

Risikoanalyse zwischen BSI 200-3 und DIN/ ISO 27005

Kai Wittenburg

Geschäftsführer



IT-Sicherheit



IT-Systemhaus



Schulungen

Ihre IT in
sicheren Händen

Unternehmen



Gründung 1996

Paderborn,
Wiesbaden & Berlin

ca. 90 Mitarbeiter

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



Management-Systeme (ISMS)

- ISO 27001
- BSI Grundschutz

Business Continuity

- Notfallvorsorge
- Notfallbehandlung

Penetrationstests

- Infrastruktur
- Web-Anwendungen
- Social-Engineering

Begleitung von
Zertifizierungen

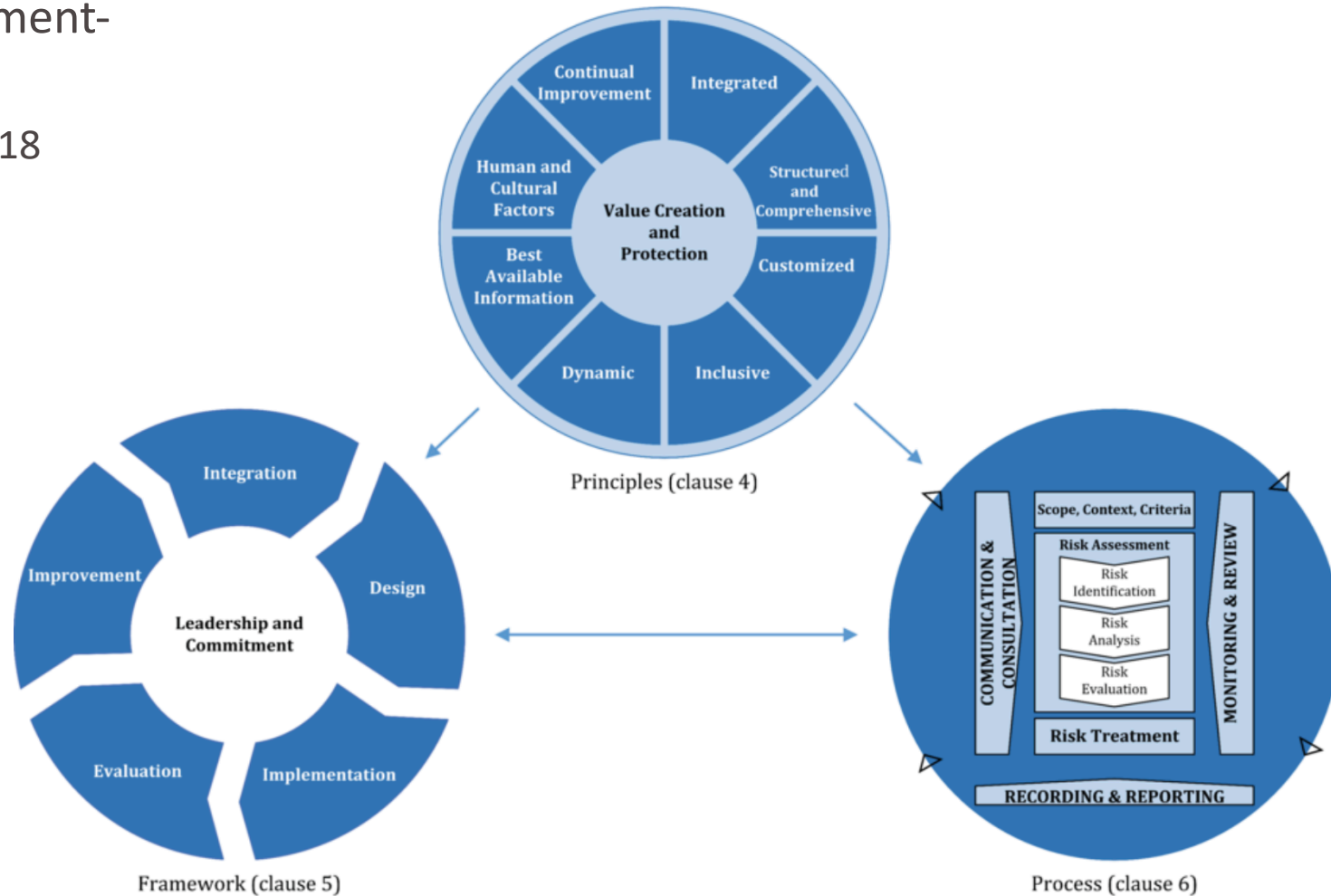
Audits

Security
Awareness

Normen zum Risikomanagement

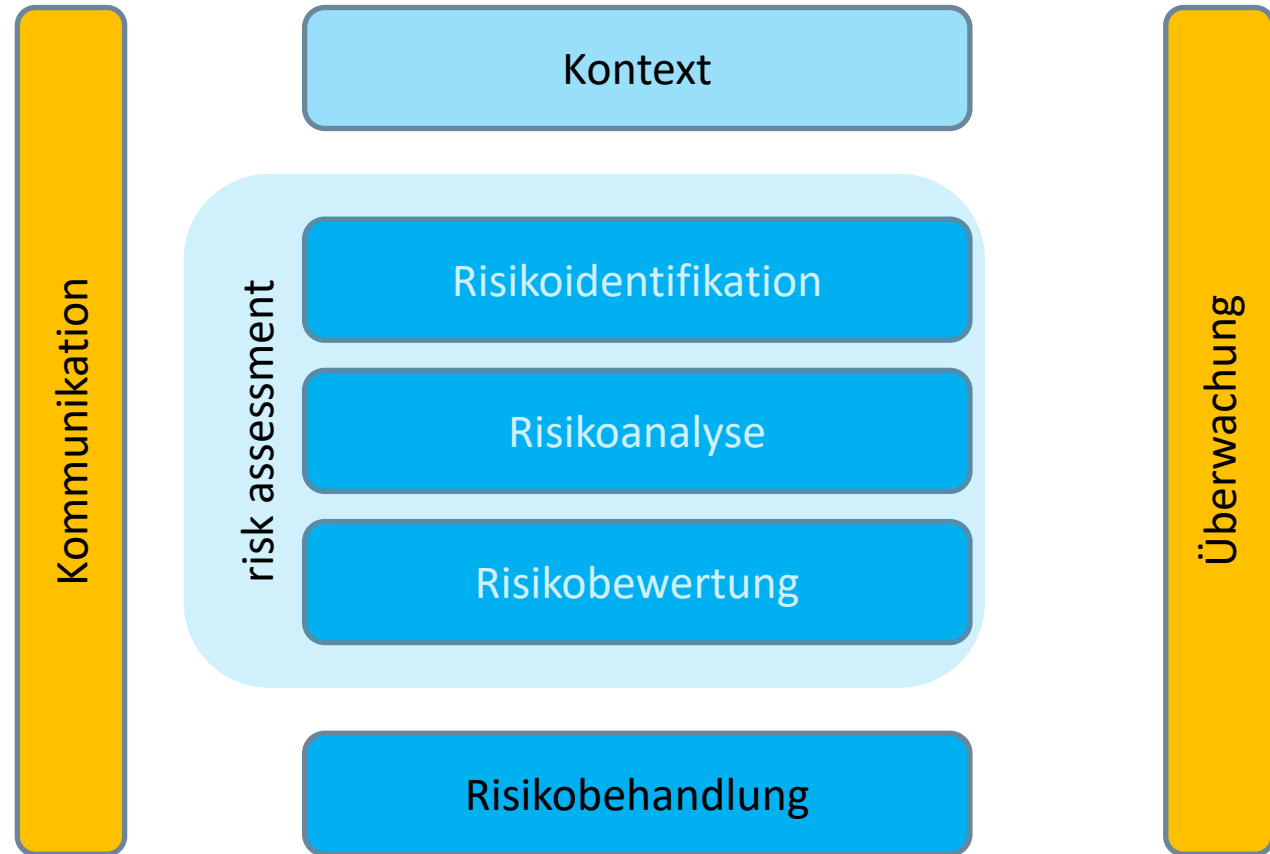
- Risikomanagementprozess
– ISO 31000:2018

Figure 1 – Principles, framework and process



Normen zum Risikomanagement

- Risikomanagementprozess
– ISO 31000:2018

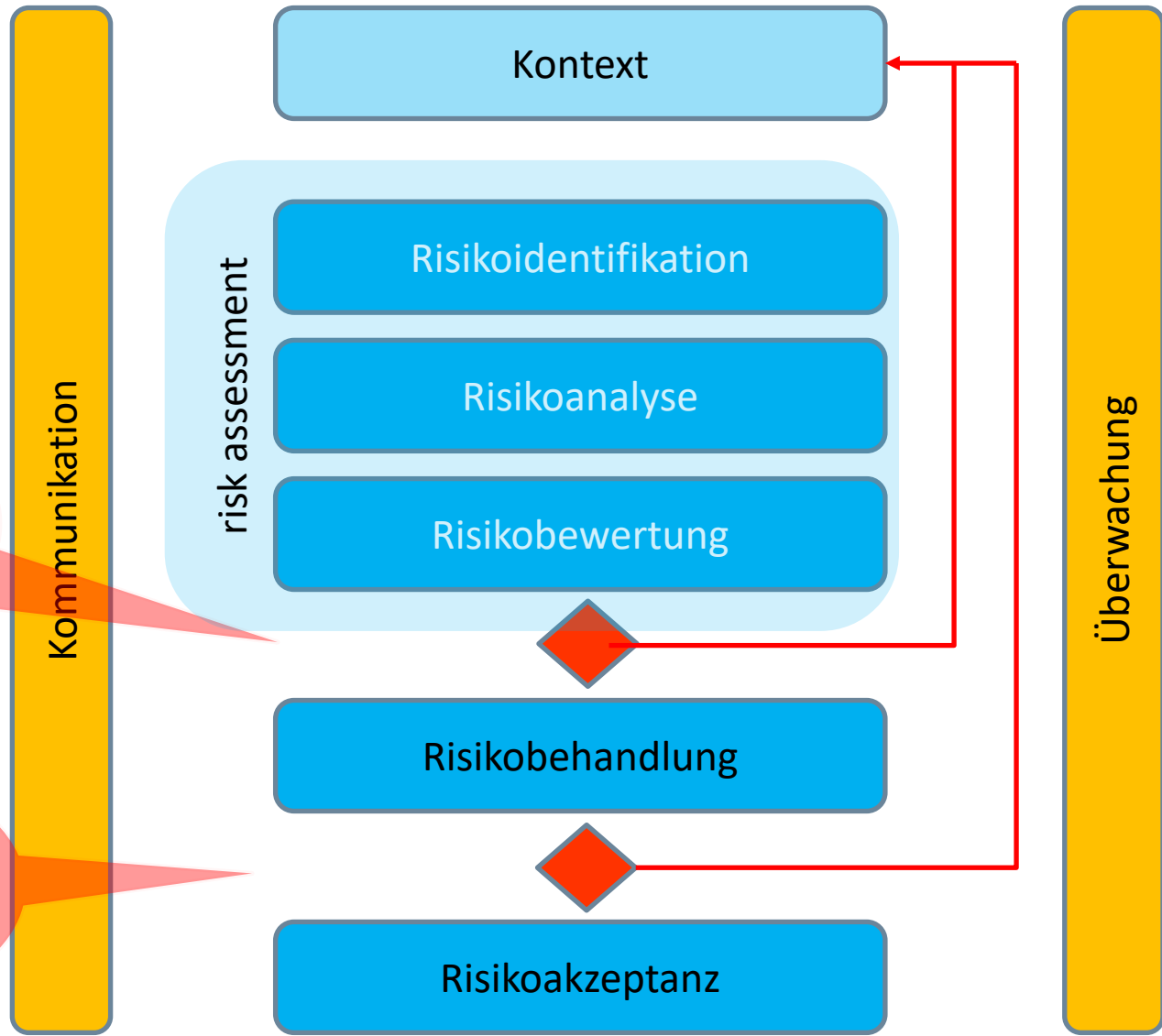


Normen zum Risikomanagement

- Risikomanagementprozess Informationssicherheit
 - ISO 27005:2018

Haben wir genügend Informationen zur Risikobehandlung?

Ist das Restrisiko akzeptabel?



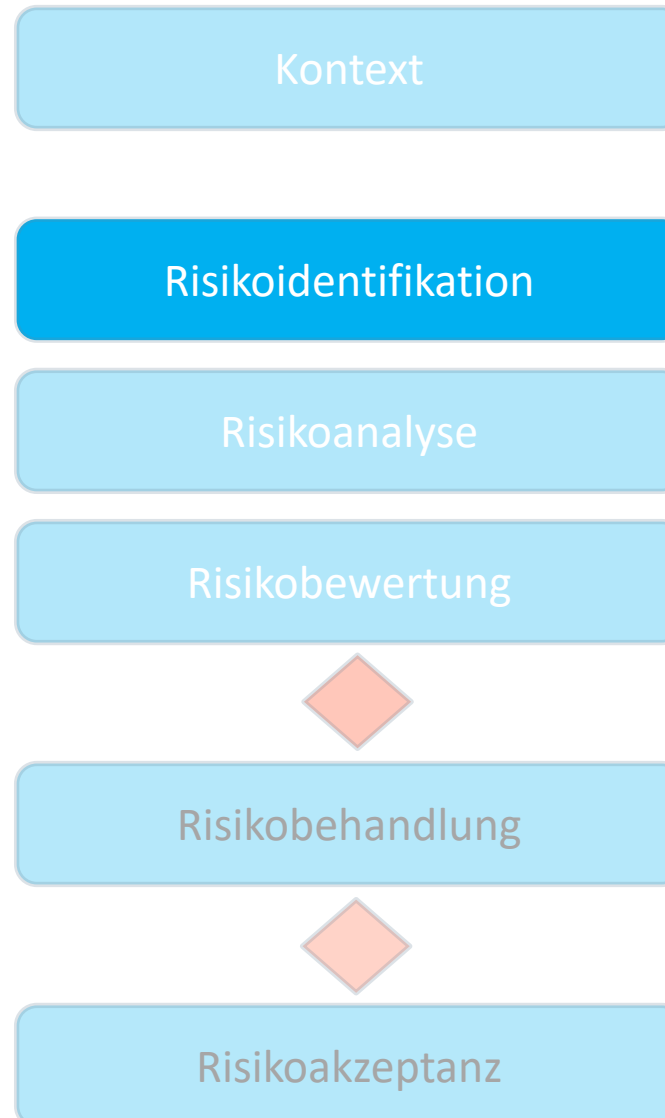
Normen zum Risikomanagement

- 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



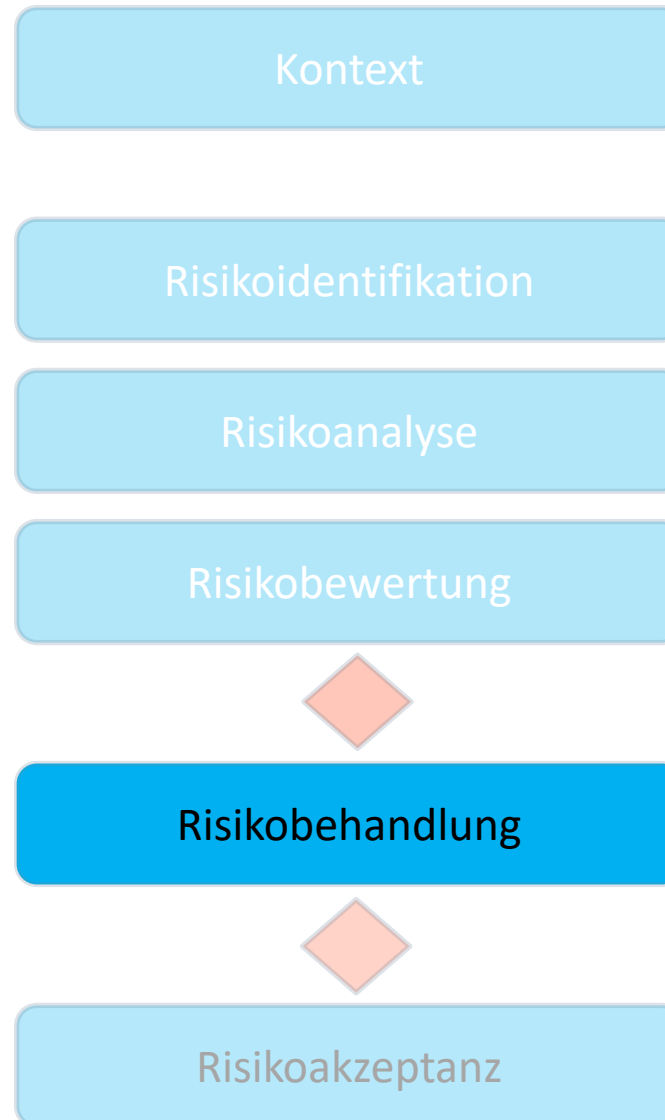
Normen zum Risikomanagement

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



Normen zum Risikomanagement

- Behandlung
 - Vermeidung
 - Reduktion
 - Transfer



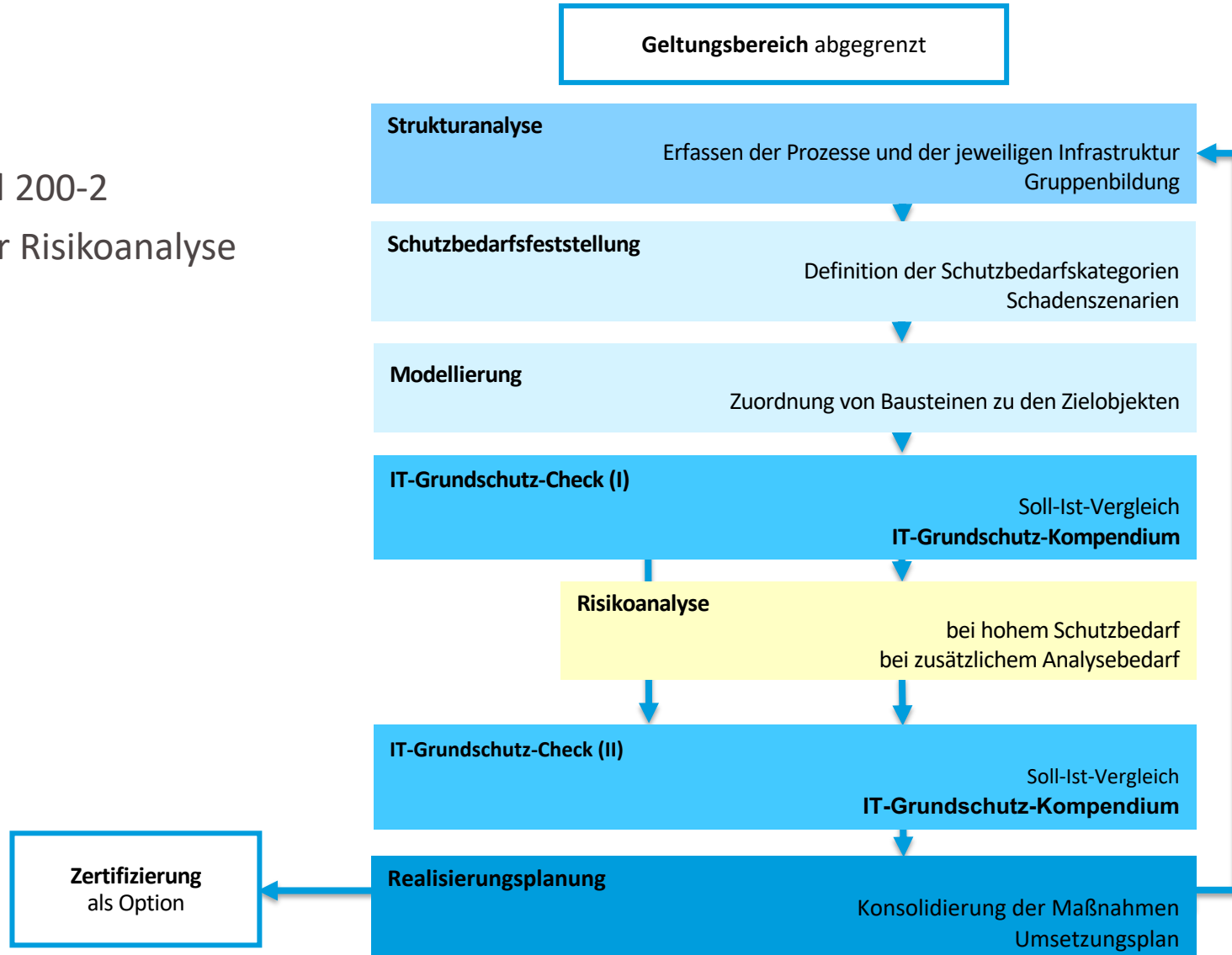
Normen zum Risikomanagement

- Akzeptanz
 - Risikokennzahl vs. Akzeptanzkriterium



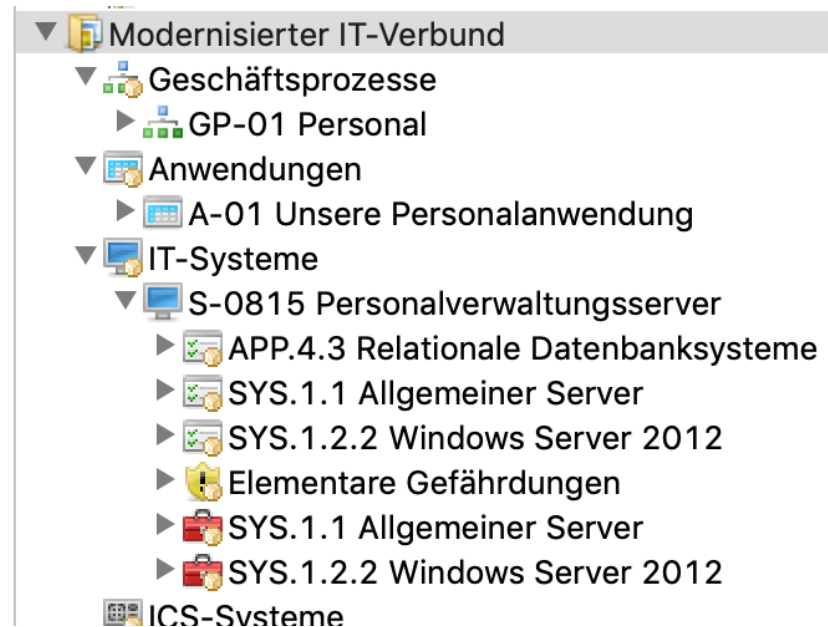
Risikomanagement im BSI IT-Grundschutz

- 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














- 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!

- ▼  Anwendungen
 - ▼  A-01 Unsere Personalanwendung
 - ▶  APP.3.1 Webanwendungen
 - ▼  Elementare Gefährdungen
 - ⚠ G 0.18 Fehlplanung oder fehlende Anpassung
 - ⚠ G 0.19 Offenlegung schützenswerter Informationen
 - ⚠ G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
 - ⚠ G 0.21 Manipulation von Hard- oder Software
 - ⚠ G 0.22 Manipulation von Informationen
 - ⚠ G 0.23 Unbefugtes Eindringen in IT-Systeme
 - ⚠ G 0.28 Software-Schwachstellen oder -Fehler
 - ⚠ G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
 - ⚠ G 0.32 Missbrauch von Berechtigungen
 - ⚠ G 0.36 Identitätsdiebstahl
 - ⚠ G 0.38 Missbrauch personenbezogener Daten
 - ⚠ G 0.39 Schadprogramme
 - ⚠ G 0.40 Verhinderung von Diensten (Denial of Service)
 - ⚠ G 0.43 Einspielen von Nachrichten
 - ⚠ G 0.46 Integritätsverlust schützenswerter Informationen
 - ▶  APP.3.1 Webanwendungen
 - ▼  IT-Systeme
 - ▼  S-0815 Personalverwaltungsserver
 - ▶  APP.4.3 Relationale Datenbanksysteme
 - ▶  SYS.1.1 Allgemeiner Server
 - ▶  SYS.1.2.2 Windows Server 2012
 - ▼  Elementare Gefährdungen
 - ⚠ G 0.8 Ausfall oder Störung der Stromversorgung
 - ⚠ G 0.9 Ausfall oder Störung von Kommunikationsnetzen
 - ⚠ G 0.14 Ausspähen von Informationen (Spionage)
 - ⚠ G 0.15 Abhören
 - ⚠ G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
 - ⚠ G 0.18 Fehlplanung oder fehlende Anpassung
 - ⚠ G 0.19 Offenlegung schützenswerter Informationen
 - ⚠ G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
 - ⚠ G 0.21 Manipulation von Hard- oder Software
 - ⚠ G 0.22 Manipulation von Informationen
 - ⚠ G 0.23 Unbefugtes Eindringen in IT-Systeme
 - ⚠ G 0.25 Ausfall von Geräten oder Systemen
 - ⚠ G 0.26 Fehlfunktion von Geräten oder Systemen
 - ⚠ G 0.27 Ressourcenmangel
 - ⚠ G 0.28 Software-Schwachstellen oder -Fehler
 - ⚠ G 0.29 Verstoß gegen Gesetze oder Regelungen
 - ⚠ G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
 - ⚠ G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
 - ⚠ G 0.32 Missbrauch von Berechtigungen

Risikomanagement

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

- ▼ Modernisierter IT-Verbund
 - ▼ Geschäftsprozesse
 - ▼ GP-01 Personal
 - ▼ GP-Gefährdungen des GP
 - ! G 0.8 Ausfall oder Störung der Stromversorgung
 - ! G 0.9 Ausfall oder Störung von Kommunikationsnetzen
 - ! G 0.14 Ausspähen von Informationen (Spionage)
 - ! G 0.15 Abhören
 - ! G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
 - ! G 0.18 Fehlplanung oder fehlende Anpassung
 - ! G 0.18 Fehlplanung oder fehlende Anpassung (Kopie 1)
 - ! G 0.19 Offenlegung schützenswerter Informationen
 - ! G 0.19 Offenlegung schützenswerter Informationen (Kopie 1)
 - ! G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
 - ! G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle (Kopie 1)
 - ! G 0.21 Manipulation von Hard- oder Software
 - ! G 0.21 Manipulation von Hard- oder Software (Kopie 1)
 - ! G 0.22 Manipulation von Informationen
 - ! G 0.22 Manipulation von Informationen (Kopie 1)
 - ! G 0.23 Unbefugtes Eindringen in IT-Systeme
 - ! G 0.23 Unbefugtes Eindringen in IT-Systeme (Kopie 1)
 - ! G 0.25 Ausfall von Geräten oder Systemen
 - ! G 0.26 Fehlfunktion von Geräten oder Systemen
 - ! G 0.27 Ressourcenmangel
 - ! G 0.28 Software-Schwachstellen oder -Fehler
 - ! G 0.28 Software-Schwachstellen oder -Fehler (Kopie 1)
 - ! G 0.29 Verstoß gegen Gesetze oder Regelungen
 - ! G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
 - ! G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
 - ! G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
 - ! G 0.32 Missbrauch von Berechtigungen
 - ! G 0.32 Missbrauch von Berechtigungen (Kopie 1)
 - ! G 0.33 Personalausfall
 - ! G 0.36 Identitätsdiebstahl
 - ! G 0.36 Identitätsdiebstahl (Kopie 1)
 - ! G 0.37 Abstreiten von Handlungen
 - ! G 0.38 Missbrauch personenbezogener Daten
 - ! G 0.38 Missbrauch personenbezogener Daten (Kopie 1)
 - ! G 0.39 Schadprogramme
 - ! G 0.39 Schadprogramme (Kopie 1)
 - ! G 0.40 Verhinderung von Diensten (Denial of Service)
 - ! G 0.40 Verhinderung von Diensten (Denial of Service) (Kopie 1)
 - ! G 0.41 Sabotage
 - ! G 0.42 Social Engineering
 - ! G 0.43 Einspielen von Nachrichten

Risikomanagement im BSI IT-Grundschutz



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

- 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.

-

+



- 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

- Gefährdungsbewertung – Bewertungskriterien
 - Auswirkung in verinice

 *Informationsverbund 

<input type="text" value="unkritisch"/>	Die Schadensauswirkungen sind gering und können vernachlässigt werden.
<input type="text" value="normal"/>	Die Schadensauswirkungen sind begrenzt und überschaubar.
<input type="text" value="hoch"/>	Die Schadensauswirkungen können beträchtlich sein.
<input type="text" value="sehr hoch"/>	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Risikomanagement im BSI IT-Grundschutz



- Risikoakzeptanz
 - Abbildung im verinice

Auswirkung

sehr hoch

hoch

normal

unkritisch

mittel	hoch	sehr hoch	sehr hoch	sehr hoch
mittel	mittel	unbearbeitet	sehr hoch	sehr hoch
gering	gering	mittel	hoch	sehr hoch
gering	gering	gering	mittel	hoch

sehr selten

selten

mittel

häufig

sehr häufig

Eintrittshäufigkeit

Risikomanagement im BSI IT-Grundschutz



- Gefährdungsbewertung
 - Abbildung im verinice

Identifizier	G 0.25
Titel	Ausfall von Geräten oder Systemen
Tags	
Beschreibung	
Dokument	
Betrifft Vertraulichkeit	<input type="checkbox"/>
Betrifft Integrität	<input type="checkbox"/>
Betrifft Verfügbarkeit	<input checked="" type="checkbox"/>
▼ Risiko ohne zusätzliche Maßnahmen	
Eintrittshäufigkeit	häufig
Auswirkung	beträchtlich
Risiko	hoch
▼ Risikobehandlungsoption	
Risikobehandlung	Risikoreduktion
Erläuterung zur Risikobehandlung	

Risikomanagement & Datenschutz

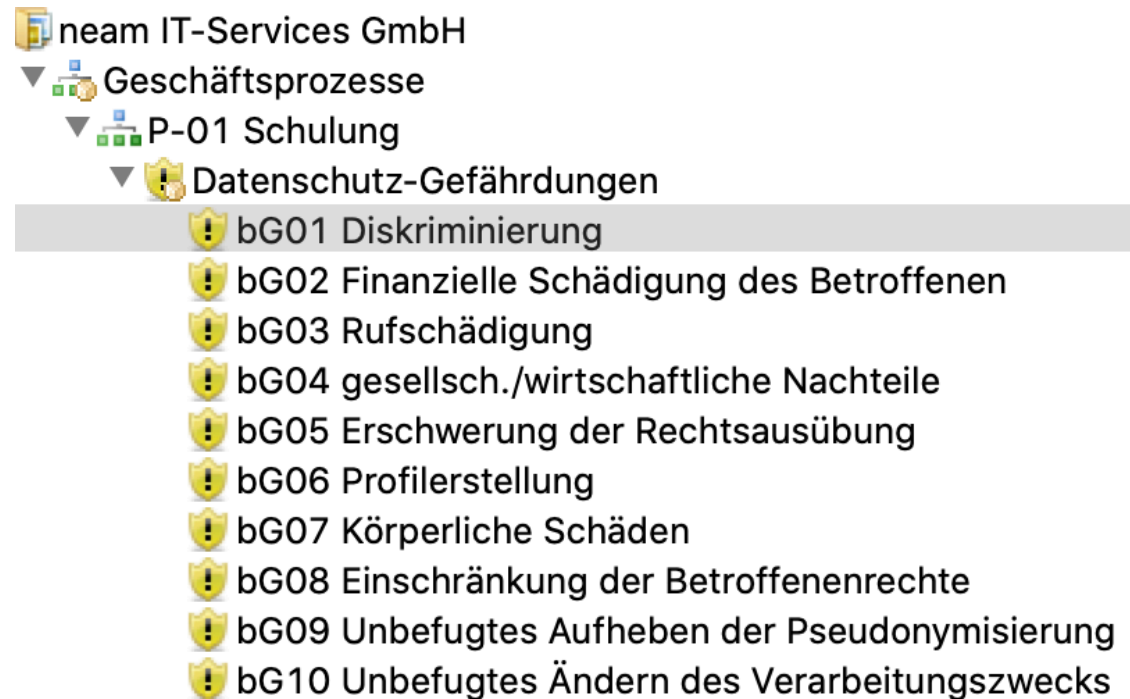


- Informationssicherheit
 - Sicht der Organisation
 - ISO 27005, BSI Standard 200-3
- Datenschutz
 - Sicht der Betroffenen
 - DSGVO Art 32 (TOMs), 35 (DSFA)
 - Standarddatenschutzmodell (SDM)

Unter Berücksichtigung des **Standes 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-Kompodium
 - CNIL
 - ISO 29151
- Bestandteil einer DSFA



Schwachstelle

Bedrohung

Dokument

Betrifft Vertraulichkeit

Betrifft Integrität

Betrifft Verfügbarkeit

▼ Risiko ohne Maßnahmen

Eintrittshäufigkeit

Auswirkung

Risiko

▼ Risiko ohne zusätzliche Maßnahmen

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

▼ Risiko mit zusätzlichen Maßnahmen

Eintrittshäufigkeit

Auswirkung

Risiko

Unter Berücksichtigung des **Standes 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>
