zentric
Intelligent Solutions

Firmenporträt

Ihr IT-Partner für
Ihre Sicherheit

zentric
Intelligent Solutions

Zur Person

Thomas Conrad

Senior Cyber Security Consultant

- CISSP
- CISA
- CDPSE

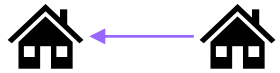
Zentric GmbH -- Zug

IT-Sicherheitskonzept // IT-Security Konzept

Eine Ortsbestimmung…

Für das eigene Unternehmen

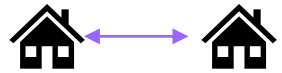
- Informationsverbund
- Angestrebtes Sicherheitsniveau (C-I-A)
- Risikoanalyse



Vom eigenen Unternehmen für Kunden/Regulatoren…

- Zertifizierungen (ISO27k)
- SOC2 / ISAE
- C5
- Complianceguidelines

Thema heute

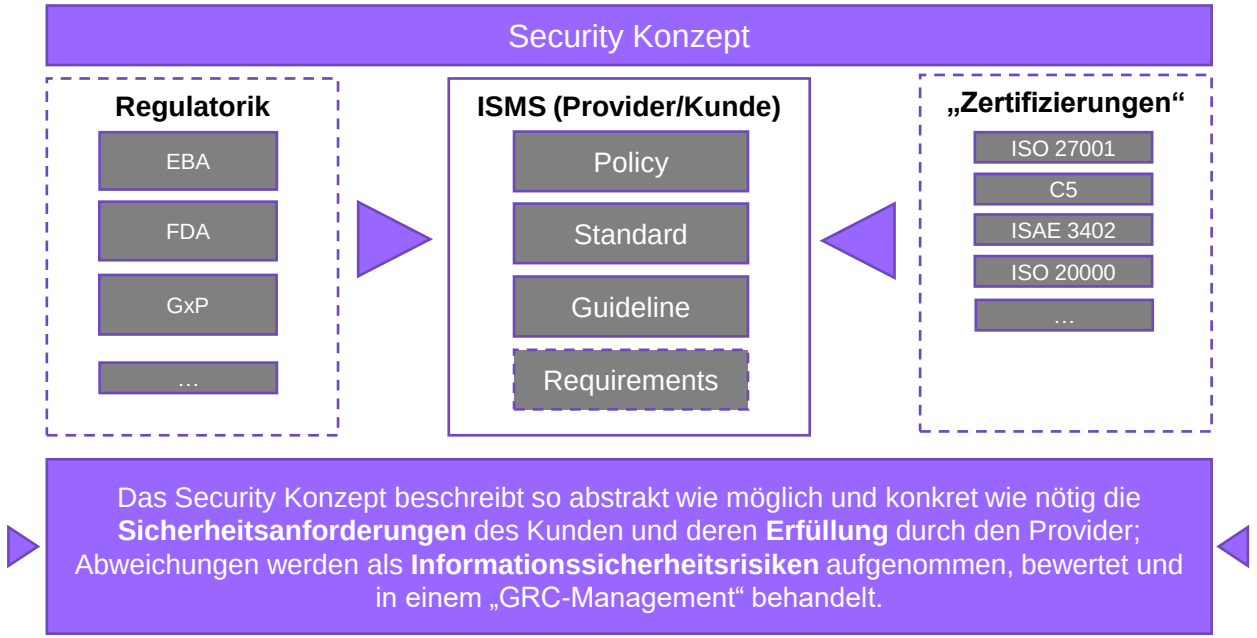


Für Kunden (Outsourcing)

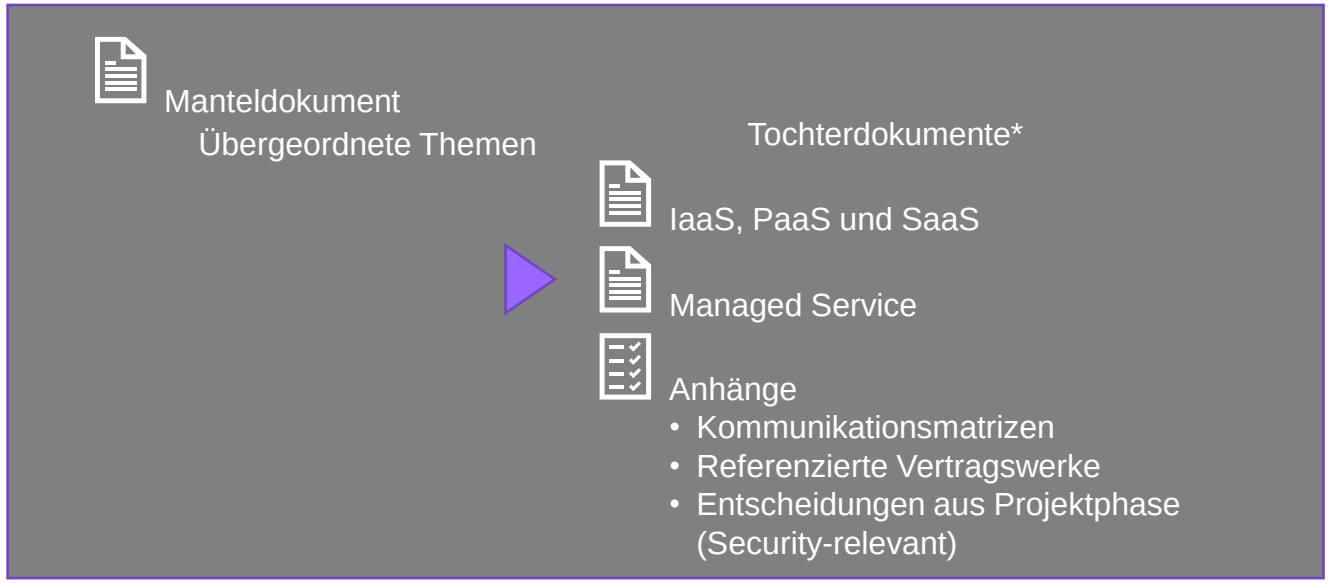
→ Folgefolien

Sicherheitskonzept vermittelt zwischen Kunden und Provider

Sicherheitskonzept



Aufbau des Sicherheitskonzepts



*ein Tochterdokument je Service

Sicherheitskonzept: Inhalte und Vorgehen – Empfehlungen aus der Praxis

Sicherheitskonzept

0 Verzeichnisse

0.1 Inhaltsverzeichnis

Kunde	Provider
Zulieferung Security Baseline	
	Abgleich Sicherheitsarchitektur Provider – Erstellung Architektur des Sicherheitskonzepts (Version 0.2) (Identifikation von Abweichungen und Handlungsbedarfen)
Abnahme Architektur Sicherheitskonzept	
	Erstellung First Draft (Version 0.4) (IT-Sicherheitskonzeption (Klassifizierung der Daten, Festlegung Schutzbedarf) sowie IT-Sicherheitsrichtlinien)
Review (Abnahme) Version 0.4	
	Erstellung Final Draft (Version 0.8) (Detaillierung des Sicherheitskonzepts, Definition von technischen und organisatorischen Maßnahmen (TOMs*), Erarbeitung Risiken)
Review (Abnahme) Version 0.8	
	Veröffentlichung Final (1.0)

*Spezielle Kunden-TOMs – nicht „Datenschutz-TOMs“

zentric
Intelligent Solutions

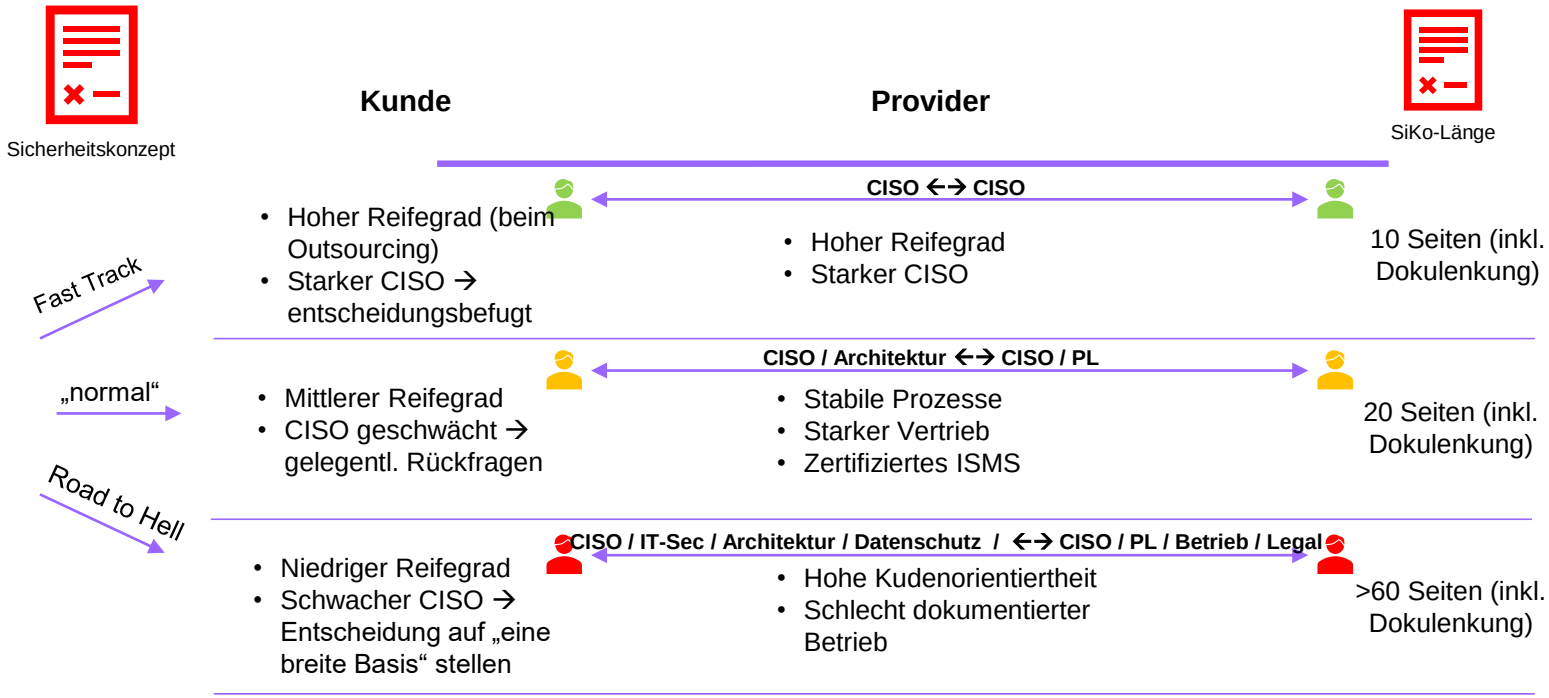
Sicherheitskonzept: Und was alles schief gehen kann…

Sicherheitskonzept

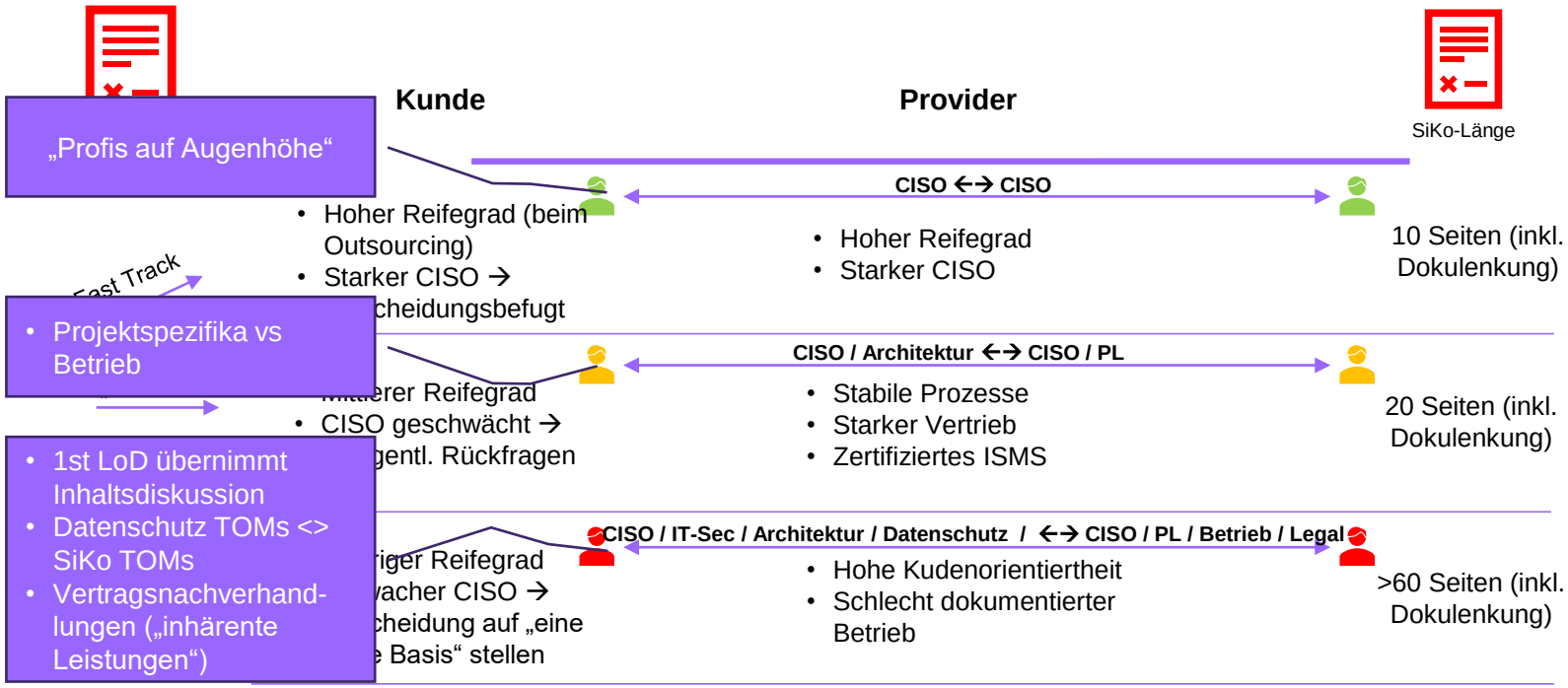
	Kunde	Provider	SiKo-Länge
Fast Track	• Hoher Reifegrad (beim Outsourcing) • Starker CISO → entscheidungsbefugt	• Hoher Reifegrad • Starker CISO	10 Seiten (inkl. Dokulenkung)
„normal“	• Mittlerer Reifegrad • CISO geschwächt → gelegentl. Rückfragen	• Stabile Prozesse • Starker Vertrieb • Zertifiziertes ISMS	20 Seiten (inkl. Dokulenkung)
Road to Hell	• Niedriger Reifegrad • Schwacher CISO → Entscheidung auf „eine breite Basis“ stellen	• Hohe Kudenorientiertheit • Schlecht dokumentierter Betrieb	>60 Seiten (inkl. Dokulenkung)

zentric
Intelligent Solutions

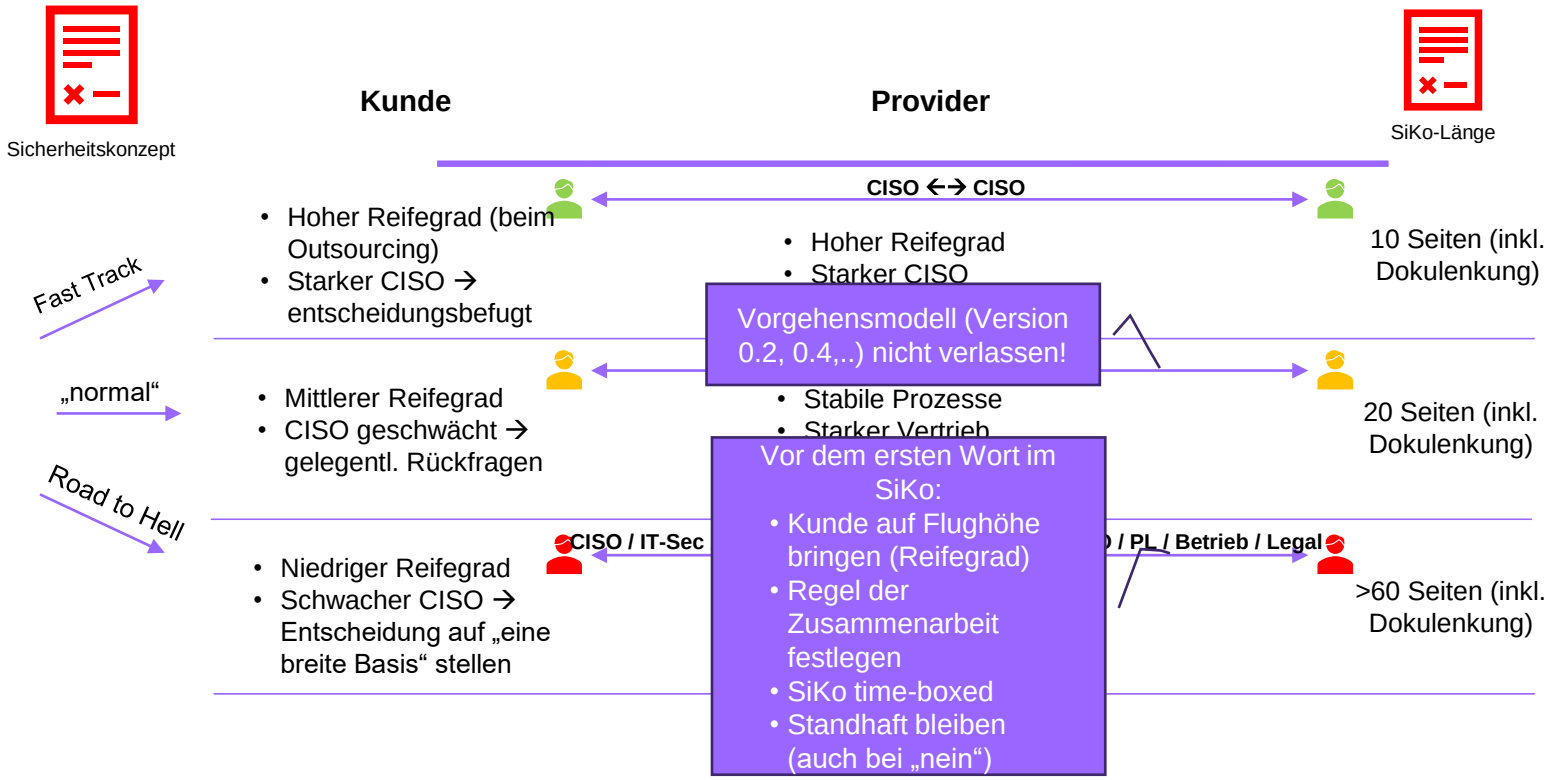
Sicherheitskonzept: die „falschen“ und die „richtigen“ Player…



Sicherheitskonzept: Viele Köche verderben den Brei



Sicherheitskonzept: Gegenmassnahmen (aus der Praxis)



Sicherheitskonzept: Zusammenfassung

Sicherheitskonzept

Wichtigste Inhalte

- **Shared Responsibility**
- **Risikoinventar (und Abgrenzung zu „GRC“-Risiken im Betrieb)**

Wer sollte **nicht** mitmachen?

- **1st LoD**
- **Datenschutz**
- **Architektur**
- **Projektmanagement / Vertrieb**

Hauptproblemfelder

- **Mangelnder Reifegrad**
- **Falsche Vorstellung von Funktion des Sicherheitskonzepts**

zentric
Intelligent Solutions

Abschluss…