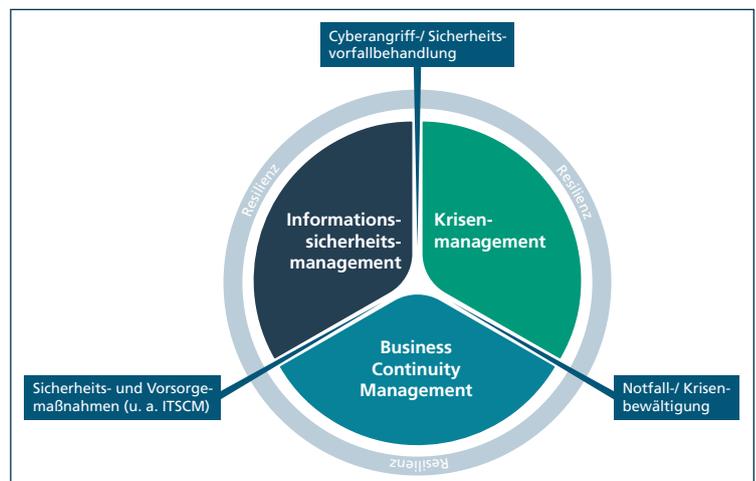


## CyberUp: Handout für Ihren Notfallplan

Jeden Tag gibt es neue Nachrichten über kritische Situationen und insbesondere über IT-Sicherheitsvorfälle. Die Bedrohung durch Ransomware-Angriffe und IT-Ausfälle war noch nie so groß. Die zunehmend digitalen Bedrohungen und komplexer werdenden Risikoszenarien erfordern eine systematische Vorgehensweise bei einer unternehmenskritischen Notfallsituation.

- Eine Vorbereitung auf Notfälle ist sinnvoll; es gibt zwei Möglichkeiten:
  - Einfacher Notfallplan oder
  - aufwändiges Business Continuity Management
- Ein Notfallplan, z.B. zur Informationssicherheit enthält:
  - Vorbeugung,
  - Detektion,
  - Reaktion,
  - Nacharbeit
- Ein Computer Emergency Response Teams (CERT) kann Hilfestellung bei Vorfällen leisten
- Mit dem BSI-Standard 100-4 steht ein Umsetzungsrahmenwerk zum Notfallmanagement zur Verfügung (<https://www.bsi.bund.de/>; Stichwortsuche „100-4“)
- Business Continuity Management
  - Umfangreiche Vorbereitung auf Ausfälle aller Art
  - Management nach Norm
  - Business Impact Analyse – Was schadet dem Unternehmen am meisten?
  - Ziel ist ein umfassendes Notfallkonzept
- Normen und Standards zum BCM
  - Der neue BSI-Standard 200-4 „BCM“ bietet eine praxisnahe Anleitung



Notfallmanagement nach BSI-Vorlage

### Notfallmanagement ist die (Über-)Lebensversicherung

- Für Notfälle gibt es keine „zweite Chance“
- BCM ist Management-Aufgabe
- BCM erfordert weitreichende Vollmachten
- BCM ist kosten- und ressourcenintensiv
- BCM sorgt für einen etablierten Umgang mit Störfällen

Das BSI hält detaillierte Informationen unter [www.bsi.bund.de](http://www.bsi.bund.de) für Sie zu Notfallmanagement und Business Continuity Management bereit.

Handout zum Vortrag „Notfälle vorbereiten – Notfallpläne und BCM“ von Henrik Rüterjans, ATHENE / Fraunhofer SIT im Rahmen der EDITH-Initiative