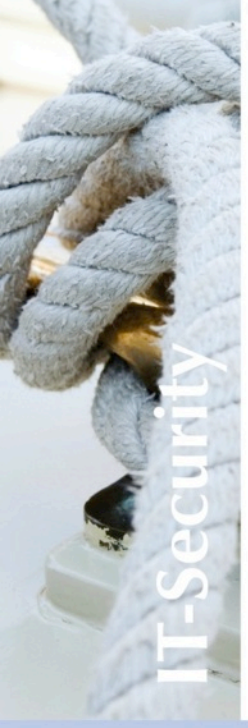


IT-Security neam Wir setzen Segel!

Einführung eines ISMS nach ISO 27001

Kai Wittenburg,

Geschäftsführer/CEO, ISO27001-Auditor (BSI)

neam

neam IT-Services GmbH | Technologiepark 21 | 33100 Paderborn
fon (+49) 52 51 / 16 52-0 | fax -444 | security@neam.de | www.neam.de

Was ist Informationssicherheit?

- **Vorhandensein von**
  - **Integrität**
  - **Vertraulichkeit und**
  - **Verfügbarkeit**

  in einem geplanten Ausmaß.

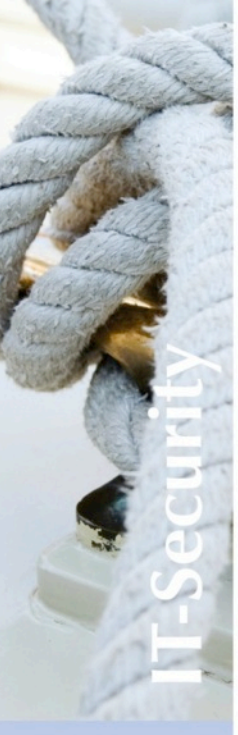
DIE Bedrohung

Wichtigste langfristige Bedrohungsquelle:

Mitarbeiter („HumanOS“)

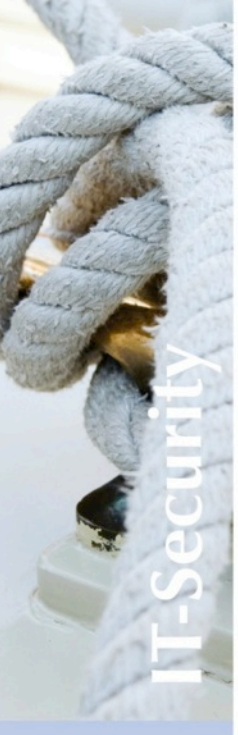
- „Schwächstes Glied“ in der Sicherheitskette
- Fehlende Sicherheitskenntnisse/ Schulungen
- Fehlende umfassende personelle Konzepte
- Leichte Opfer für Social Engineering
- Oft zu weit reichende Berechtigungen


Dieses Büro ist z.Zt.
unbesetzt.
Bitte melden Sie sich
auf einem der
benachbarten
Zimmer.



IT-Security

neam



ISO 2700x ISMS Standards

IT-Security neam Wir setzen Segel!

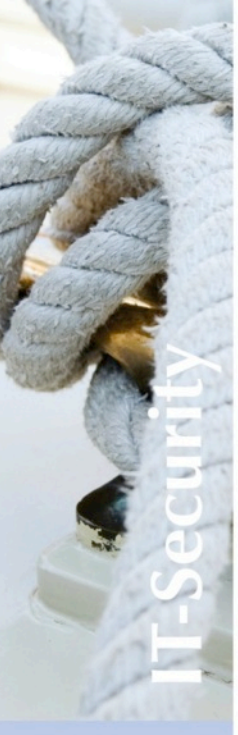
ISO 27000 Terms and Definitions

ISO 27005
Risk
Management

ISO 27001
Information Security Management System

Model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System

BS7799-2



ISO 2700x ISMS Standards

IT-Security neam Wir setzen Segel!

ISO 27000 Terms and Definitions

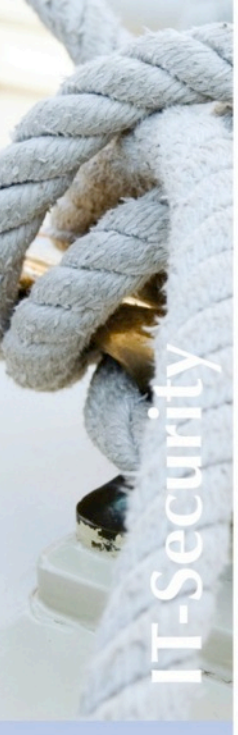
ISO 27005
Risk
Management

ISO 27001
Information Security Management System

ISO 27002
Code of Practice

Set of controls, including policies, processes, procedures, organizational structures, software/ hardware functions

BS7799-1



ISO 2700x ISMS Standards

IT-Security neam Wir setzen Segel!

ISO 27000 Terms and Definitions

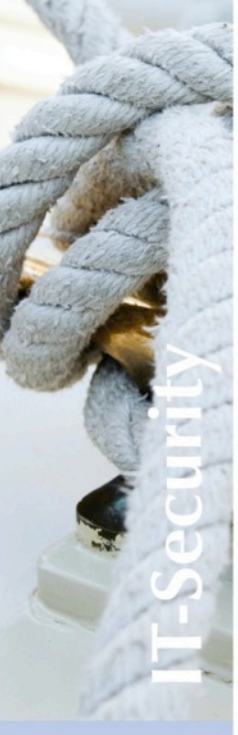
ISO 27005
Risk
Management

ISO 27001
Information Security Management System

ISO 27002
Code of Practice

ISO 27003
Implementation Guidance

Instructions how to [technically]
implement ISO 27001



ISO 2700x ISMS Standards

IT-Security neam Wir setzen Segel!

ISO 27000 Terms and Definitions

ISO 27005
Risk
Management

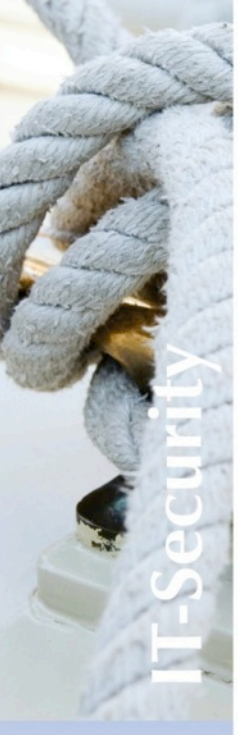
ISO 27001
Information Security Management System

ISO 27002
Code of Practice

ISO 27003
Implementation Guidance

ISO 27004
Metrics and Measurements

Definition of KPIs, quantitative/
qualitative measurements, metrics etc.



ISO 2700x ISMS Standards

IT-Security neam Wir setzen Segel!

ISO 27000 Terms and Definitions

ISO 27005
Risk
Management

ISO 27001
Information Security Management System

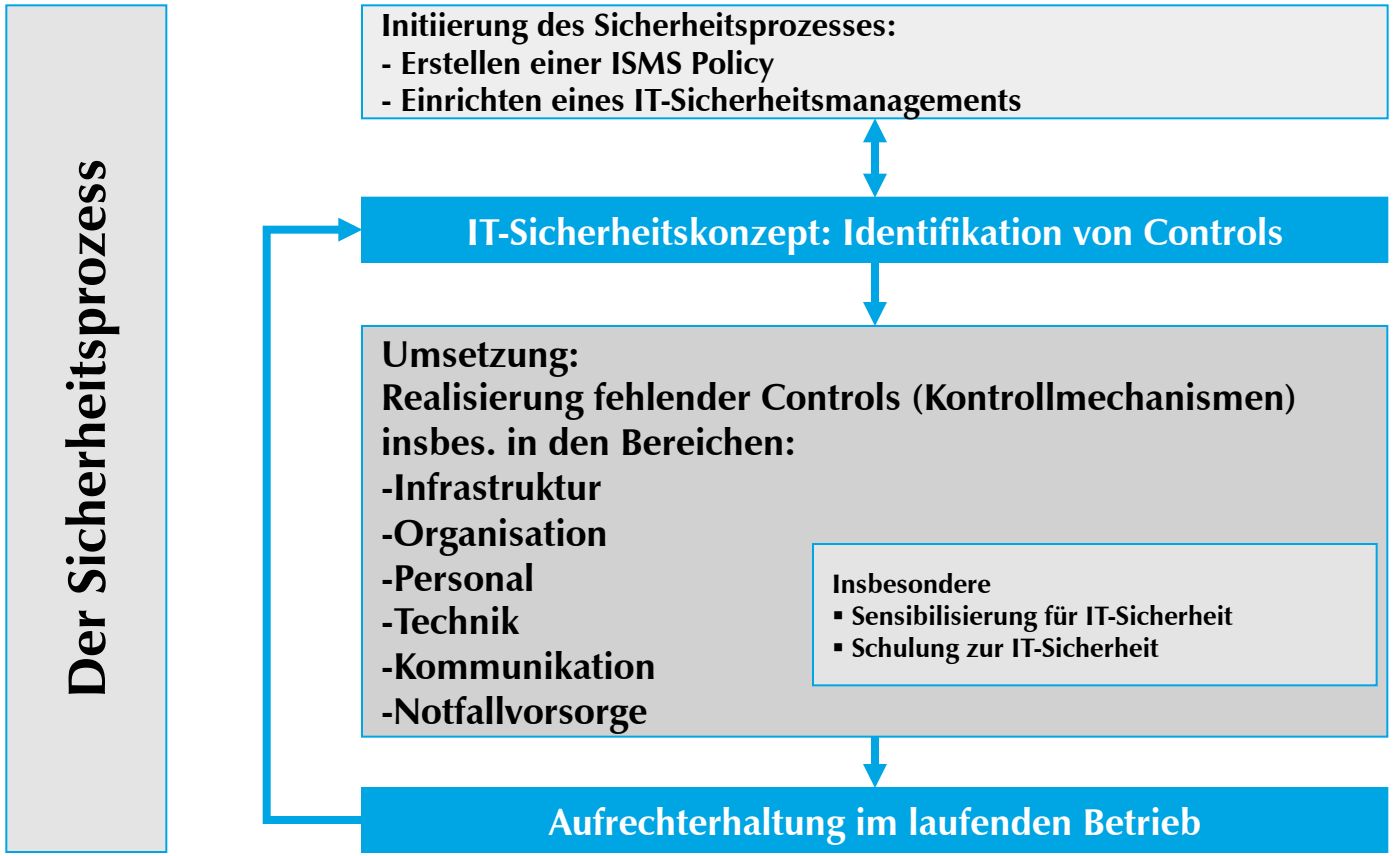
ISO 27002
Code of Practice

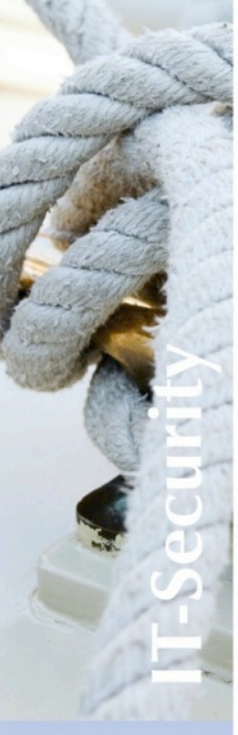
ISO 27003
Implementation Guidance

ISO 27004
Metrics and Measurements

ISO 27015 Accreditation Guidelines

Sicherheit als Prozess (PDCA)





5 Schritte zum ISMS

IT-Security neam Wir setzen Segel!

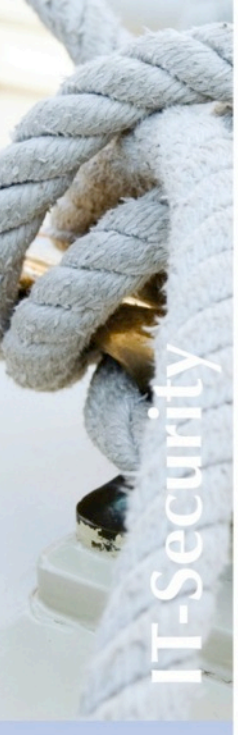
1. Schritt
- Managementunterstützung für ISMS Einführung und Aufbau

2. Schritt
- Festlegung des Geltungsbereichs
- Festlegung der Sicherheitsleitlinie (ISMS Policy)

3. Schritt
- Organisationsanalyse

4. Schritt
- Risikoanalyse
- Identifikation von Kontrollmechanismen und Maßnahmen

5. Schritt
- (Aus-)Gestaltung des ISMS



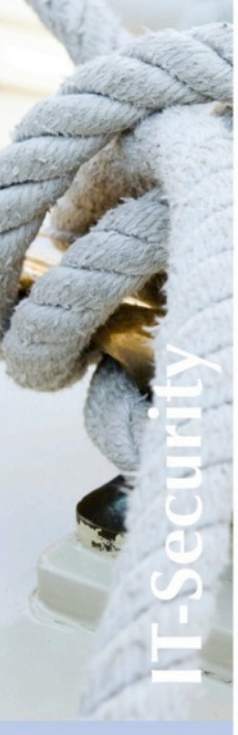
Initiierung des IT-Sicherheitsprozesses

IT-Security neam Wir setzen Segel!

Verantwortung des Managements

Einrichten des IT-Sicherheits-managements

- **Grundregeln**
  - Die Initiative für IT-Sicherheit geht vom Management aus.
  - Die Verantwortung für IT-Sicherheit liegt beim Management.
  - Nur wenn sich das Management um IT-Sicherheit bemüht, wird die Aufgabe "IT-Sicherheit" wahrgenommen.
  - Vorbildfunktion



5 Schritte zum ISMS

IT-Security neam Wir setzen Segel!

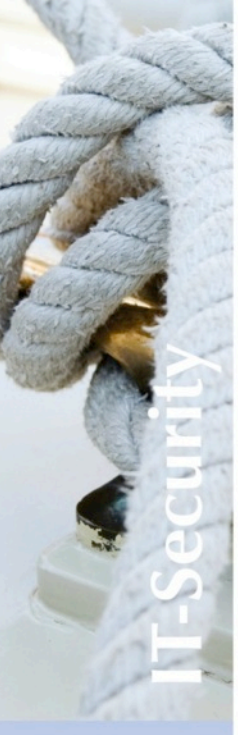
1. Schritt
- Managementunterstützung für ISMS Einführung und Aufbau

2. Schritt
- Festlegung des Geltungsbereichs
- Festlegung der Sicherheitsleitlinie (ISMS Policy)

3. Schritt
- Organisationsanalyse

4. Schritt
- Risikoanalyse
- Identifikation von Kontrollmechanismen und Maßnahmen

5. Schritt
- (Aus-)Gestaltung des ISMS



5 Schritte zum ISMS

IT-Security neam Wir setzen Segel!

1. Schritt
- Managementunterstützung für ISMS Einführung und Aufbau

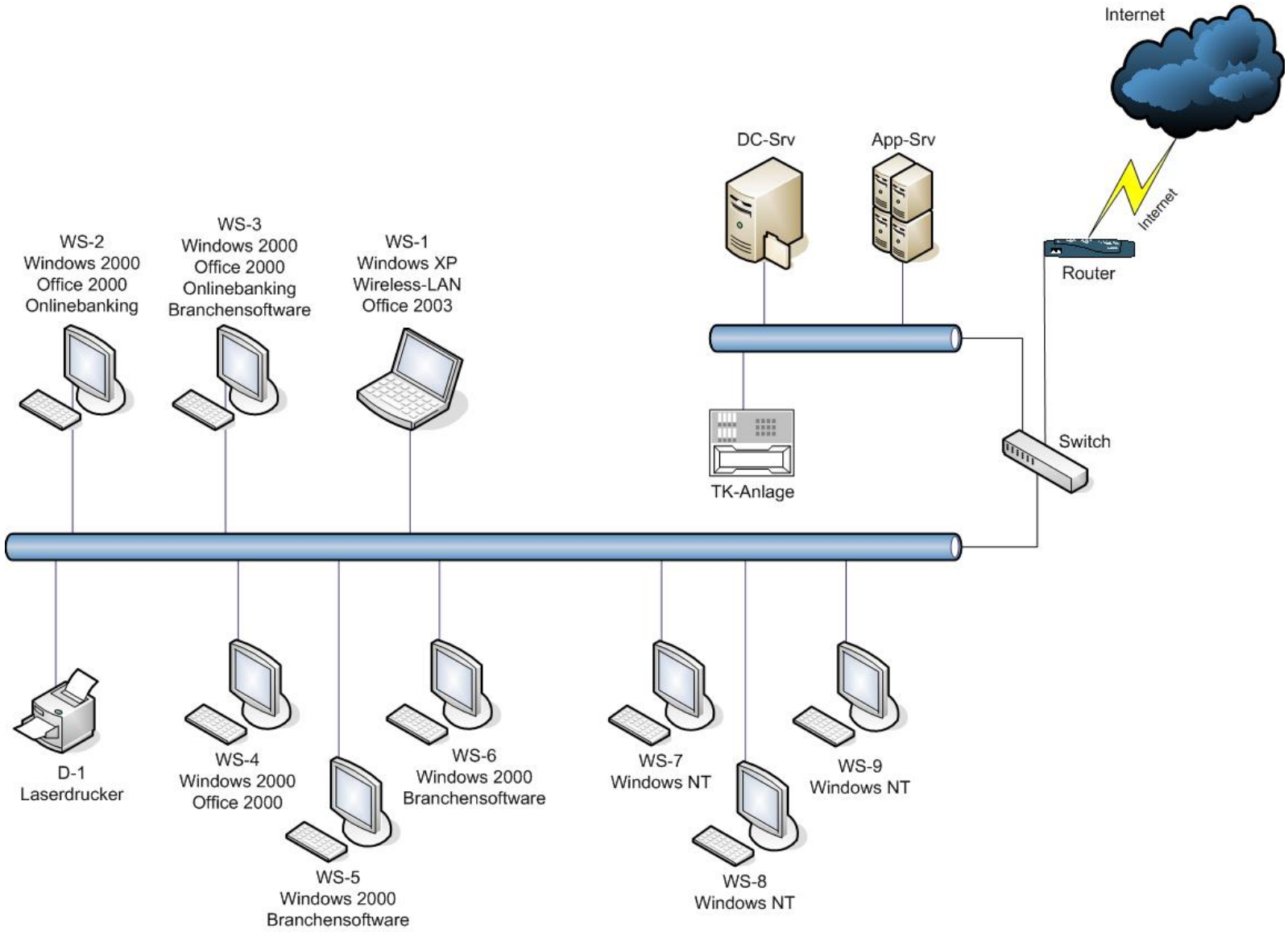
2. Schritt
- Festlegung des Geltungsbereichs
- Festlegung der Sicherheitsleitlinie (ISMS Policy)

3. Schritt
- Organisationsanalyse

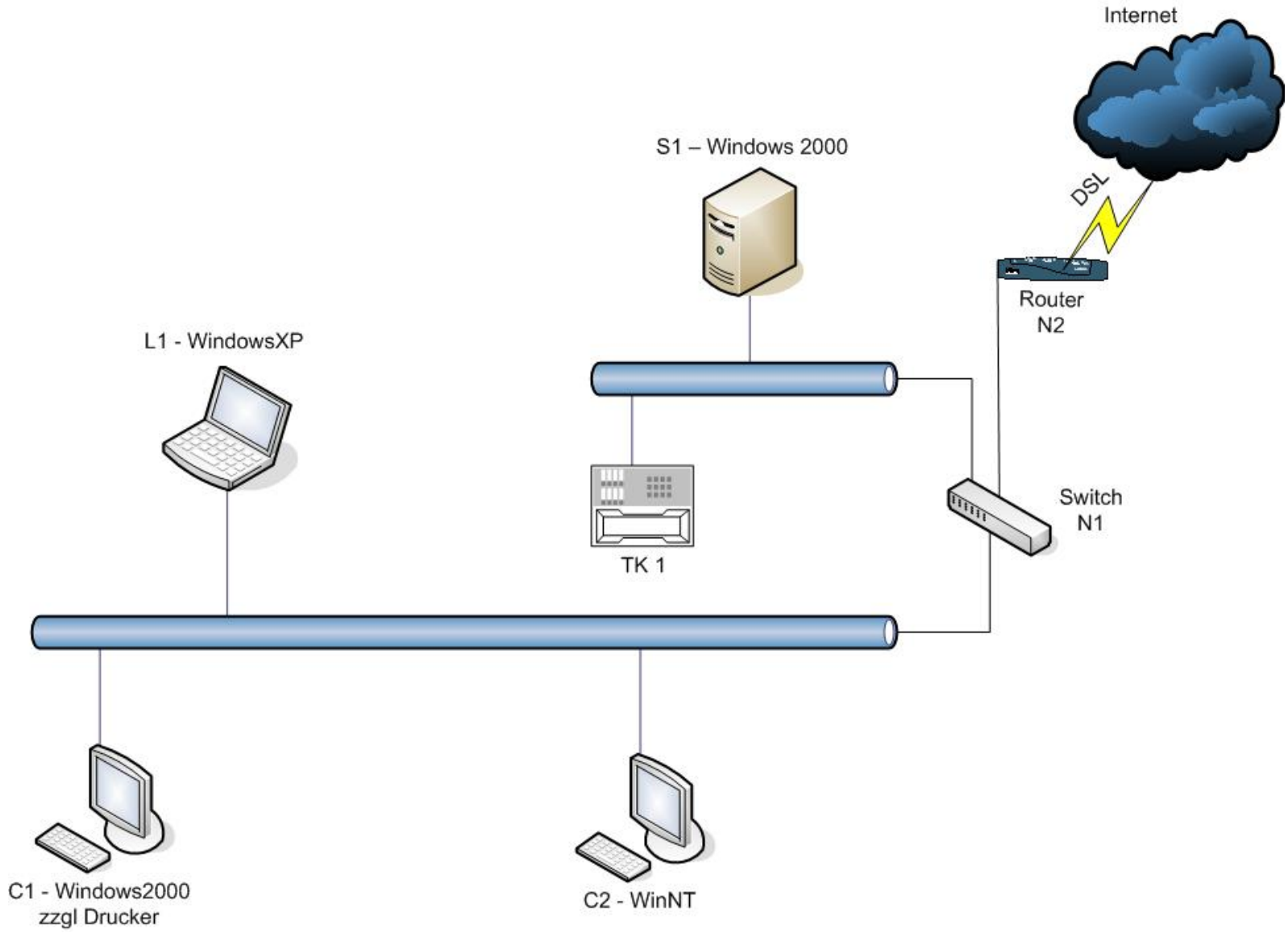
4. Schritt
- Risikoanalyse
- Identifikation von Kontrollmechanismen und Maßnahmen

5. Schritt
- (Aus-)Gestaltung des ISMS

Netzplan

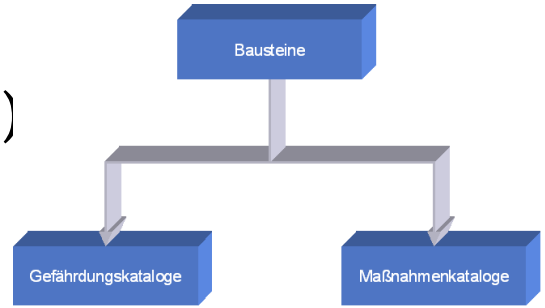

Internet
Internet
DC-Srv
App-Srv
Router
Switch
TK-Anlage
WS-2
Windows 2000
Office 2000
Onlinebanking
WS-3
Windows 2000
Office 2000
Onlinebanking
Branchensoftware
WS-1
Windows XP
Wireless-LAN
Office 2003
D-1
Laserdrucker
WS-4
Windows 2000
Office 2000
WS-5
Windows 2000
Branchensoftware
WS-6
Windows 2000
Branchensoftware
WS-7
Windows NT
WS-8
Windows NT
WS-9
Windows NT

Netzplan - bereinigt

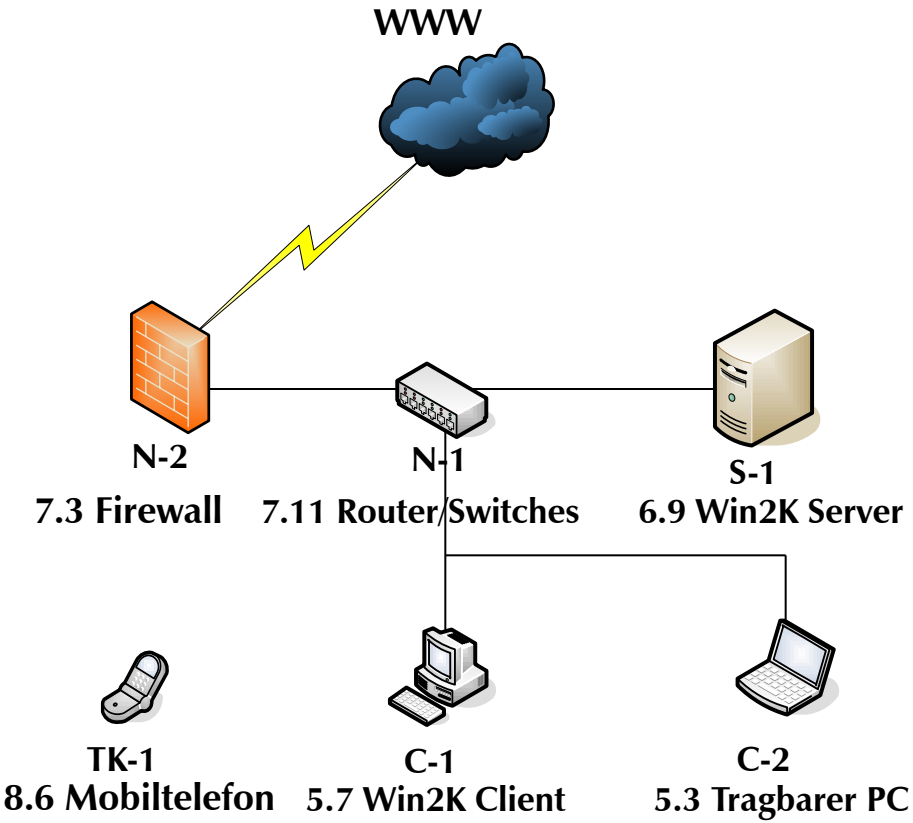


Grundschutzkataloge

- Bausteinbeschreibung
- Darstellung der Gefährdungslage
- Maßnahmenempfehlungen
  - Planung und Konzeption
  - Beschaffung (sofern erforderlich)
  - Umsetzung
  - Betrieb
  - Aussonderung (sofern erforderlich)
  - Notfallvorsorge



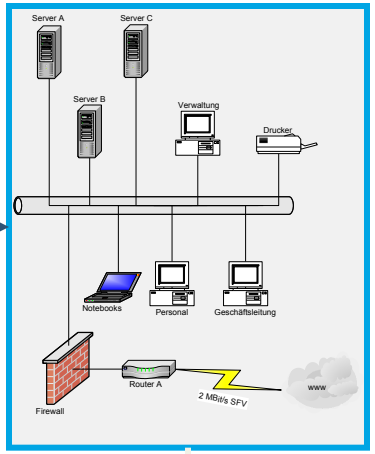
Grundschutzkataloge



IT- Grundschutzkataloge

Basis-Sicherheitscheck

IT-Grundschutzmodell

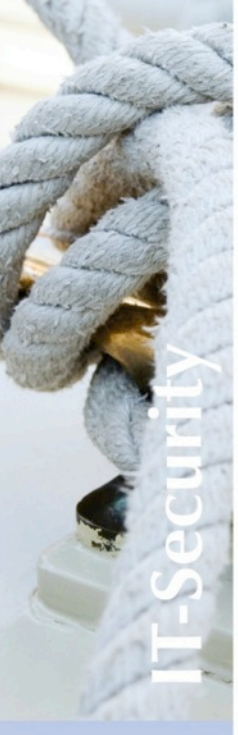


Maßnahmen-empfehlungen

Soll-Ist-Vergleich

Realisierte Maßnahmen

Sicherheitskonzept: defizitäre Maßnahmen



5 Schritte zum ISMS

IT-Security neam Wir setzen Segel!

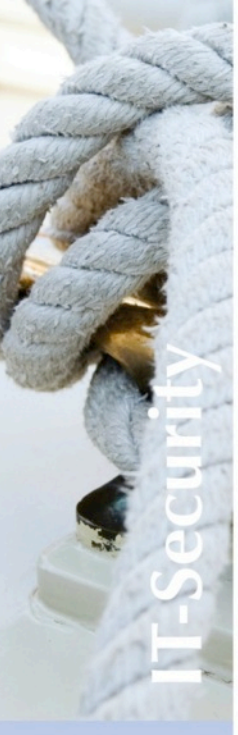
1. Schritt
- Managementunterstützung für ISMS Einführung und Aufbau

2. Schritt
- Festlegung des Geltungsbereichs
- Festlegung der Sicherheitsleitlinie (ISMS Policy)

3. Schritt
- Organisationsanalyse

4. Schritt
- Risikoanalyse
- Identifikation von Kontrollmechanismen und Maßnahmen

5. Schritt
- (Aus-)Gestaltung des ISMS



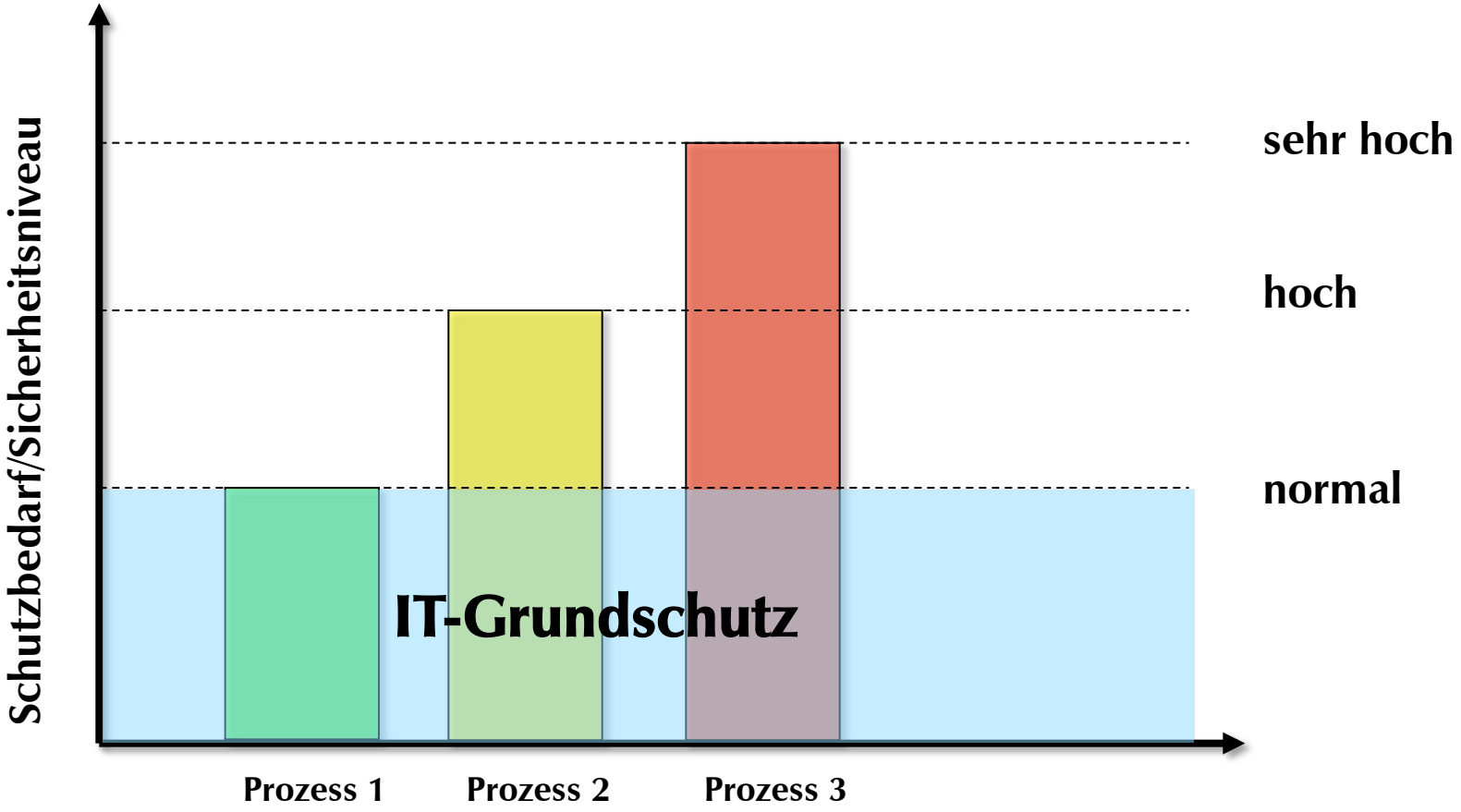
Schutzbedarfsfeststellung

Definition der Schutzbedarfs-kategorien

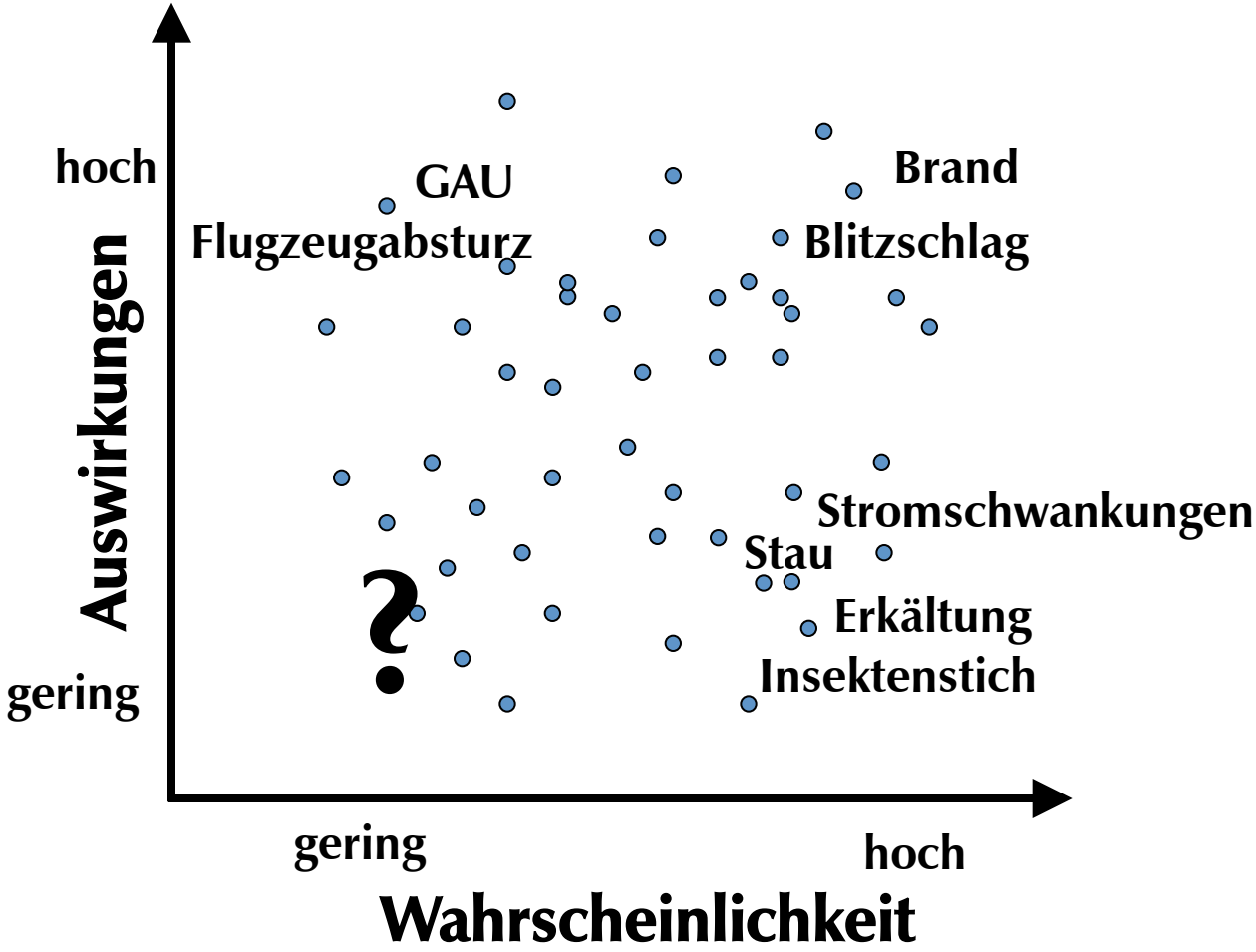
- **Definitionen der Kategorien müssen individuell angepasst werden**
- **Normal**
  - **Schadensauswirkungen sind begrenzt und überschaubar.**
- **Hoch**
  - **Schadensauswirkungen können beträchtlich sein.**
- **Sehr hoch**
  - **Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.**

Rechtliches, Datenschutz, Marketing, Finanzen, Gesundheit... => Vertraulichkeit, Integrität, Verfügbarkeit

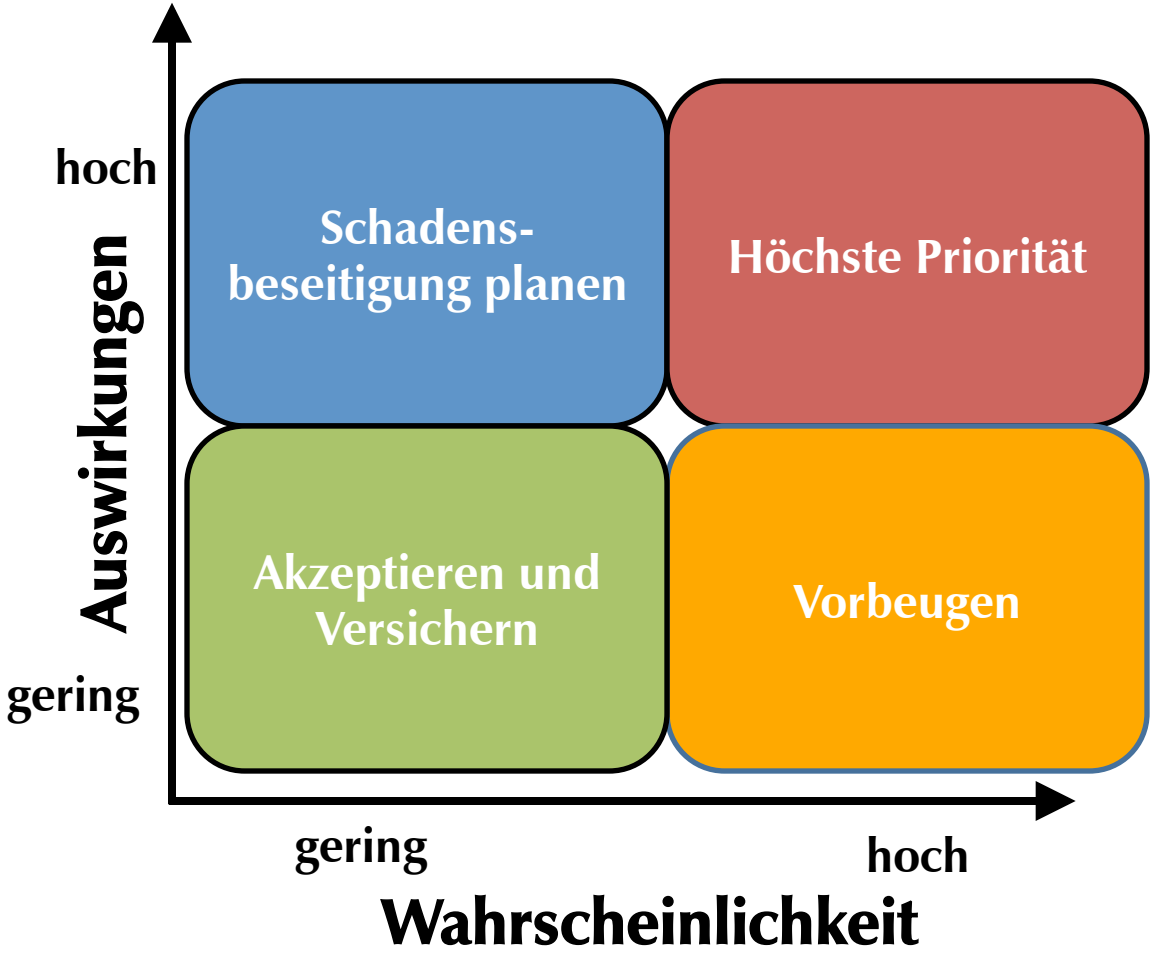
Schutzbedarfsfeststellung



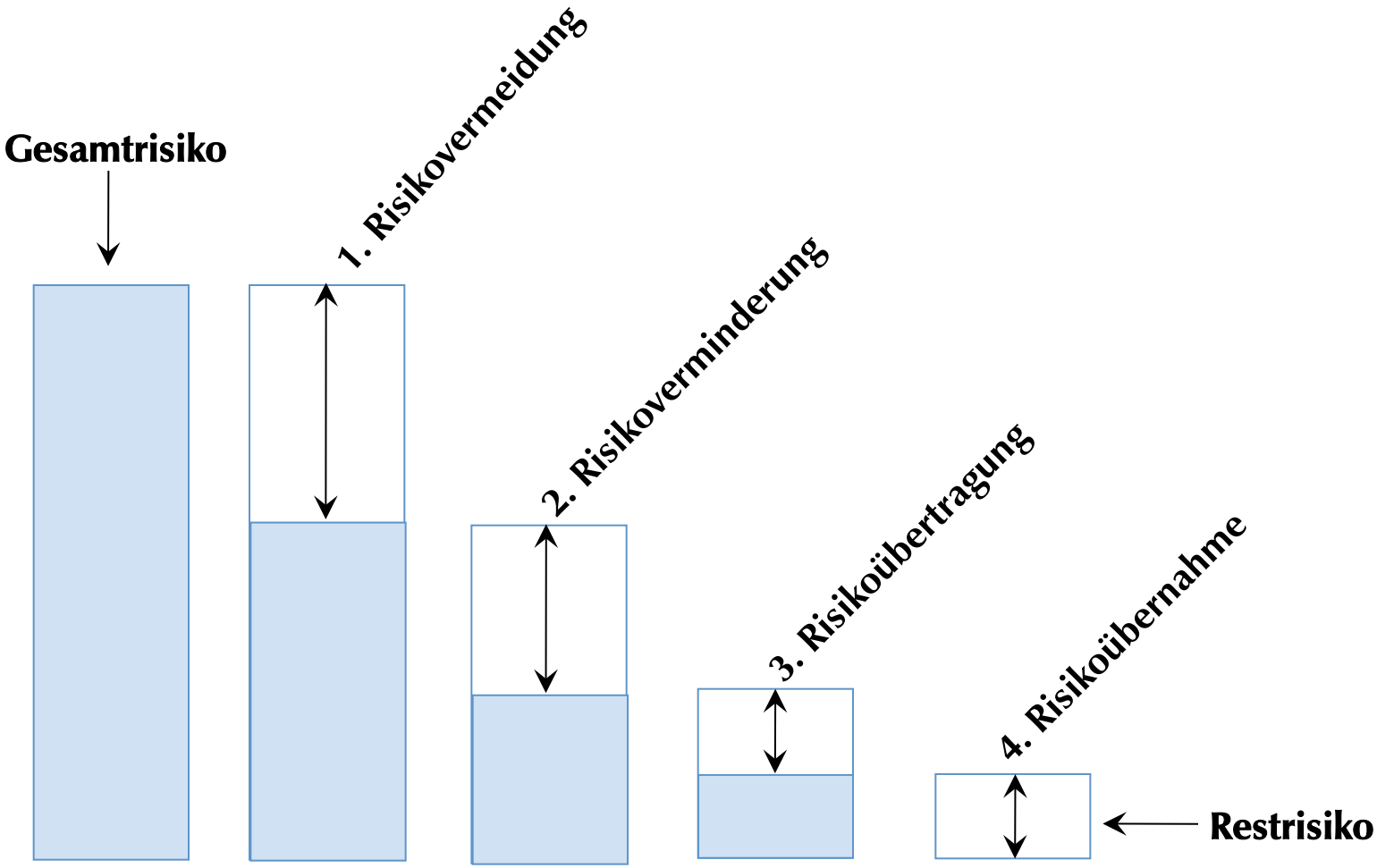
Höherer Schutzbedarf: Risikoanalyse

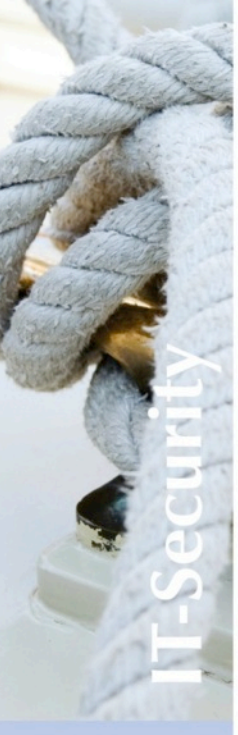


Höherer Schutzbedarf: Risikoanalyse



Abgestufte Risikobewältigung





5 Schritte zum ISMS

IT-Security neam Wir setzen Segel!

1. Schritt
- Managementunterstützung für ISMS Einführung und Aufbau

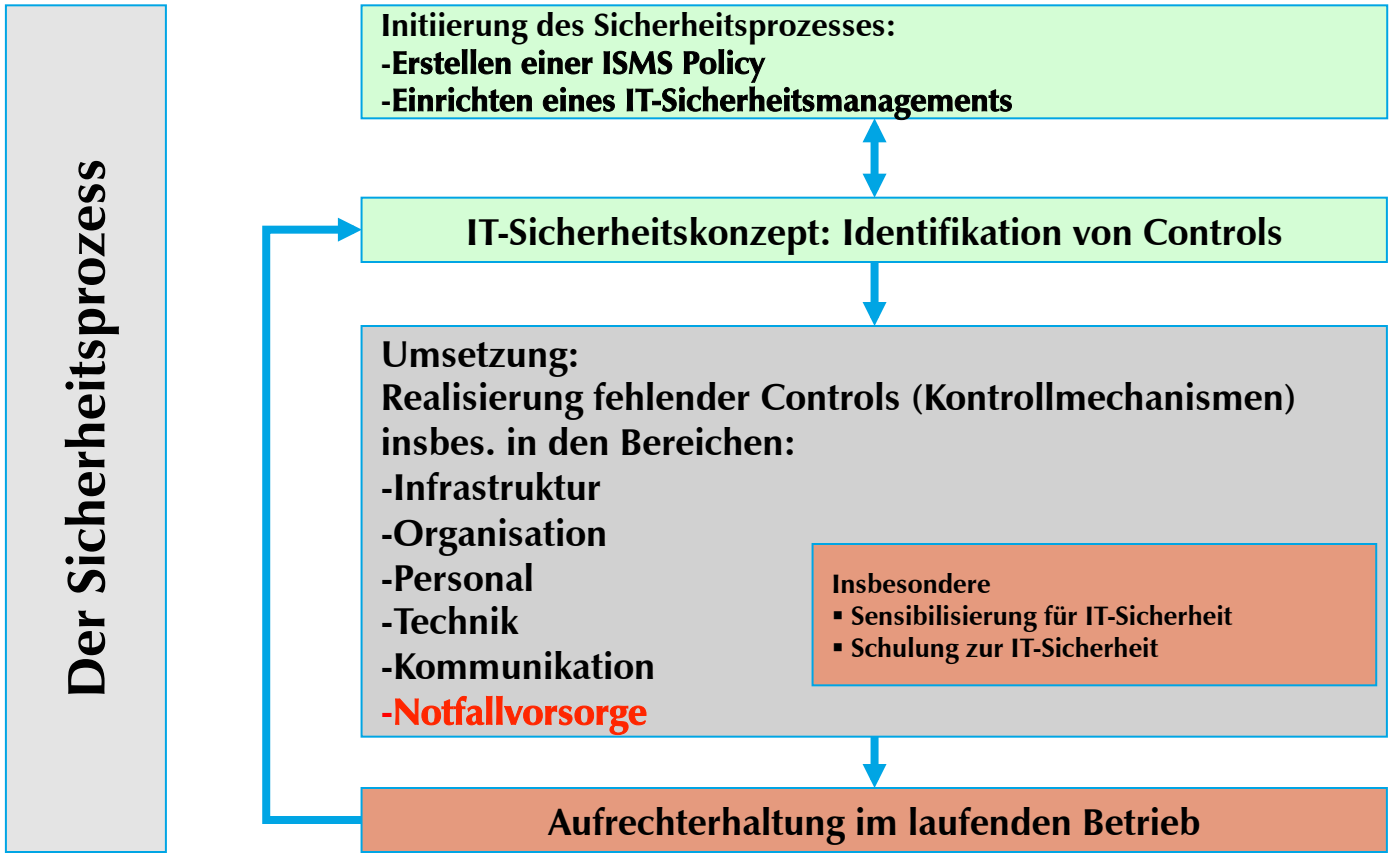
2. Schritt
- Festlegung des Geltungsbereichs
- Festlegung der Sicherheitsleitlinie (ISMS Policy)

3. Schritt
- Organisationsanalyse

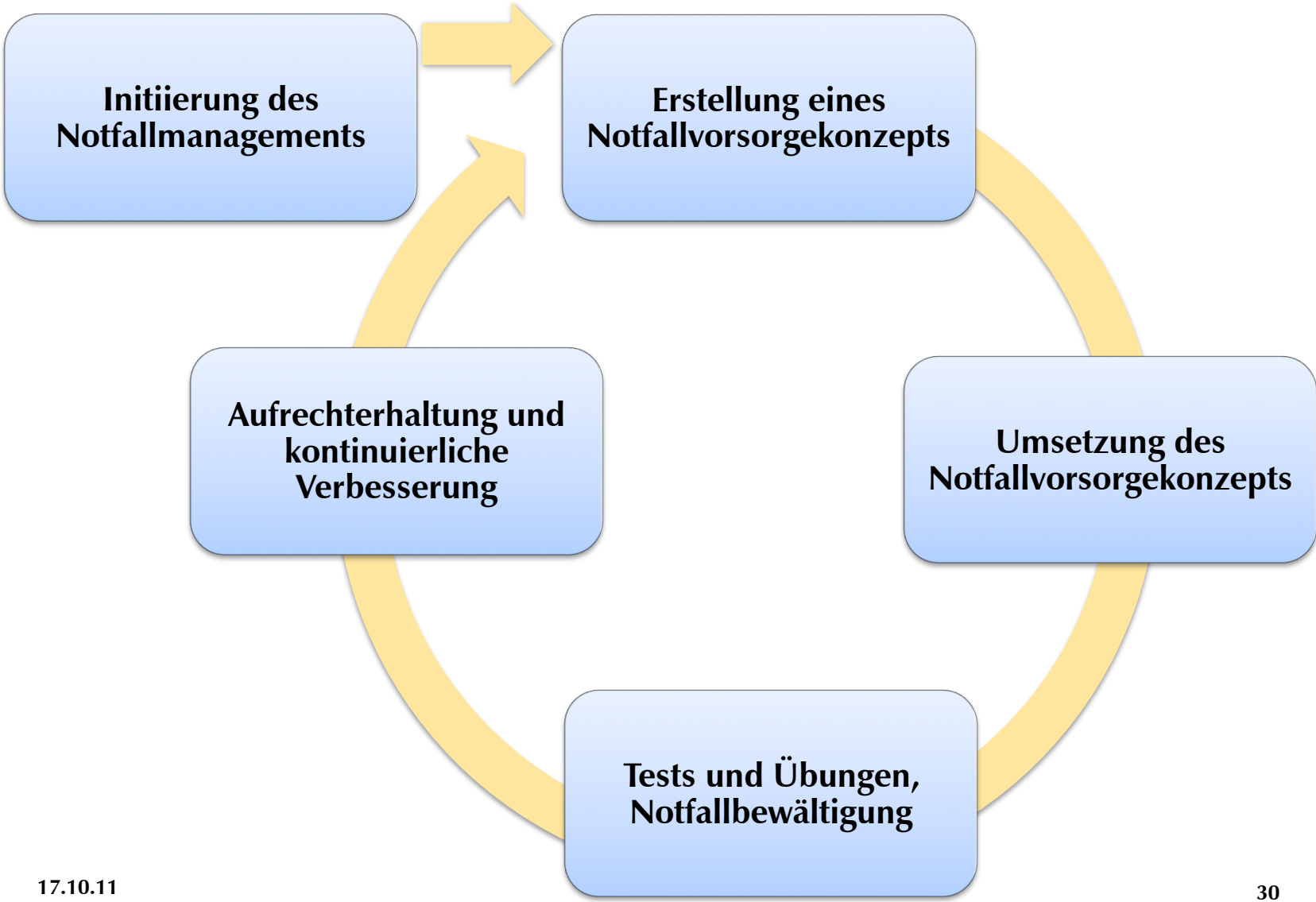
4. Schritt
- Risikoanalyse
- Identifikation von Kontrollmechanismen und Maßnahmen

5. Schritt
- (Aus-)Gestaltung des ISMS

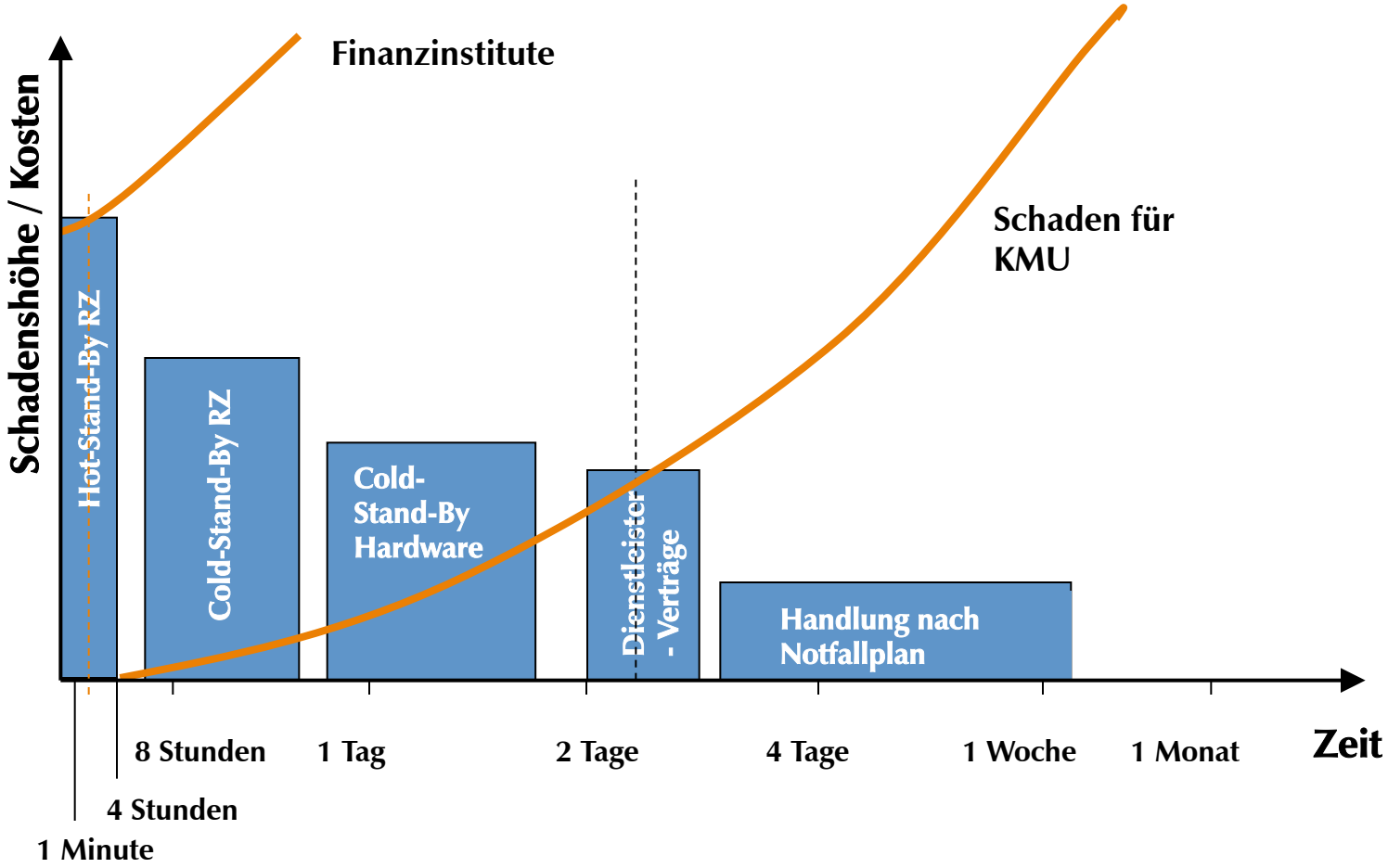
Sicherheit als Prozess (PDCA)



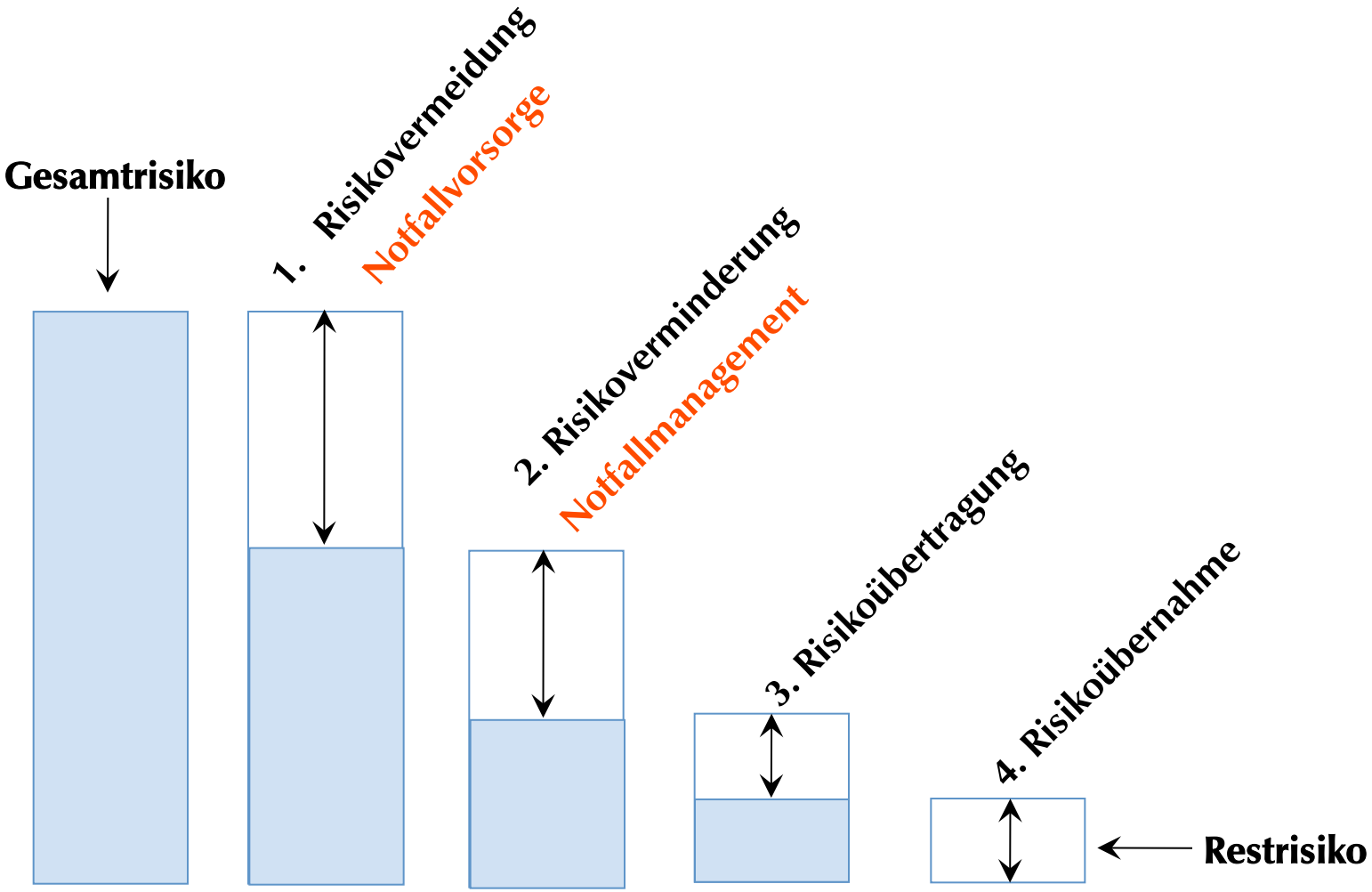
Notfallvorsorge

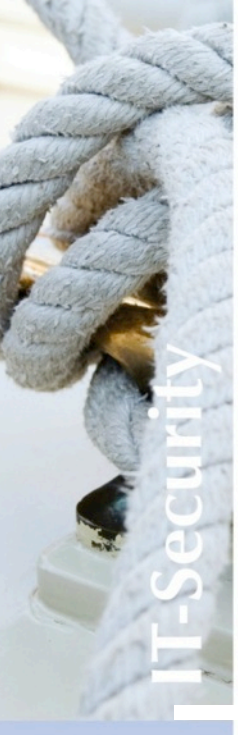


Notfallvorsorge



Risikobewältigung





IT-Security

neam

Wir setzen Segel!

neam IT-Services GmbH
Stand C11

Technologiepark 21
D-33100 Paderborn

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

http://www.neam.de
info@neam.de

17.10.11