Erfahrungen aus dem Alltag

KRITIS DO'S AND DON'TS

JESTER SECURE iT

KRITIS Do’s and Don’ts

- KRITIS Do's and Don'ts
- Scope
- Organisation
- Dokumente
- Risikomanagement
- Operative Aufgaben
- Berichtswesen
- Nachweise
- Auditvorbereitung

KRITIS Do's and Don’ts
Erfahrungen aus

- 13 Energieversorger (SW, ÜNB, VNB)
- 3 KRITIS 8a Unternehmen
- 0 B3S

Scope

- **Separates Dokument**
  - Kontext: Umfeld
  - Anforderungen interessierter Parteien
  - Netzstrukturplan (auch separat)
- **Beschreibung der kDL**
- **Abgrenzung /Schnittstellen**

- **16:0**

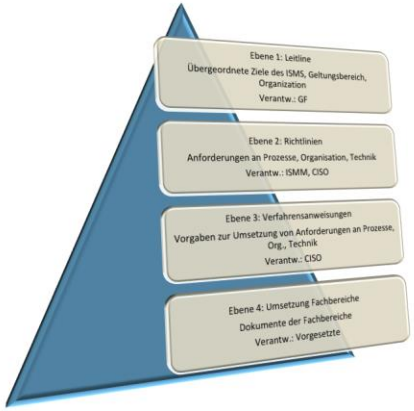
Organisation

- **ISB nach BSI Definition**
  - 3x Firewall Admin als ISB
  - 2x Leiter Leitstelle
  - 6x Bereichsleiter Technik
- **Rollenbeschreibung generisch**
  - Keinen/wenig Bezug zur kDL
- **Do’s sind Organisationsabhängig**
  - Affinität Management
  - Affinität IT, InfoSec
- **10:6**

Dokumente

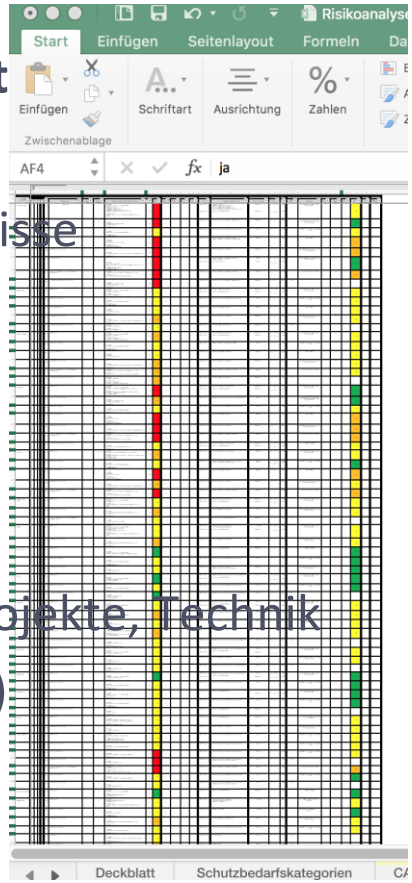
- **Pflichtdokumente**
  - Übernahme vom Berater – jede Menge
  - Inhalt generisch und ohne konkreten Bezug
  - Inhalt von anderem Unternehmen

- **Kürdokumente**
  - Nachweise fehlten
  - 0:16
- **Do's**
  - Strukturieren und behalten
  - Vorhandenes DMS beachten
  - Freigabeverfahren vereinfachen



Risikomanagement

- **Vorgabe der Berater**
- **Excel Tapeten - erst Ausdruck A0 ergibt eine Übersicht**
  - All-Gefahren Ansatz formell erfüllt
  - Kein Verständnis für Vorgehensweise und Ergebnisse
  - Aktuelle Bedrohungen nicht bewertet
- **1:15**



- **Do's**
  - Muss operative Arbeit unterstützen: Prozesse, Projekte, Technik
  - Top 5 Risiken sichtbar (Management Verständnis)
- **Don't:**
  - Excel (nicht auf lange Sicht)

Operative Aufgaben

- **F: Hr. ISB, wie sieht der Plan aus für Ihre Arbeit im nächsten Jahr?**
- **A: 😮 …***
- **0:16**

- **Do's**
  - Tagesaufgaben: Vorfälle
  - Wochenaufgaben: Projekt Begleitung, Risiko Analysen
  - Monatsaufgaben: InfoSec Team anleiten, Führungskreise informieren
  - Quartal…, Jahr…
  - Risikoanalysen zu Vorfällen, Meldungen, Patches, Projekten
- **Don't**
  - Projektende ist ISMS Ende

* Berater springt ein: Ich werde weiterhin kommen und Sie unterstützen, stimmts?

Berichtswesen

- **KPI** **0:16**
  - Berater gibt 6 KPI vor
  - Messung = ausfüllen des KPI Berichtes
- **Audits** **6:10**
  - durch MA derselben Berater-Firma
  - Auditbericht = Excel Sheet, ohne
- **Management Review** **0:16**
  - PPT inhaltlich wie Statusreport – wenig konkretes

- **Do's:**
  - KPI sollten Ziele untertstützen & KPI regelmäßig messen (M/Q/J)
  - Unabhängige Auditoren – Audit Bericht muss was hermachen
  - Management Bericht muss was hermachen

Nachweise

- **“Tu Gutes und mache Notizen!”**
  - KPI Messungen
  - Auditberichte / Auditprogramm
  - Korrekturmassnahmen

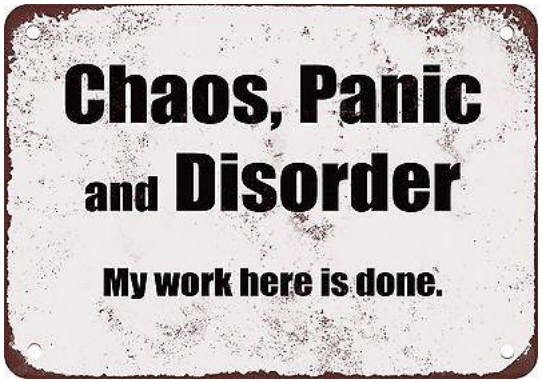
Schlußwort

- Meine liebsten Berater Kommentare:

Wir haben doch die Vorlage vom BSI genommen…

Der andere Auditor hat uns dafür gelobt…

Komisch, bei uns hat das gepasst…



Leistungstest

- **Was habe ich nicht erwähnt?**

JESTER SECURE iT