE: Noch zu unreif

- Nutzen: Bereinigte bzw. bekannte Risiken
 - Transparenz und Verprobung bei Rollenvergabe
 - Handling von „Personalunionen“
 - Bewußtsein (trotz Jammerei)
- Dokumentierte Workflows: Beispiel Eintritt



- Ein derartiges Projekt ist ausschliesslich mit Artikulation und Unterstützung durch den Vorstand machbar
- Sinn bzw. Notwendigkeit sind permanent in Erinnerung zu rufen
- Zertifizierte Implementierung (Berater)
- Rolle des Controllings ist gefordert
- Verständnis für „Functionowner“ und „Dataowner“ muss aufgebaut werden
- Streitfälle ausschliesslich über Vorstand und Controlling regeln
- SAP GRC 5.3: Reifegrad weiter steigerbar, RE?
- Aufräumen kostet Kraft, Geduld und Ausdauer



- Modeunternehmen im Schuhhandel

 CORTI DOMINICI HUMANIC



- Aktuell ca. 320 Filialen in 8 Ländern:
AT, DE, PL, CZ, SK, HU, SI, RO
- Umsatz 2007 455 Mio €
- Ca. 800.000 Artikel
- Ca. 3300 Mitarbeiter, davon fast 50%
international
- Unternehmenszentrale in Graz

VIDEO

Herzlichen Dank!

