neam IT-Services GmbH

Risikoanalyse zwischen BSI 200-3 und DIN/ ISO 27005

Kai Wittenburg
Geschäftsführer

IT-Sicherheit

IT-Systemhaus

Schulungen

Ihre IT in *sicheren* Händen

Unternehmen

neam IT-Services GmbH

Gründung 1996

Paderborn,
Wiesbaden & Berlin

ca. 90 Mitarbeiter

IT-Systemhaus & IT-Sicherheit
IT-Schulungen & Workshops

neam IT-Services GmbH

Management-Systeme (ISMS)

- ISO 27001
- BSI Grundschutz

Business Continuity

- Notfallvorsorge
- Notfallbehandlung

Penetrationstests

- Infrastruktur
- Web-Anwendungen
- Social-Engineering

Begleitung von Zertifizierungen

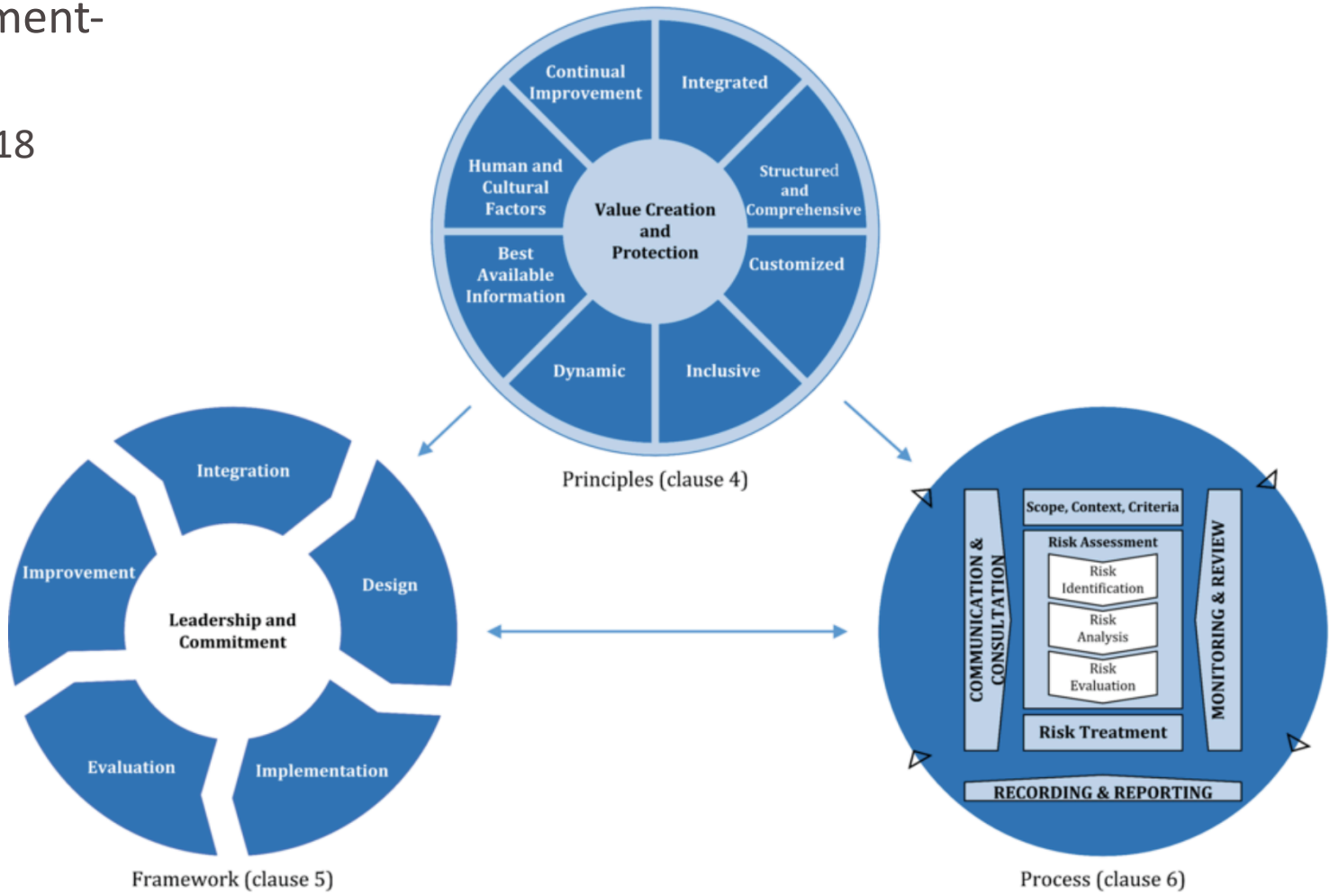
Audits

Security Awareness

Normen zum Risikomanagement

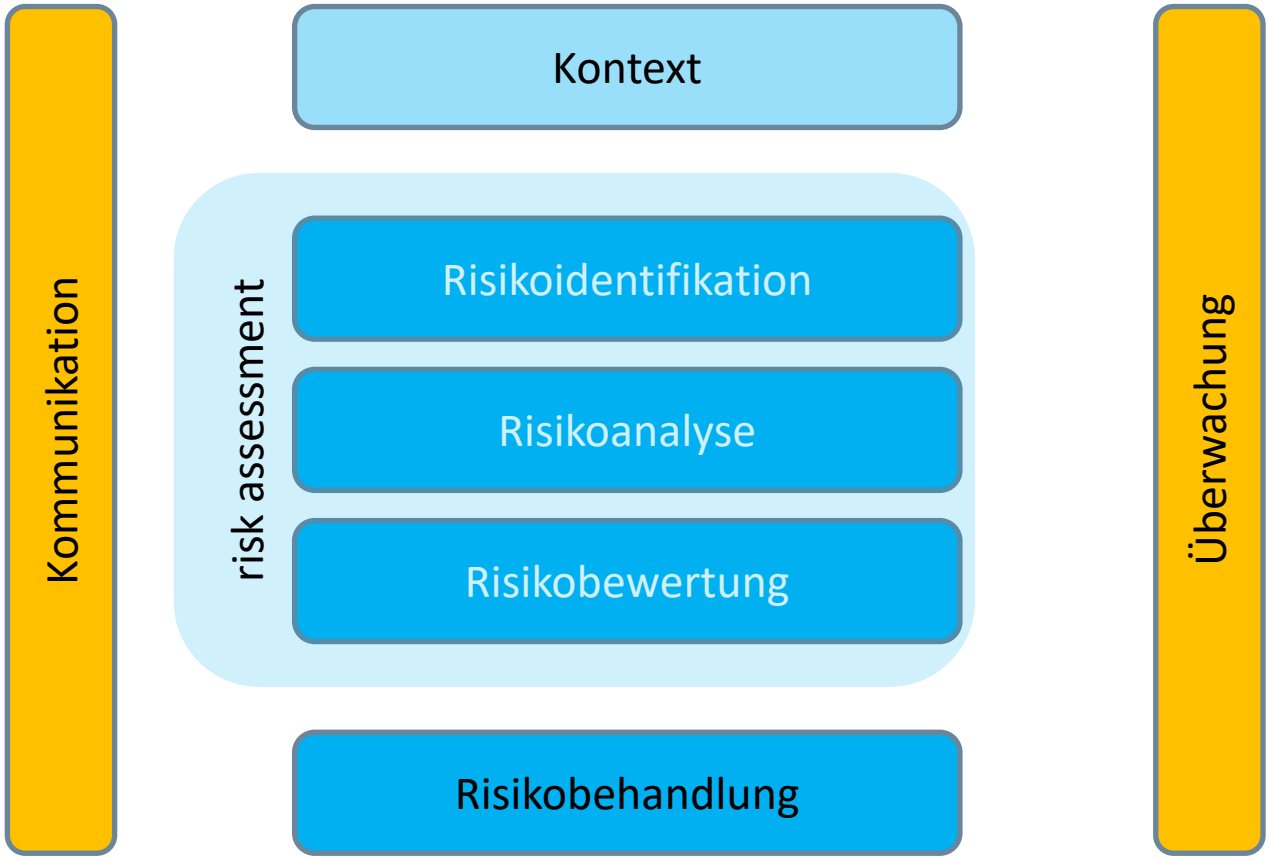
- Risikomanagement-prozess
  - ISO 31000:2018

Figure 1 — Principles, framework and process



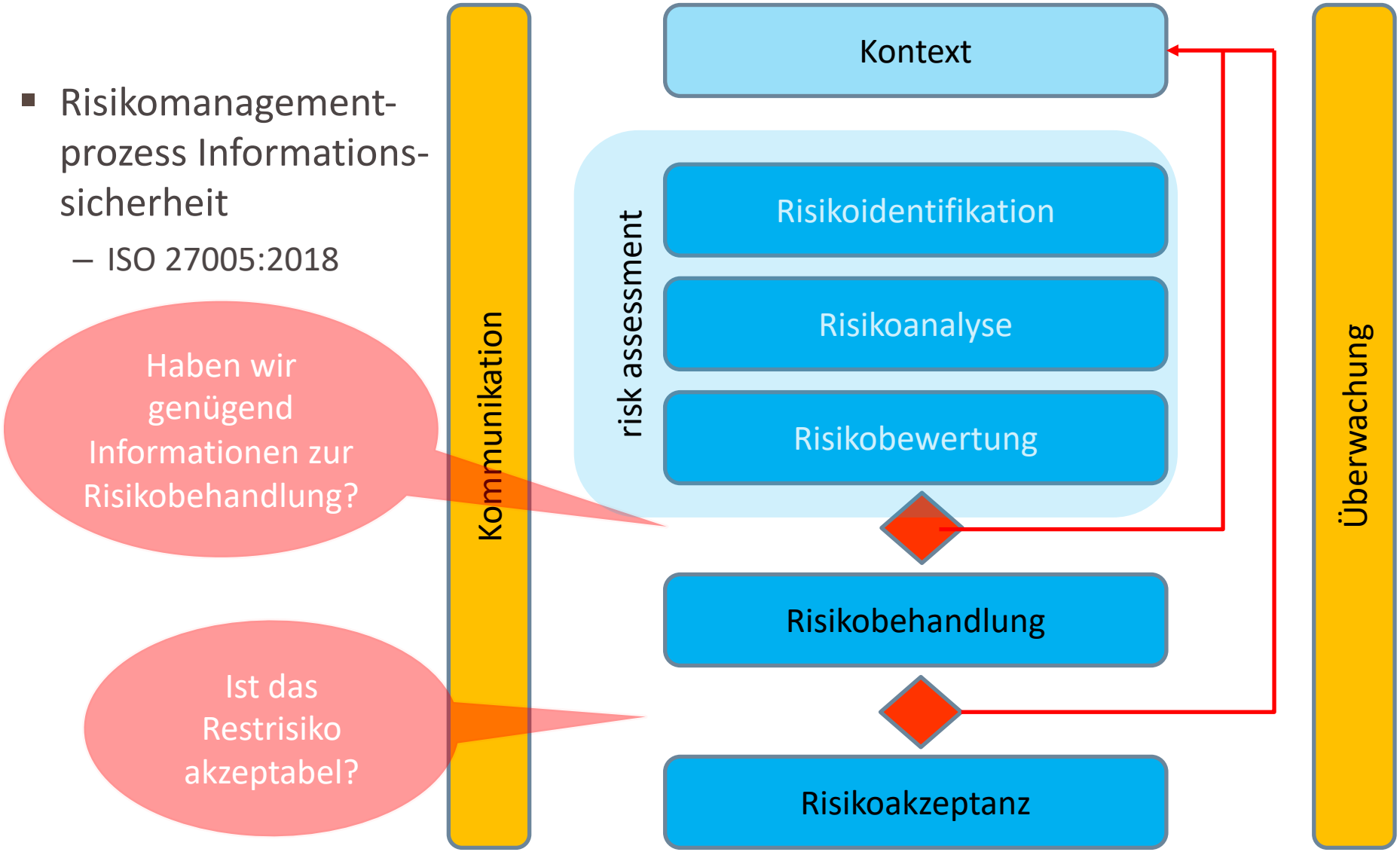
Normen zum Risikomanagement

- Risikomanagement-prozess
  - ISO 31000:2018



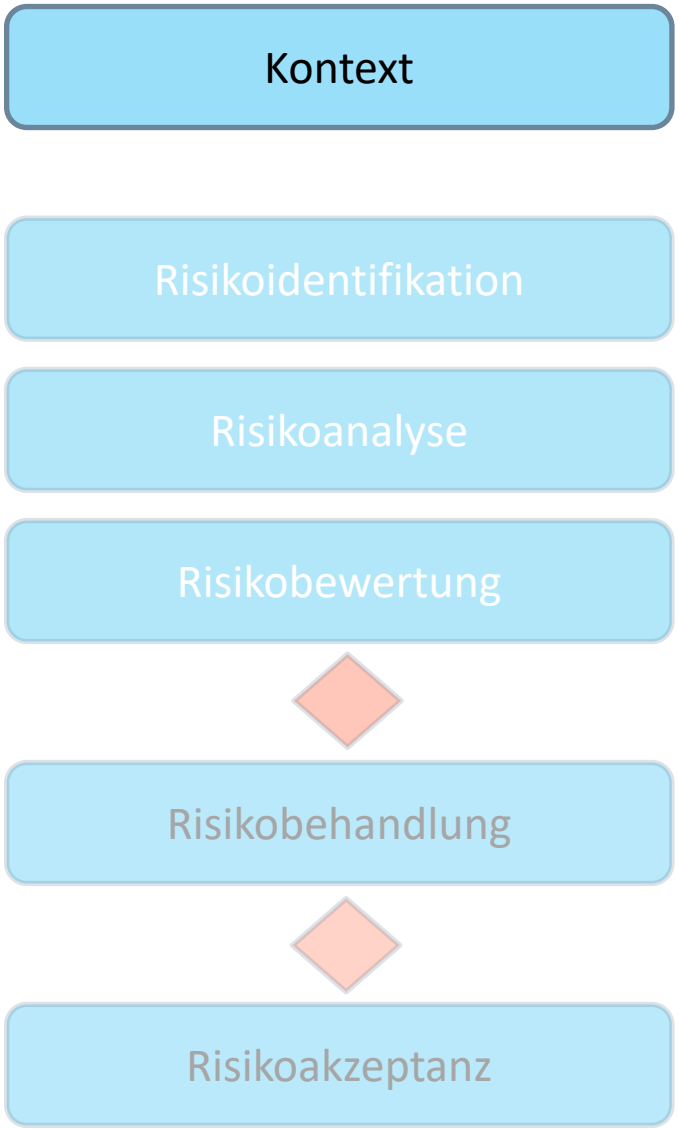
Normen zum Risikomanagement

- Risikomanagement-prozess Informations-sicherheit
  - ISO 27005:2018



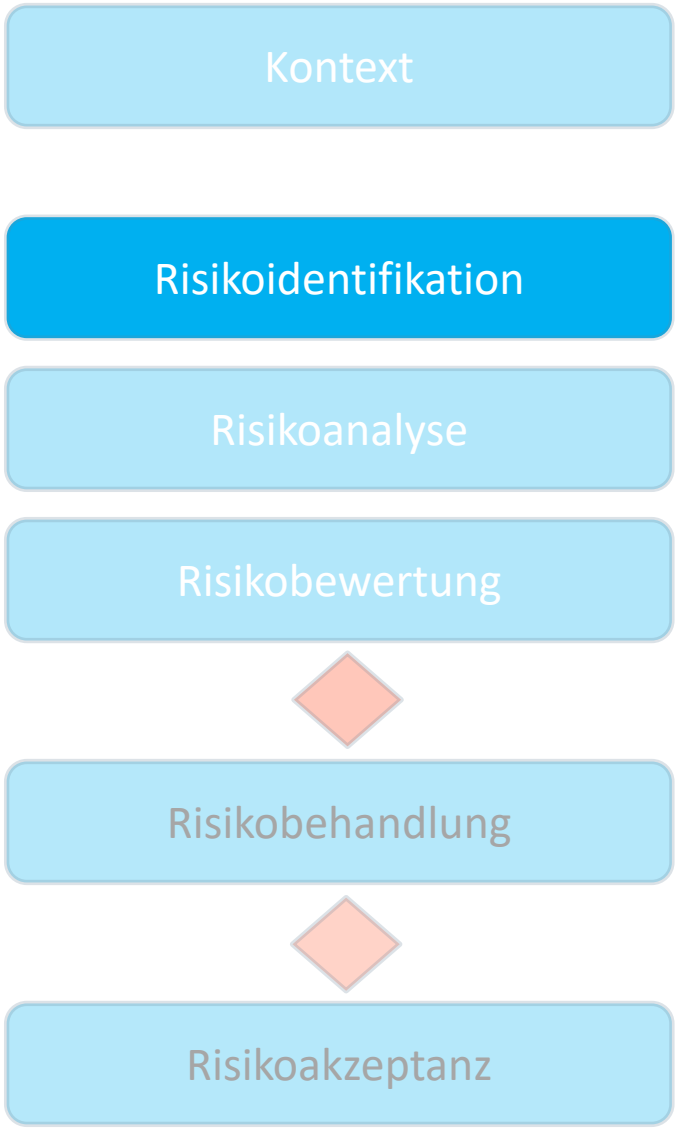
Normen zum Risikomanagement

- Kontext – Annex A
  - Organisation
  - Methode
  - Kriterien
    - Bewertung
    - Auswirkungen
    - Akzeptanz



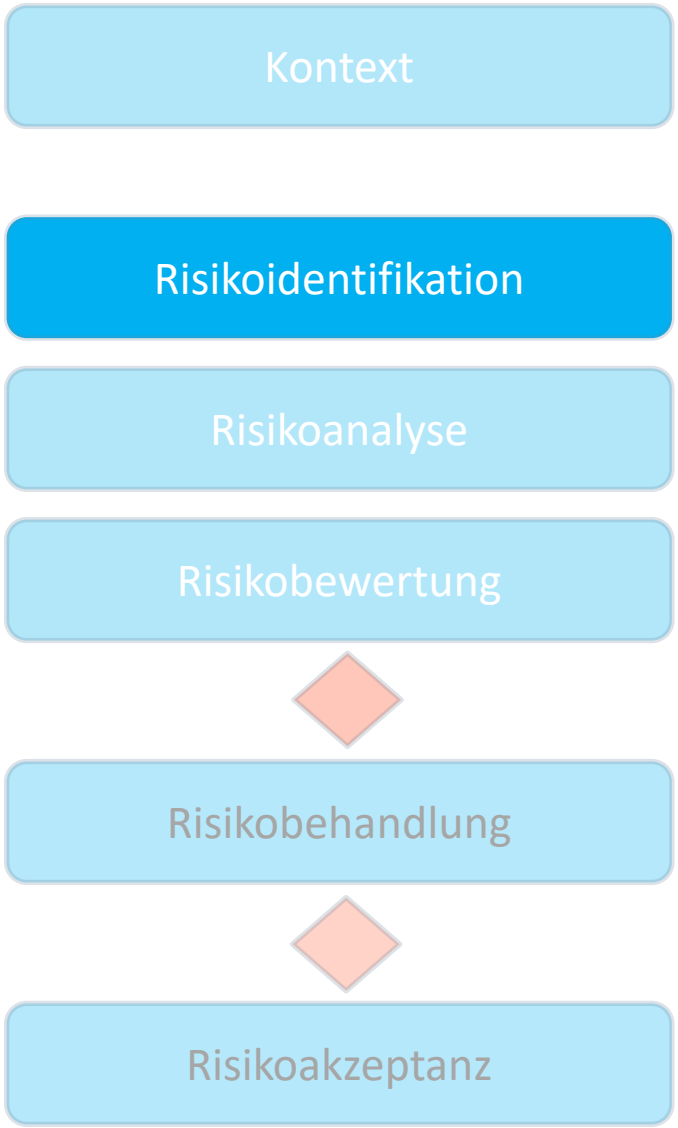
Normen zum Risikomanagement

- Assets – Annex B
  - Eigentümer
  - Primäre Assets
    - Geschäftsprozesse
    - Informationen
  - Unterstützende Assets
    - IT
    - Personal
    - Organisation
  - Schutzbedarf(skategorien)
- Maßnahmen
  - Umgesetzt
  - Geplant
  - Aktueller Status



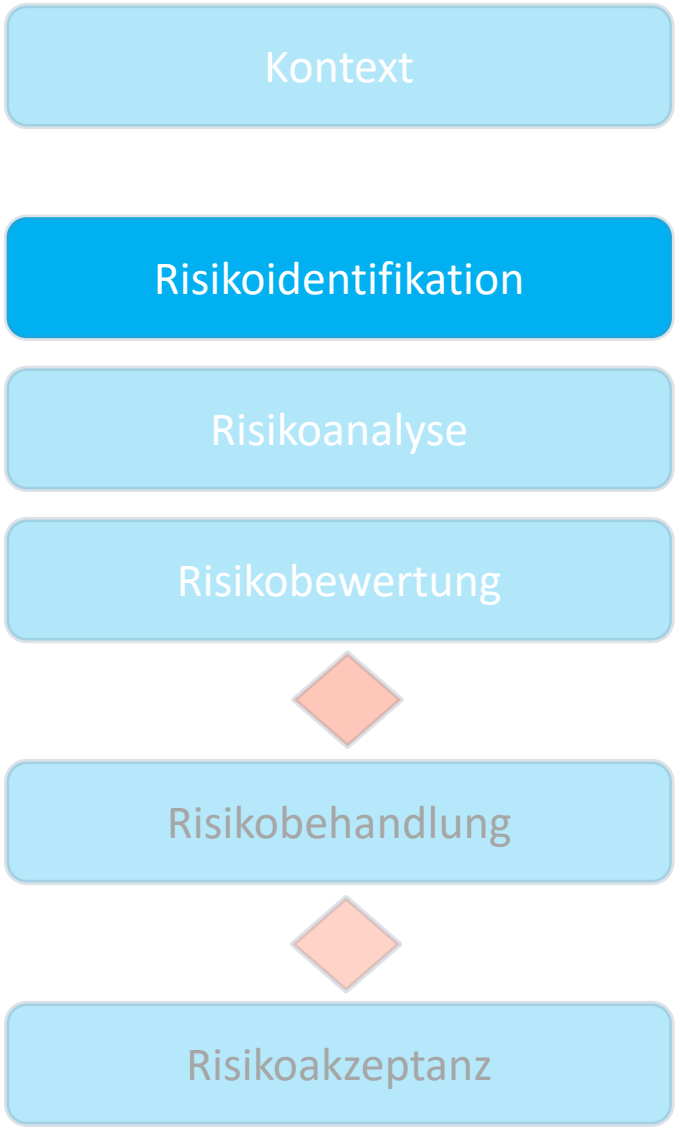
Normen zum Risikomanagement

- Bedrohungen – Annex C
  - Phys. Schaden
    - Feuer
    - Wasser
    - ...
  - Naturereignisse
    - Klima
    - Überflutung
    - ...
  - Technische Defekte
    - Systemausfall
    - Softwarefehler
    - ...
  - ...



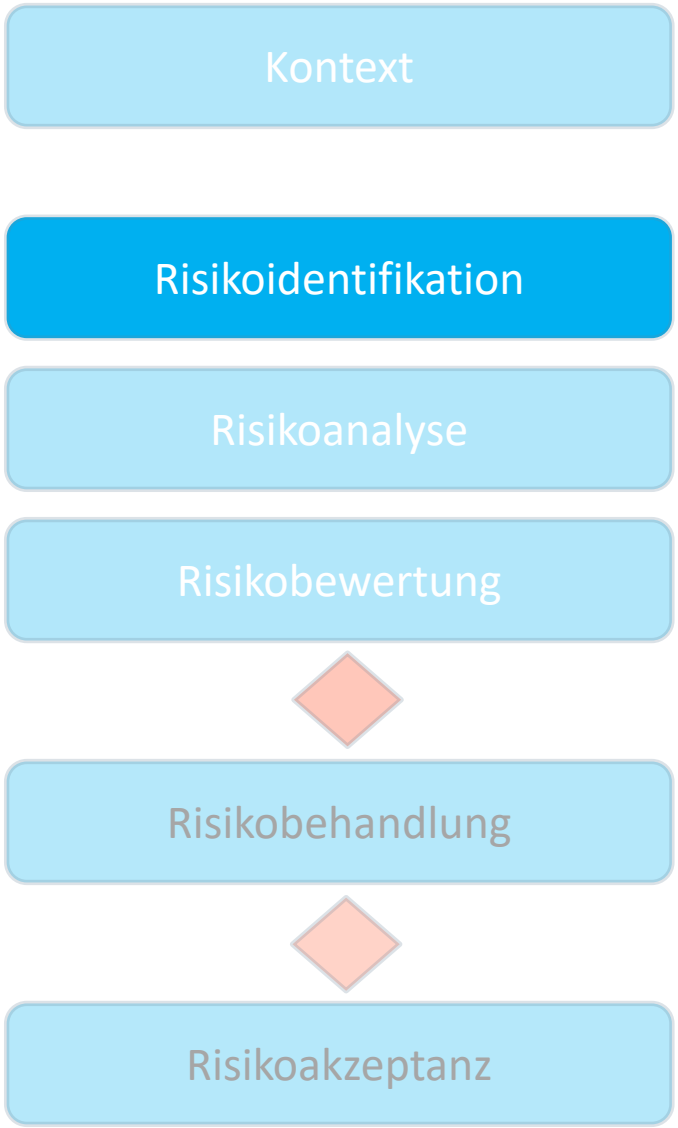
Normen zum Risikomanagement

- Schwachstellen – Annex D
  - Hardware
    - Ungenügende Wartung
    - Anfällig gg. Staub
    - ...
  - Software
    - Kompliziertes User Interface
    - Ungenügende Dokumentation
    - ...
  - Personal
    - Fehlendes Bewusstsein
    - Fehlende Regelungen
    - ...
  - ...



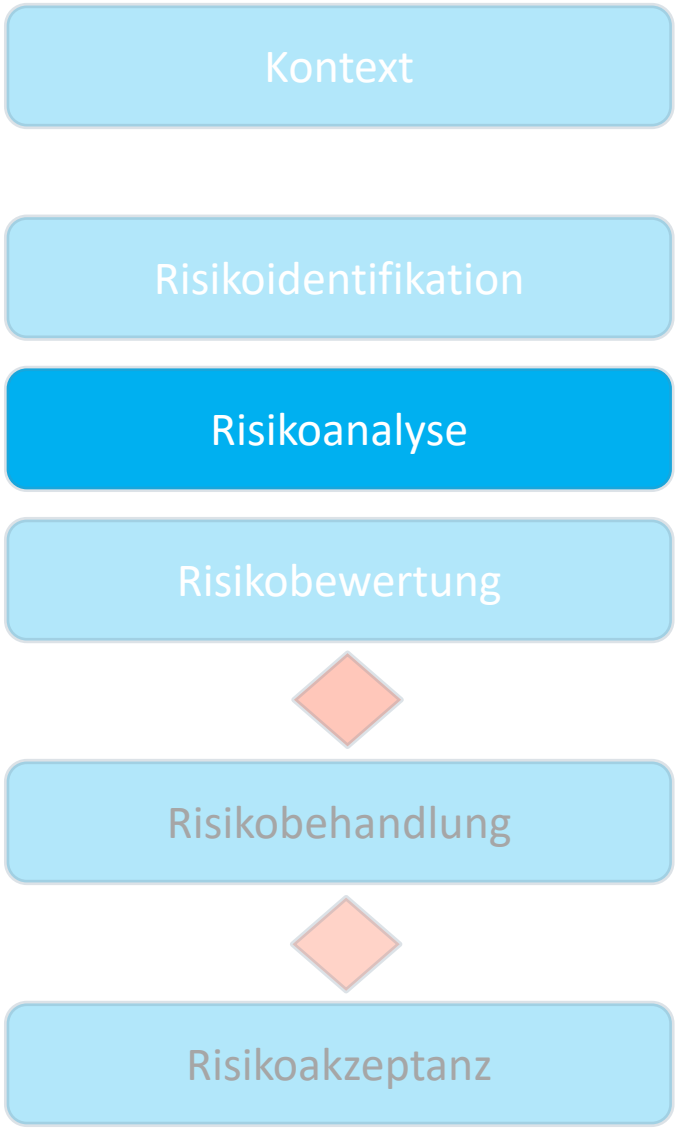
Normen zum Risikomanagement

- Schadensszenarien mit
  - Assets
  - Bedrohungen
  - Schwachstellen



Normen zum Risikomanagement

- Analyse
  - Methode
    - Qualitativ
    - Quantitativ
  - Schadensszenarien
    - Auswirkungen
    - Eintrittswahrscheinlichkeit
  - Risikokennzahl

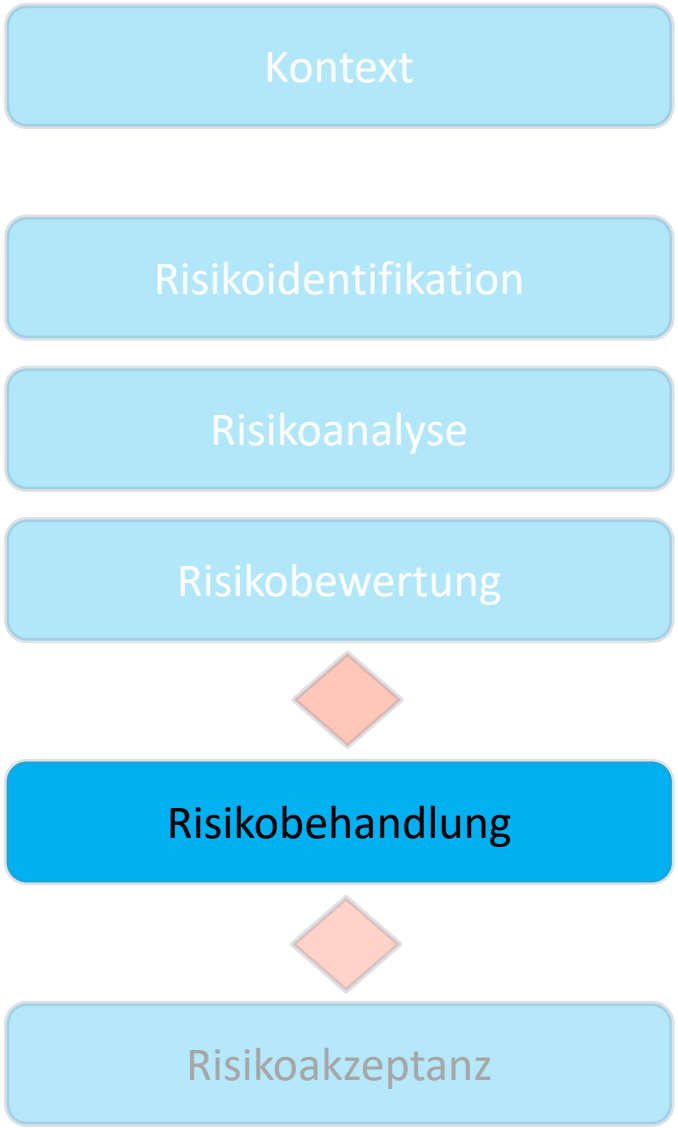


Normen zum Risikomanagement

- Bewertung
  - Risikokennzahlen vs. Bewertungs- & Akzeptanzkriterien
  - Entscheidungsbasis für Risikobehandlung

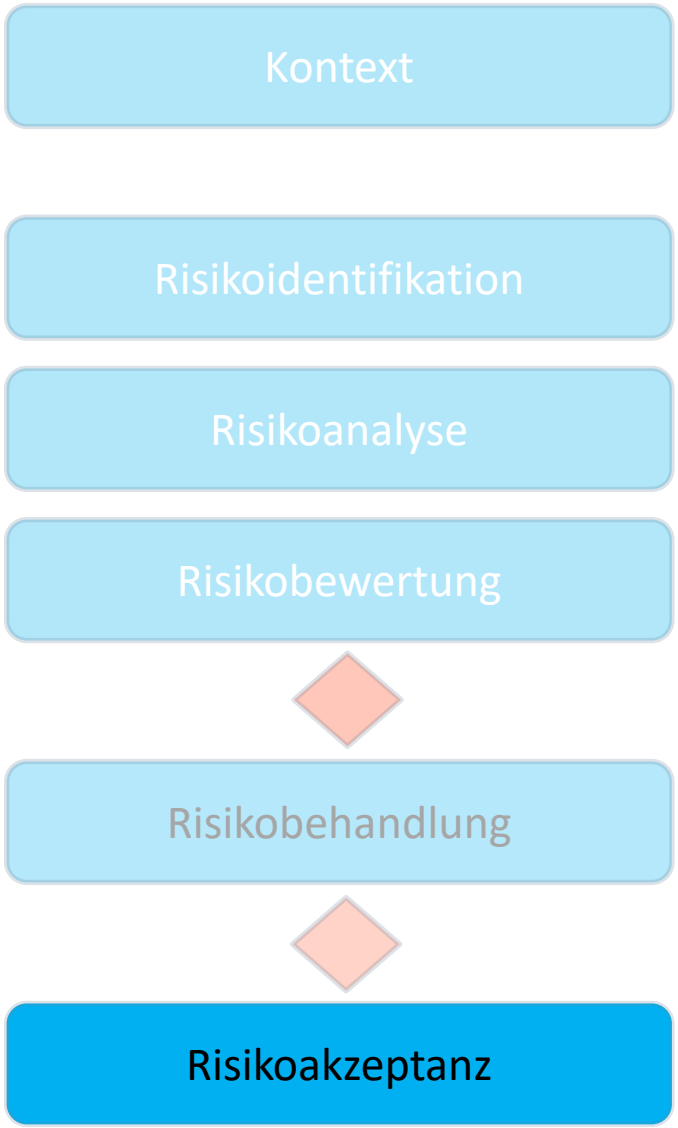
Normen zum Risikomanagement

- Behandlung
  - Vermeidung
  - Reduktion
  - Transfer



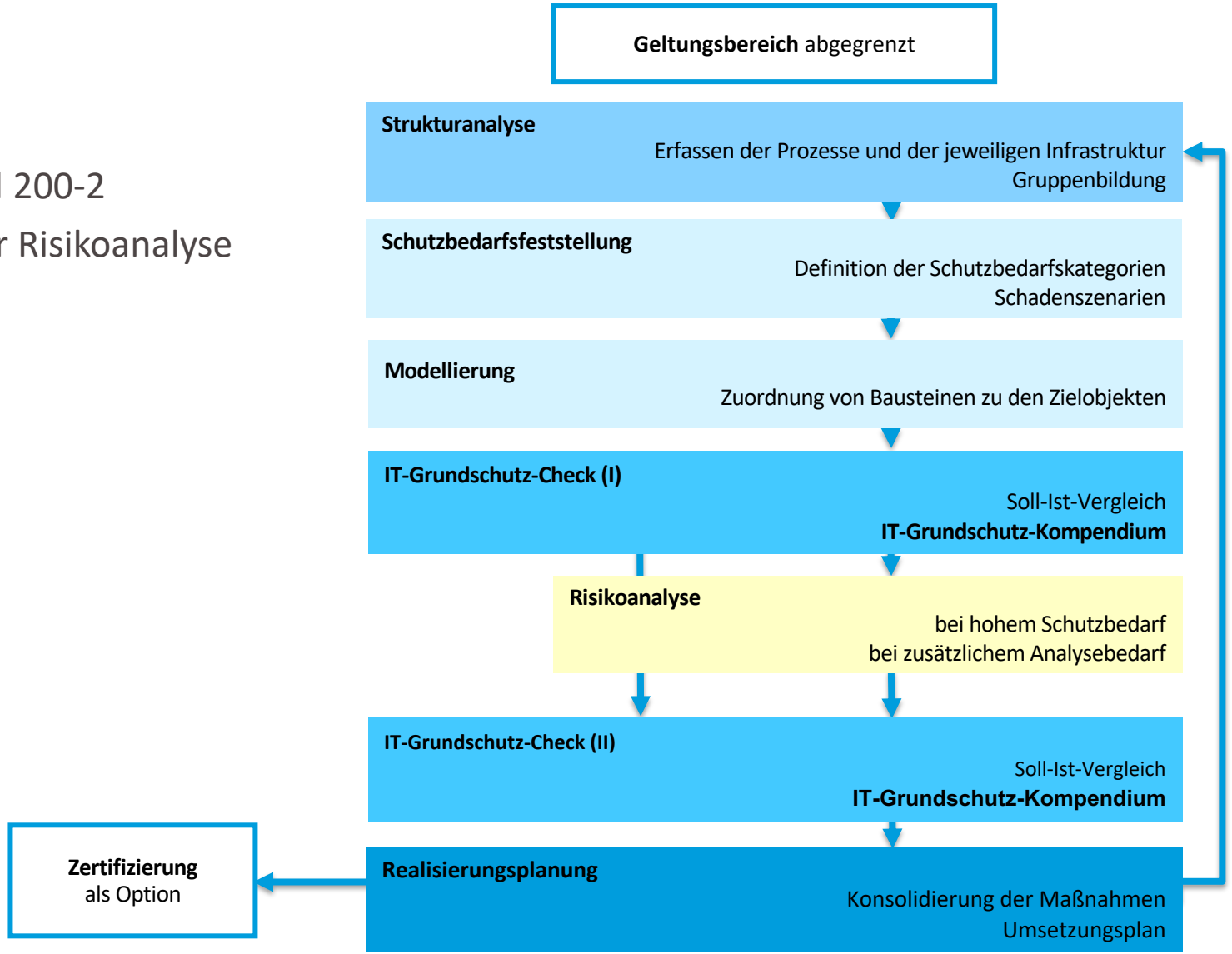
Normen zum Risikomanagement

- Akzeptanz
  - Risikokennzahl vs. Akzeptanzkriterium



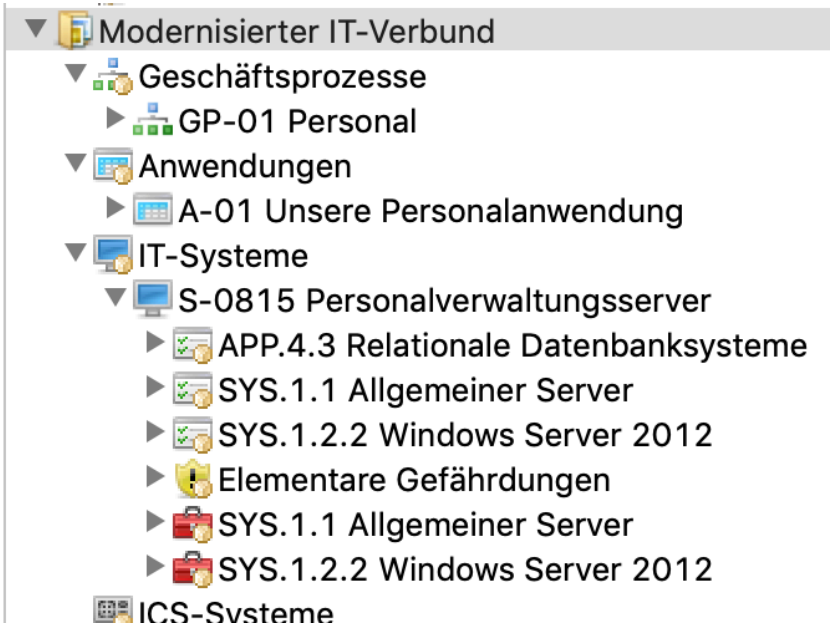
Risikomanagement im BSI IT-Grundschutz

- Vorarbeiten
  - BSI Standard 200-2
  - Richtlinie zur Risikoanalyse



Risikomanagement im BSI IT-Grundschutz

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste
     - Zielobjekte der Strukturanalyse (Gruppen)
     - Priorisierung (gem. Schutzbedarf?)
     - Durchführung auf Ebene der Geschäftsprozesse???
  2. Erstellung einer Gefährdungsübersicht
  3. Gefährdungsbewertung
  4. Risikobehandlungsplan

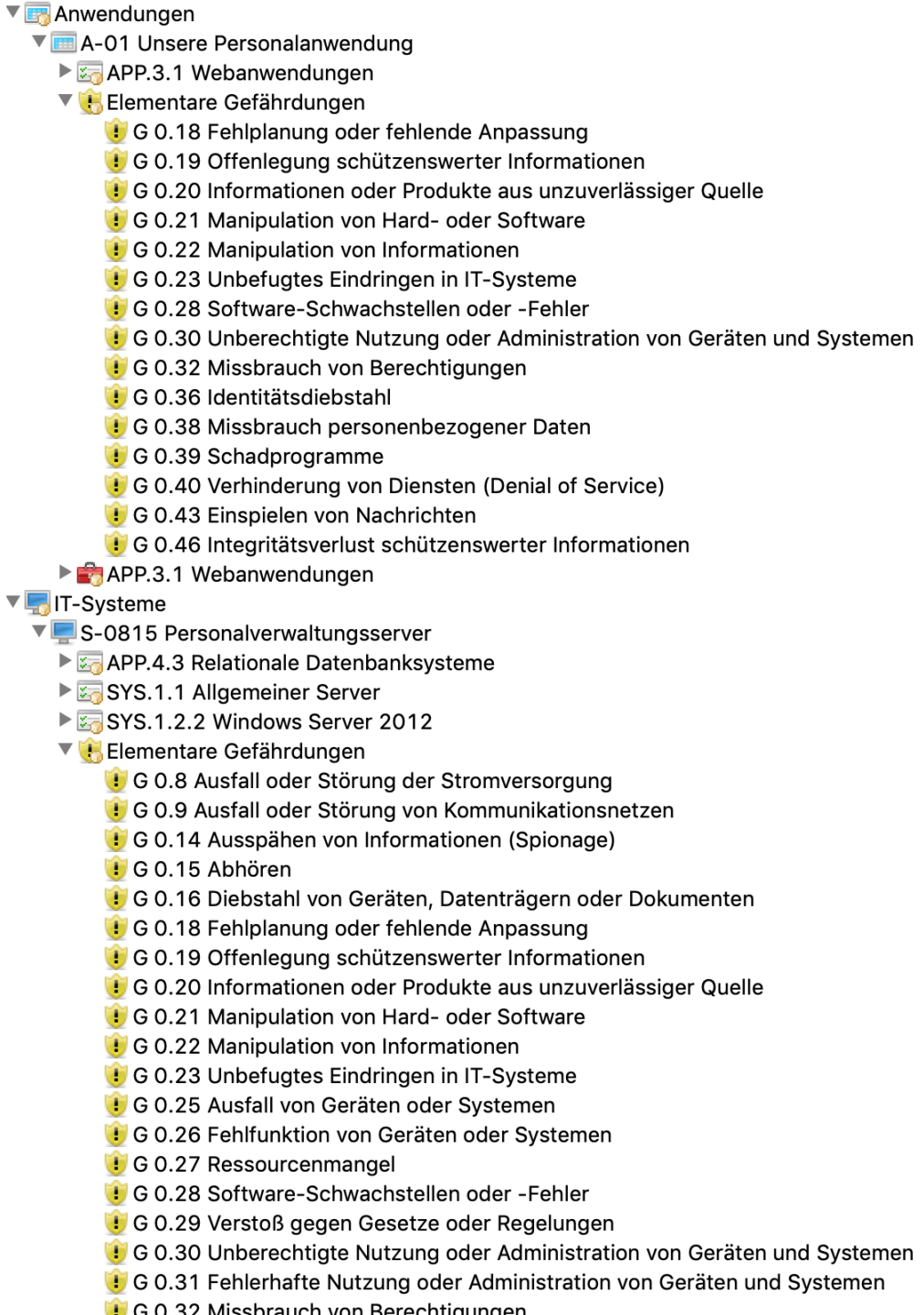


Risikomanagement im BSI IT-Grundschutz

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste
  2. Erstellung einer Gefährdungsübersicht
     - BSI G.0 mit 47 elementare Gefährdungen
     - IT-Grundschutz-Kompendium (IT-GS-integriert)
     - Kompatibel zu internationalen Katalogen und Standards
     - Grundwert (CIA)
     - Zusätzliche/ spezifische Gefährdungen?
     - Relevanz für das Zielobjekt (direkt, indirekt oder nicht relevant)?
  3. Gefährdungsbewertung
  4. Risikobehandlungsplan

Risikomanagement

- Basis: Zielobjekte
  - Detailliert
  - Aufwand!



Risikomanagement

- Basis: Geschäftsprozess
  - Konform BSI 200-3
  - Zertifizierungsfähig?
    - Ja.
    - Ergänzt um Asset-spezifische Betrachtung (risiko-orientiert)

Risikomanagement im BSI IT-Grundschutz

- Prozesse mit (sehr) hohem Schutzbedarf
  1. Assetliste
  2. Erstellung einer Gefährdungsübersicht
  3. Gefährdungsbewertung
     - Eintrittswahrscheinlichkeit
     - Auswirkung
  4. Risikobehandlungsplan

Risikomanagement im BSI IT-Grundschutz

- Gefährdungsbewertung – Bewertungskriterien
  - Eintrittswahrscheinlichkeit

sehr selten	sehr unwahrscheinlich, ist noch nie vorgekommen
selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

- +

Risikomanagement im BSI IT-Grundschutz

- Gefährdungsbewertung – Bewertungskriterien
  - Auswirkung

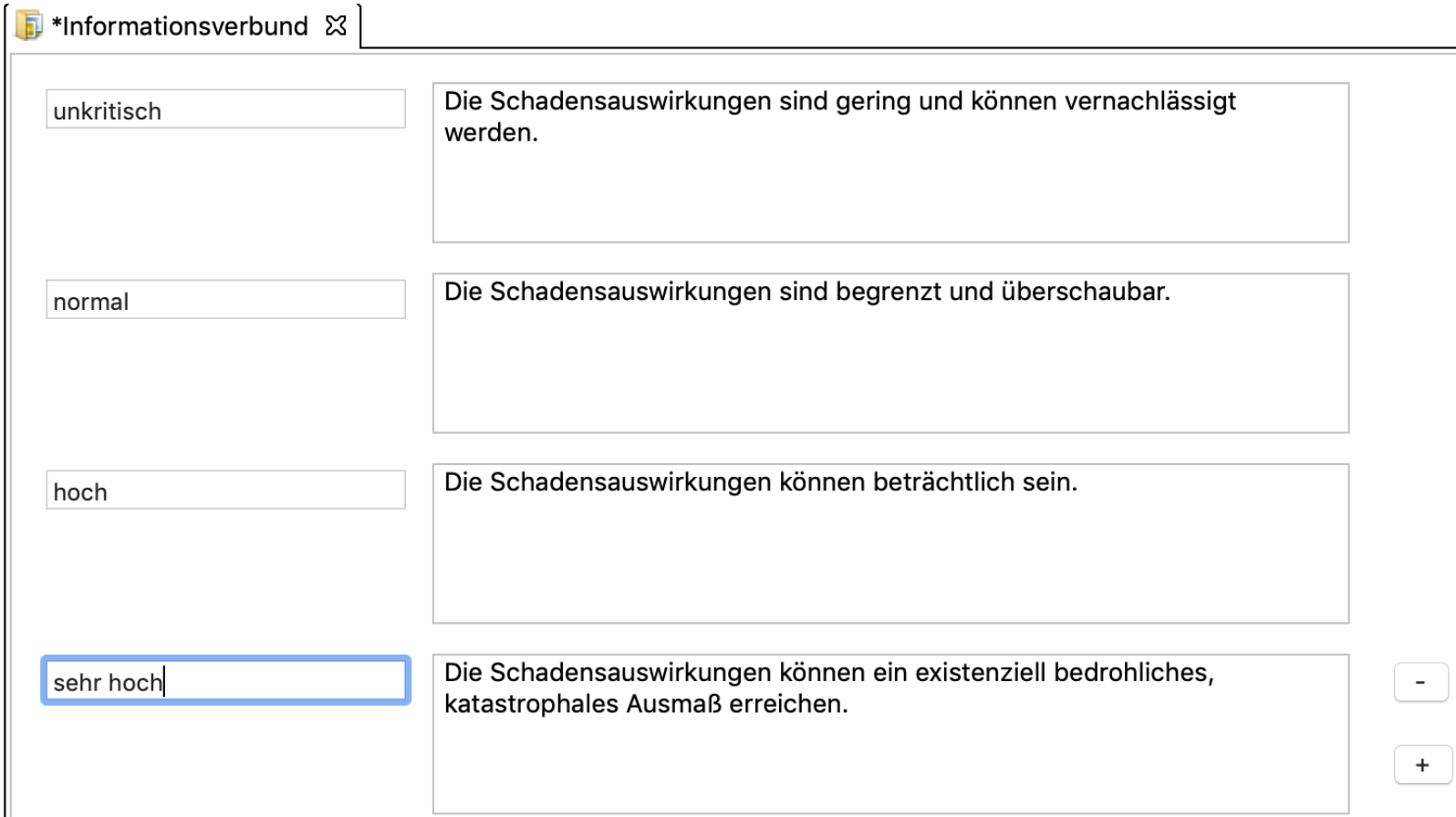
Schutzbedarf für Vertraulichkeit	Wert
normal	1
hoch	2
sehr hoch	3

Schutzbedarf für Integrität	Wert
normal	1
hoch	2
sehr hoch	3

Schutzbedarf für Verfügbarkeit	Wert
normal	1
hoch	2
sehr hoch	3

Risikomanagement im BSI IT-Grundschutz

- Gefährdungsbewertung – Bewertungskriterien
  - Auswirkung in verinice

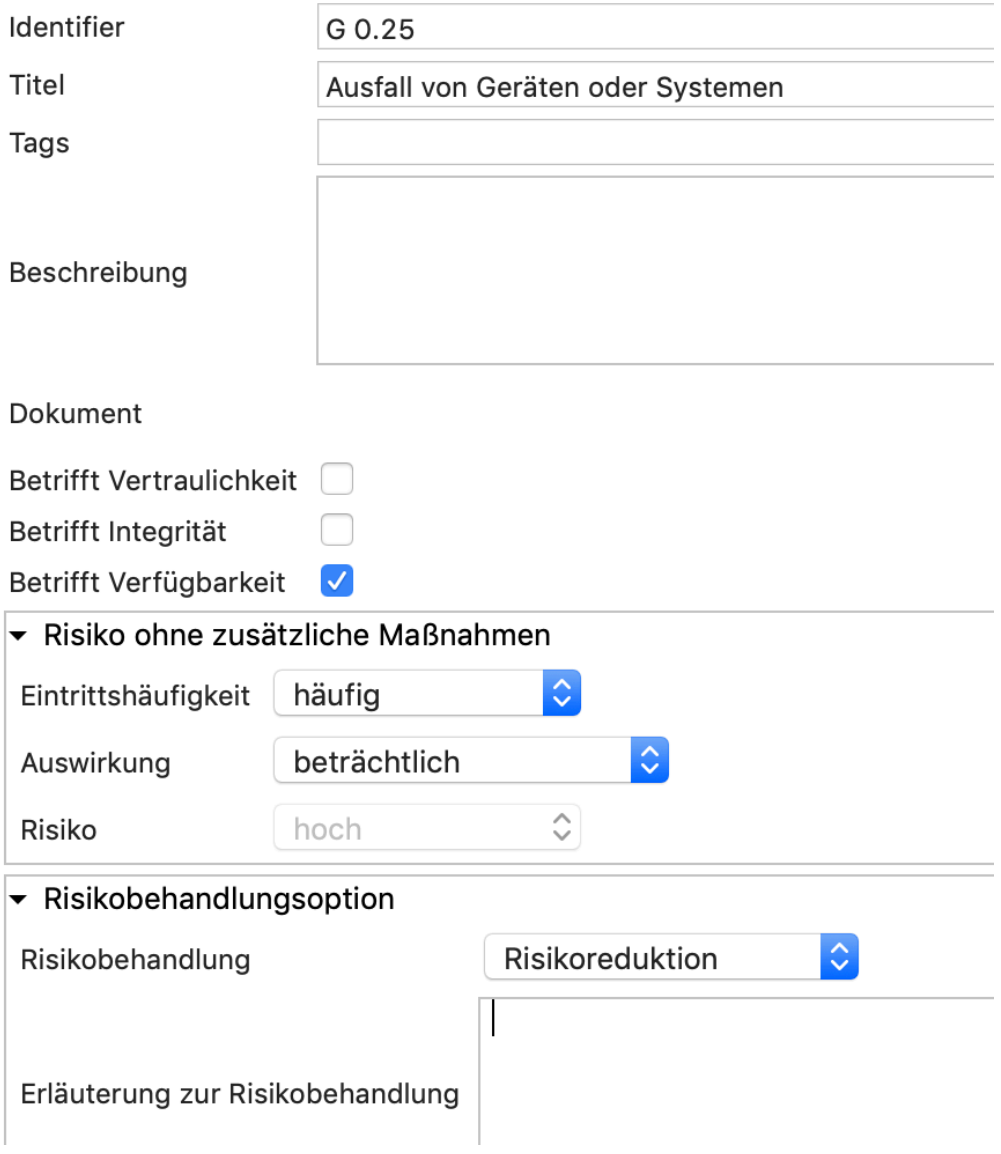


Risikomanagement im BSI IT-Grundschutz

- Risikoakzeptanz
  - Abbildung im verinice

Risikomanagement im BSI IT-Grundschutz

- Gefährdungsbewertung
  - Abbildung im verinice



Risikomanagement & Datenschutz

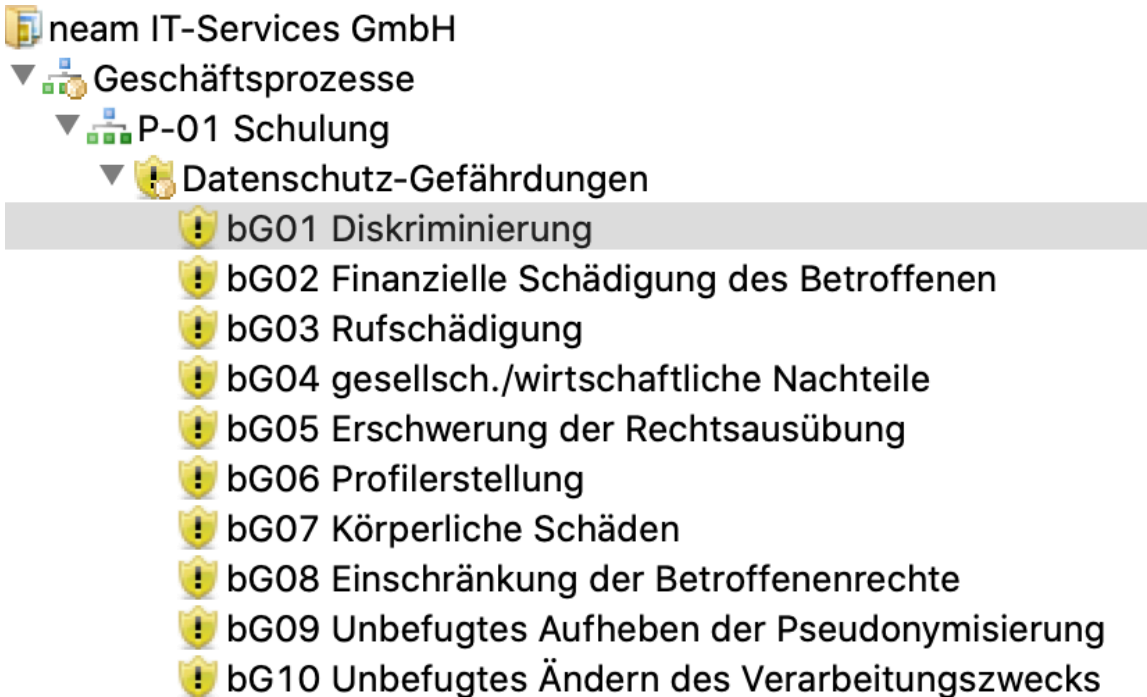
- Informationssicherheit
  - Sicht der Organisation
  - ISO 27005, BSI Standard 200-3
- Datenschutz
  - Sicht der Betroffenen
  - DSGVO Art 32 (TOMs), 35 (DSFA)
  - Standarddatenschutzmodell (SDM)

Risikomanagement Datenschutz
DSGVO – Art. 32

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke **der Verarbeitung** sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des ***Risikos*** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem ***Risiko*** angemessenes Schutzniveau zu gewährleisten

Risikomanagement Datenschutz

- Verarbeitungsverzeichnis
  - Assetliste
- Gefährdungen
  - Betroffene!
- Maßnahmen
  - IT-Grundschutz-Kompendium
  - CNIL
  - ISO 29151
- Bestandteil einer DSFA



Schwachstelle: Organisatorische Mängel

Bedrohung: Unbefugter Zugriff

Dokument

Betrifft Vertraulichkeit ☑

Betrifft Integrität ☑

Betrifft Verfügbarkeit ☐

Risiko ohne Maßnahmen

Eintrittshäufigkeit: mittel

Auswirkung: existenzbedrohend

Risiko: hoch

Risiko ohne zusätzliche Maßnahmen

P-04 Schulung		Vertraulichkeit: **Hoch**		Integrität: **Hoch**		Verfügbarkeit: **Normal**
bG01	Diskriminierung	Betrifft Vertraulichkeit:	**Ja**	Betrifft Integrität:	**Ja**	Betrifft Verfügbarkeit: **Nein**
	Risiko ohne Maßnahmen:	Eintrittshäufigkeit: **mittel**		Auswirkungen: **existenzbedrohend**		Risikokategorie: **hoch**
	Risiko ohne ergänzende Maßnahmen:	Eintrittshäufigkeit: **selten**		Auswirkung: **beträchtlich**		Risikokategorie: **mittel**
	Risikobehandlungsoption:	Risikoreduktion	Erläuterungen:			
	Risiko mit ergänzenden Maßnahmen:	Eintrittshäufigkeit: **selten**		Auswirkung: **vernachlässigbar**		Risikokategorie: **gering**

Risiko mit zusätzlichen Maßnahmen

Eintrittshäufigkeit: selten

Auswirkung: vernachlässigbar

Risiko: gering

Risikomanagement Datenschutz
DSGVO – Art. 32

Unter Berücksichtigung des **Stands der Technik**, der **Implementierungskosten** und der **Art**, des **Umfangs**, der **Umstände** und der **Zwecke** **der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere** des **Risikos** für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten

neam IT-Services GmbH
Technologiepark 8
D-33100 Paderborn

+49 5251 1652-0
+49 5251 1652-444

http://www.neam.de