

GOVERNANCE, RISK & COMPLIANCE - CHEAT SHEET

Wichtige Frameworks, Standards & Best Practices auf einen Blick

Erstellt am 9. Juni 2026

Disziplin



GOVERNANCE & STRATEGIE

(Fundament und Führung)



INFORMATION SECURITY

(Schutz der Assets)



RISK MANAGEMENT

(Identifikation & Steuerung)



BCM & RESILIENCE

(Überleben im Ernstfall)



Konzeptionell & Regulatorisch



COBIT

(Brücke zwischen Business & IT)



ISO/IEC 38500

(Corporate Governance of IT)



ISO/IEC 27001

(ISMS Fundament)



NIS-2

(EU-Infrastruktur-Pflichten)



DORA

(Resilienz im Finanzsektor)



ISO 31000

(Unternehmensweiter Risiko-Kompass)



COSO ERM

(Enterprise Risk Management
- v.a. Finance)



ISO 22301

(BCM Standardwerk
= was?)



BSI Standard 200-4

(DACH-BCM
Klassiker; = wie?)

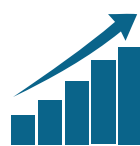


Best Practices & Operative Umsetzung



ITIL 4/5

(IT-Service-Management)



CMMI

(Prozess-Reifegradmodell)



ISO/IEC 27002

(93 konkrete Controls)



NIST CSF 2.0

(106 konkrete Controls)



CIS Controls

(18 Baseline Controls)



ISO/IEC 27005

(Spezifische IT-Risiken)



NIST SP 800-30

(Praktische Risikobewertung)



ISO/IEC 27031

(ICT Bereitschaft für BCM)



NIST SP 800-34

(IT Contingency Planning, v.a. US-Behörden)



Hinweis:

Die Frameworks ergänzen sich. Sie decken unterschiedliche Perspektiven ab, von der strategischen Führung bis zur operativen Umsetzung und Resilienz im Ernstfall.



Governance gibt Richtung vor und stellt Werte sicher.



Security schützt Daten, Systeme und Prozesse.



Risk Management identifiziert Risiken und steuert sie.



BCM & Resilience sichern den Fortbestand im Ernstfall.

