

# KRITIS SECURITY MANAGEMENT



## Projektverlauf „KRITIS Security Management“

### 1 BESTANDSAUFNAHME

#### Ganzheitliche Modellierung

Modellierung aller Security-relevanter Bestandteile und eigens entwickelte Software, speziell zugeschnitten auf IT-Sicherheit

- › Infrastruktur
- › Technik
- › Organisation

 Ganzheitliches Modell

#### Security Audit

Erfassung des Status Update zum ISMS im Abgleich mit gängigen Normen

- › Managementstruktur ISMS
- › Abgleich mit ISO 27001, B3S
- › Personal und Schulung

 GAP Analyse ISMS

### 2 RISIKOANALYSE

#### Bedrohungen und Schwachstellen

Top-Down Risikoanalyse für Gebäude, Systeme und Prozesse

- › Konform zu ISO 27005/ IEC 62443-3-2
- › Ganzheitliche Identifikation aller Bedrohungen und Sicherheitslücken

 Angriffsbaum

#### Risikobewertung

Analysen von Sicherheitslücken und Bedrohungen mit Risikobewertung

- › zusätzliche Schutzmaßnahme
- › Vergleich der Risiken

 Risikomatrix & Liste der Restrisiken

### 3 MASSNAHMENKATALOG

#### Maßnahmendefinition

Priorisierter Katalog für bauliche, technische und organisatorische Maßnahmen

- › Reduktion von Risiken
- › Verbesserung des ISMS

 Maßnahmenkatalog & Abschlussbericht

#### Gesamtkonzept

Sicht auf interne und externe Risiken führt zu vollständiger Absicherung

- › Risikobasiert
- › Begleitung des Unternehmens
- › Aufbau des ISMS


 Priorisierung, Umsetzungsplan & ISMS-Dokumente

### 4 AWARENESS

#### Trainings

Geschulte Mitarbeiter als wichtige Ressource zur Aufrechterhaltung der Sicherheit

- › Schulungsbedarf ermitteln
- › Mitarbeiterschulungen

 Schulungsunterlagen, Teilnahmeprotokolle

#### ISMS Kontrolle

Begleitung bis zur Überprüfung der korrekten Umsetzung eines umfänglichen Sicherheitssystems

- › Überprüfung und Weiterentwicklung
- › Interne Audits

 Aktualisierte IT-Sicherheitsrichtlinien, interne Auditberichte

## Referenzen

- › DB, Projekt DiB: Netzwerkkonzept: Modellierung Gebäude, OT-Systeme und Vernetzung
- › DB & SBB: Security Audits: Bewertung der konzernweiten Prozesse und Richtlinien Betriebsführungskonzepte: Beschreibung neuer Prozesse für sichere Betriebsführung, Gebäude- und IT-Management
- › Risikomanagement SBB & DB: Ganzheitliche Assessments: Angriffsbäume, Risikobewertung, Maßnahmenkataloge (TÜV-zertifiziert)
- › DEKRA: ISO Schulungen: Ausbildung von Information Security Officern

- › Diverse Projekte: ISMS & TISAX Beratung: Von IST-Analyse bis Zertifizierungsbegleitung ISMS Kontroll-Audits: Rezertifizierungsvorbereitung

**PATRIC BIRR**  
M. Sc., CISSP  
Head of Business Center Security  
Mobile: +49 172 728 05 80  
E-Mail: Patric.Birr@ics-gmbh.de