

Modul 234  
Risiken beim Betrieb  
von IT-Systemen  
bewirtschaften

**1 Identifizieren**  
Gefahren und Bedrohungen  
werden gesucht, gesammelt und erfasst

**2 Analysieren**  
Erfasste Risiken werden  
betreffend Auswirkung (Schadensausmass)  
untersucht und Priorisiert

**3 PLAN DO CHECK**  
Plannen

**4 Einleiten**

**5 Überwachen**  
Regelmässige Überprüfung

- Umfeldrisiken  
- Prozessrisiken  
- Informationsrisiken



Risikomodell (S.26-S.27)

**Risikomanagement  
Prozess (S.25)**

**Risikostrategie**  
Risikovermeidung

**Risikoakzeptanz**  
Nichts "tun" --> akzeptieren

**Risikoübertragung**  
Transfer des Risiko ("Outsourcen")

**Risikoreduzierung**

**Risikoerhöhung**

- Infrastruktur  
- Personal  
- Organisation  
- Hardware & Software  
- Kommunikation

Massnahmenkatalog  
(S55-S67)



Massnahmenplanung/-einleitung



Risikobeeinflussung (S.52-S53)

- 1) Vorbeugen
- 2) Aufdeckung
- 3) Korrektur und
- 4) Wiederherstellung

- Vertraulichkeit ( confidentiality)  
- Integrität ( integrity)  
- Verfügbarkeit ( availability)  
- Verbindlichkeit ( accountability, non-repudiation)  
- Authentizität ( authenticity)  
- Betriebssicherheit ( reliability)



Sicherheitsziele

Beispiel eines Inhalt's:

- Ausgangslage
- Auftrag
- Organisation
- Funktionen
- Normalbetrieb
- Einsatzfunktionen (Pers.Funktionen)
- Diverses
- Ausbildung Unterhalt Notfallkonzept Kosten
- Einsatz
- Auslöser
- Vorgehen
- Eskalation
- Deeskalation
- Abschluss
- Dokumentation



Notfallkonzept  
(Bsp Inhaltsverzeichnis)

**Verletzbarkeit (S.15)**  
- Vertraulichkeit (Daten sollen von unbefugten Zugriff geschützt sein)  
- Integrität (Daten sollen aktuell und korrekt sein)  
- Verfügbarkeit (IT-Systeme sollen wie gefordert zur Verfügung sein)

**Schaden (S.15)**  
- Direkter Schaden (Maschine, Server, Programme, Datenträger, HD usw.)  
- Indirekter Schaden (Kosten für die Rekonstruktion von Daten, Betriebssystem usw.)  
- Folgekosten (Entgangenen Gewinn durch Betriebsunterbruch)

**Risiken**  
- Organisatorische  
- Anwendungsbezogene  
- Infrastrukturelle  
- Bauliche

- Umfeldrisiken  
- Prozessrisiken  
- Informationsrisiken



Risiko

Critical Success Factors (CSF)  
(S.17)

Risikomanagement als klare Priorität erklären

Risikomanagement richtig Positionieren

Risikomanagement systematisch umsetzen

- Ermitteln Schutzbedürftigkeit  
- Bedrohungsanalyse  
- Risikoanalyse  
- Erstellung eines Sicherheitskonzept



BSI Verfahren  
(British Standard Institut  
(Risikoanalyse))

**Vorsätzliche Handlung (VH)**

- Auslöser eine Person  
- Eine Handlung wird bewusst mit einem Ziel  
ausgeführt um Schaden zu verursachen

**Menschlicher Versagen (MV)**

- Auslöser eine Person die berechtigterweise am  
oder mit dem System arbeitet.  
- Passiert in einem Zusammenhang mit solchen Arbeiten zu  
Schäden kommt, wurde oft nachlässig oder unkonzentriert gearbeitet  
- Eine Person die aus Überzeugung, er handle richtig- fehler begeht  
oder die zu einem Schadenfall führen

**Technisches Versagen (TV)**

- Die Ursachen sind für einen Schaden im  
Umfeld eingesetzter Infomatikmittel zu suchen.  
- Hardware, Software, Netzwerk oder Datentechnik

**Höhere Gewalt (HG)**

- Geht immer von der Umwelt unseres  
IT-Systems oder von Elementarereignissen aus  
- Feuer, Hitze, Wasser, Rauch, Sturm, Erdbebewegungen

**Organisatorische Unzulänglichkeit (OU)**

- Die Ursachen des Problems auch hier sind die Mitarbeiter  
- Es besteht doch hier keine Muttwilligkeit oder  
Nachlässigkeit im eigentlichen Sinne vor



Gefahr (Bedrohung)  
(S.11-S.14)



Risikokatalog  
(Themen)

- Bedrohung/Risiko  
- Kategorie  
- Möglicher Schaden  
- Auswirkung auf den Betrieb/Firma  
- Eintretenswahrscheinlichkeit  
- Schadensausmass  
- Resultat eine Zahl

**Risikomatrix**  
(Lehrmittel S. 39)

Bsp: Massnahmen Matrix (S.53)

**Risikokatalog**  
- Nr (Nummerierung)  
- Bedrohung/Risiko (Bezeichnung, Text)  
- Kategorie ( HG, TV usw.)  
- Möglicher Schaden (Bezeichnung, Text)



Darstellungsarten

**Risk Map**  
Excel Tabelle Risikoausmass/Schadenspotenzial  
Eintretenswahrscheinlichkeit (Lehrmittel S.34)

**Risikoniveaus Darstellung (S.31)**

**Sicherheitsmassnahmen  
(S.55-S70)**

- Personelle Massnahmen  
- Organisatorische Massnahmen  
- Technische Massnahmen  
- Bauliche Massnahmen



Risikobewertung

**Risikomessung**

Quantitative Bewertung S.41-S.42

Qualitative Bewertung mittels Faktor (S.41)

**Wichtigkeit:**  
2-Sehr wichtig  
1-Wichtig  
0-Unwichtig  
0-Weiss nicht

**Risiko:**  
3-Hoch  
2-Mittel  
1-Tief  
0-Unbedeutend  
0-Weiss nicht

**Erfüllung:**  
0-Ausgezeichnet  
1-Sehr Gut  
2-Befriedigend  
3-Schlecht  
3-Weiss nicht

**Kontrolle:**  
0-Dokumentiert  
1-Weiss nicht  
2-Nicht sicher / keine

Control Risk Self Assessment  
(CRSA)  
(Lehrmittel S.43-26)

Planung & Organisation  
Beschaffung & Implementieren  
Betrieb & Unterstützung  
Überwachung

Cobit

COSO

Alternative Bewertungsmethoden

ZHA ( Zürich Hazard Analyse)

Balanced Score Card (BSC)