Was beinhaltet der Begriff *IT-Sicherheit*?

Dauer: 45 min (Präsentation inklusive Diskussion)

IHK Darmstadt / IT-Leiter-Treff am 02. Dezember 2010

(rev.)

Unternehmensberatung *Holliday Consulting*

- gegründet Anfang 2004

- berät und begleitet Umsetzungen zu den Themen:

- **IT-Sicherheit**
- **IT-Prozessmanagement**
- **IT-Servicemanagement nach ITIL**

- Internetadresse: www.holliday-consulting.com

Unternehmensberatung *Holliday Consulting*

- kooperiert mit vielfältigen Partnerunternehmen zur Lösung komplexer Aufgabenstellungen:

- **zur Unternehmenssteuerung (Balanced Scorecard)**
- **zum Business Process-Reengineering (TQM)**
- **zur Erzielung eines IT-Sicherheitszertifikats nach ISO 27001 oder BSI IT-Grundschutz**

Der Begriff *IT-Sicherheit*

- **noch besser:** ***Informationssicherheit (IS)***
- **Zielsetzung der IS:**
  - Informationen und Daten schützen vor dem Verlust von:
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - Echtheit (Authentizität)
  - betrifft nicht nur elektronisch abgespeicherte Daten, sondern auch das gesprochene Wort, sowie materielle Dokumentationen (Papiere, Aufzeichnungen, Mikrofilme etc.)

Informationssicherheit (IS)

- **erfordert eine konzertierte systemische Handlungsweise (ein ganzheitliches Handeln) mit den Aspekten:**
  - Organisation
  - Regelwerke
  - Personal
  - Bewusstheit („Awareness“)
  - Schulung („Skills entwickeln“)
  - Technologie (die „IT-Sicherheit“)
  - Überprüfungen

Bedrohungen der IS

- *55 %* aller Bedrohungen kommen von Innen

- Verteilung nach Art der Bedrohungen:

Datendiebstahl	*78 %*
Fahrlässigkeit der Mitarbeiter	*65 %*
Viren	*50 %*
Hacker	*41 %*
Spam	*32 %*
Sabotage	*15 %*
Fehler an HW oder SW	*12 %*
Finanzieller Betrug	*8 %*

System D - BSI IT-Grundschutz

- **entwickelt vom nationalen *B*undesamt für *S*icherheit in der *I*nformationstechnik (www.bsi.de)**

- **mit der Zielsetzung:**

  - Anwendern aus Behörden und Unternehmen praxisnahe und handlungsorientierte Hinweise für IT-Sicherheit zu geben

  - um hochkomplexe Vorgehensweisen zu vermeiden

  - um die Einstiegshürde in einen IT-Sicherheitsprozess so niedrig wie möglich zu halten

  - in der neueren Ausgabe die ISO 27001 (internationale Zertifizierung für Informationssicherheit) zu integrieren

BSI IT-Grundschutz - die Idee

- ***Typische*** **IT-Komponenten**
- ***Typische*** **Gefährdungen, Schwachstellen und Risiken**
- **Konkrete Umsetzungshinweise für das IT-Sicherheitsmanagement**
- **Empfehlung geeigneter Bündel von Standard-IT-Sicherheitsmaßnahmen**
- **Vorbildliche Lösungen aus der Praxis – „Best Practice"-Ansätze**

BSI IT-Grundschutz - IT-Sicherheitsprozess

- **Maßnahmen für die erfolgreiche Etablierung eines kontinuierlichen und effektiven IT-Sicherheitsprozesses:**

  - die Einführung eines IT-Sicherheitsmanagements, das die Aufgaben zur IT-Sicherheit konzipiert, koordiniert und überwacht
  - die Analyse und Dokumentation der Struktur der vorliegenden Informationstechnik (IT)
  - die Durchführung einer Schutzbedarfsfeststellung, um zu ermitteln, welcher Schutz für die Informationen und die eingesetzte IT ausreichend und angemessen ist
  - die Modellierung der Komponenten des vorliegenden IT-Verbunds durch die Bausteine der IT-Grundschutz-Kataloge
  - die Durchführung eines Basis-Sicherheitschecks, um einen Überblick über das vorhandene IT-Sicherheitsniveau zu erhalten
  - die Umsetzung der fehlenden Sicherheitsmaßnahmen

Exkurs: „Prozess“

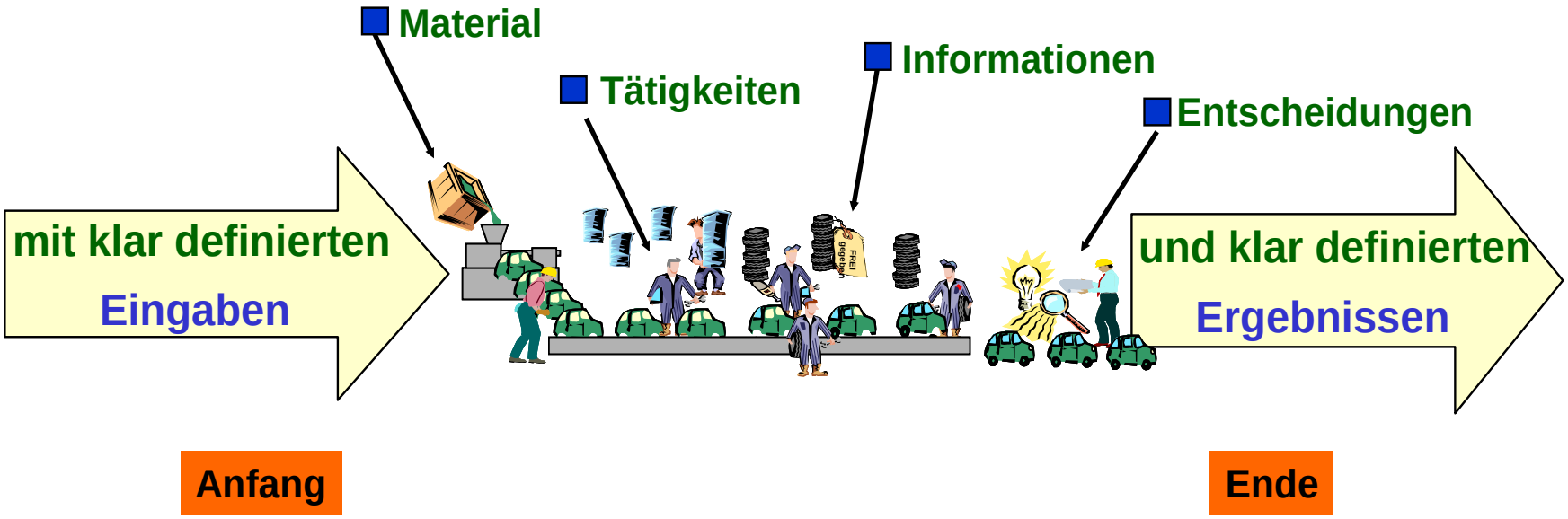
- **Begriffsdefinition:**

Ein Prozess ist

- eine zeitlich logische Abfolge
- miteinander verknüpfter Tätigkeiten
- zur Umwandlung von Eingaben
  in Ergebnisse (materiell und immateriell).

Exkurs: „Prozess“

- **Prozess im schematischen Schaubild:**

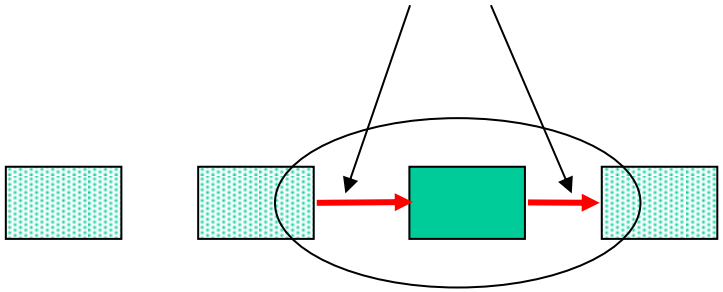


Exkurs: „Prozess“

- **funktionalorientierte vs. prozessorientierte Organisation:**

Funktionalorientierte Organisation

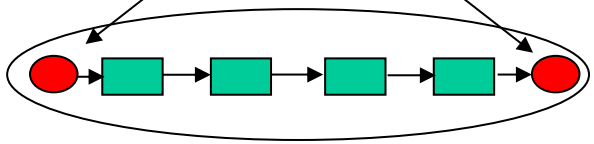
Denken in Bereichen



Bereichsorientierte Kunden/Lieferantenbeziehungen

Prozessorientierte Organisation

Denken in Prozessen und Gesamtergebnissen



Optimale Beziehungen zwischen Kunden und Lieferanten entlang der Wertschöpfung werden angestrebt

BSI IT-Grundschutz - Publikationen

- der BSI IT-Grundschutz ist ursprünglich in Form eines Grundschutzhandbuchs **(GSHB)** in verschiedenen Auflagen publiziert worden

- zwecks Harmonisierung mit dem Normenpaar **ISO 27001** und **27002** wird er seit August 2006 in zwei Bestandteilen herausgebracht:

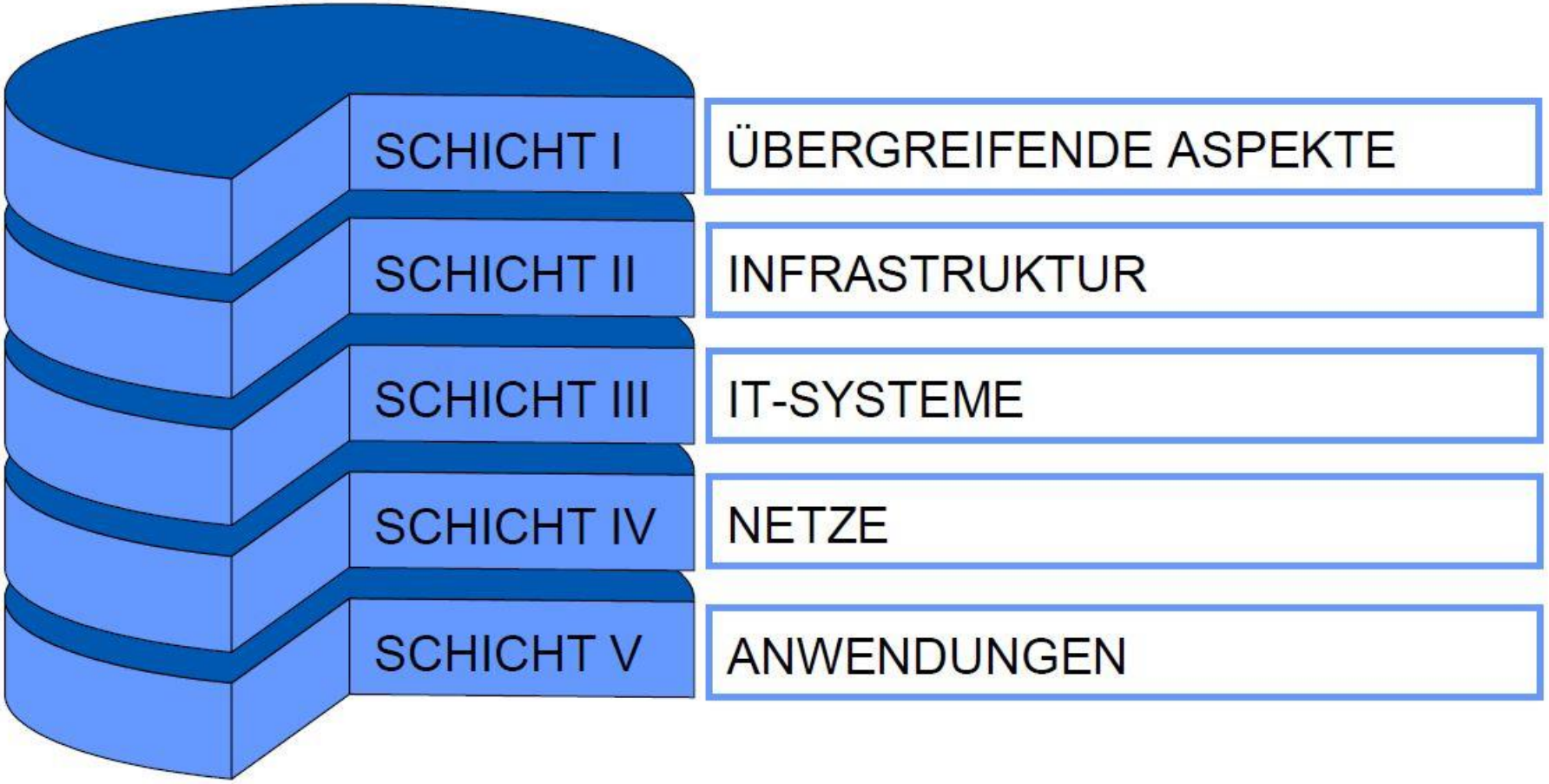
  - die BSI-Standardreihe zum Informationssicherheitsmanagement bestehend aus vier Bänden und einem Prüfschema:
    - **BSI-Standard 100-1**
      Managementsysteme für Informationssicherheit
    - **BSI-Standard 100-2**
      Vorgehensweise nach IT-Grundschutz
    - **BSI-Standard 100-3**
      Risikoanalyse auf der Basis von IT-Grundschutz
    - **BSI-Standard 100-4**
      Notfallmanagement
    - **Prüfschema:** ISO 27001-Zertifizierung mit IT-Grundschutz

  - die **IT-Grundschutz-Kataloge** („IT-Grundschutzhandbuch")

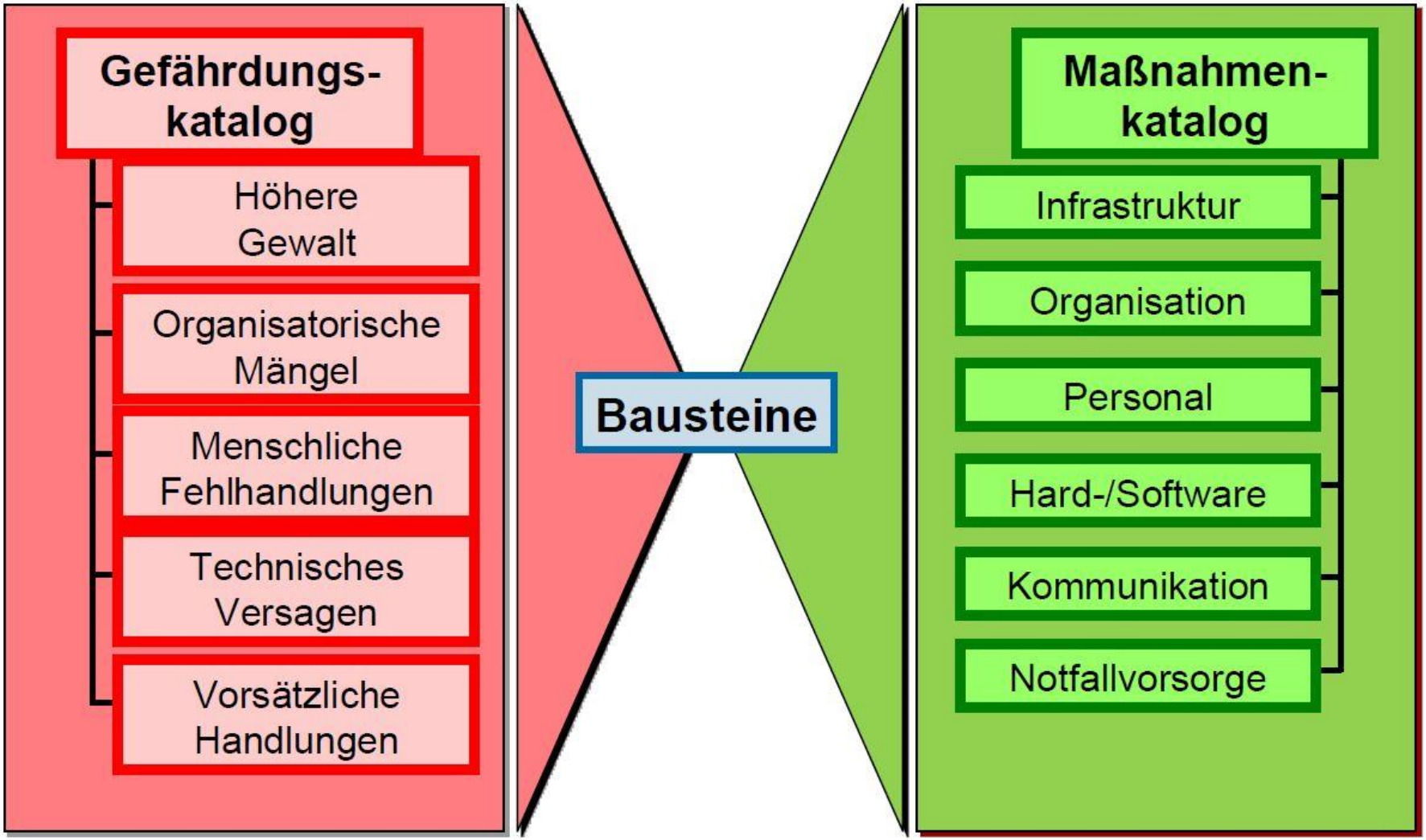
BSI Grundschutz – IT-Grundschutz-Kataloge

- **die IT-Grundschutz-Kataloge:**
  - haben voran gestellte Kapitel zur Einführung
    - über die Anwendungsweise der IT-Grundschutz-Kataloge
    - geben Hinweise zur Modellierung
  - die Grundschutz-Bausteine sind gruppiert anhand eines Schichtenmodells
  - das Schichtenmodell dient dazu
    - die Bausteine des Handbuchs einfacher auf einen komplexen IT-Verbund abzubilden
    - Redundanzen zu vermeiden, indem übergeordnete Aspekte und gemeinsame infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet werden

BSI Grundschutz – Themengebiete der Bausteine



BSI Grundschutz – Struktur der Bausteine



System I - ISO 27000 Familie

- **Die aktuelle ISO 2700X Familie:**
  - ISO 27000:2009 Überblick und Vokabular
  - ISO 27001:2005 die „Zertifizierungs-ISO“
    - Titel der ISO 27001: „ISMS - Requirements“
  - ISO 27002:2005
    - Titel der ISO 27002: „Code of Practice for ISM“
    - sie beinhaltet im Wesentlichen generische Best Practice Empfehlungen zur Handhabung der Informationssicherheit
  - ISO 27003:2010 Leitfaden zur Implementierung
  - ISO 27004:2009 IS-Management - Metriken und Messungen
  - ISO 27005:2008 ISMS – Risikomanagement
  - ISO 27006:2007 Anforderungen an Zertifizierstellen

ISO 27001 („Zertifizierungs-ISO“)

- **Historie:**
  - die ISO 27001 ist aus dem British Standard BS 7799-2 (-2 steht für Teil 2) hervorgegangen
  - sie beinhaltet den normativen Teil für die Zertifizierbarkeit eines Informationssicherheit-Managementsystems
- **die aktuelle Version ISO 27001 wurde am 15. Oktober 2005 herausgegeben**
- **sie hat den Titel: „Information Security Management System - Requirements“**

ISO 27001 im Überblick

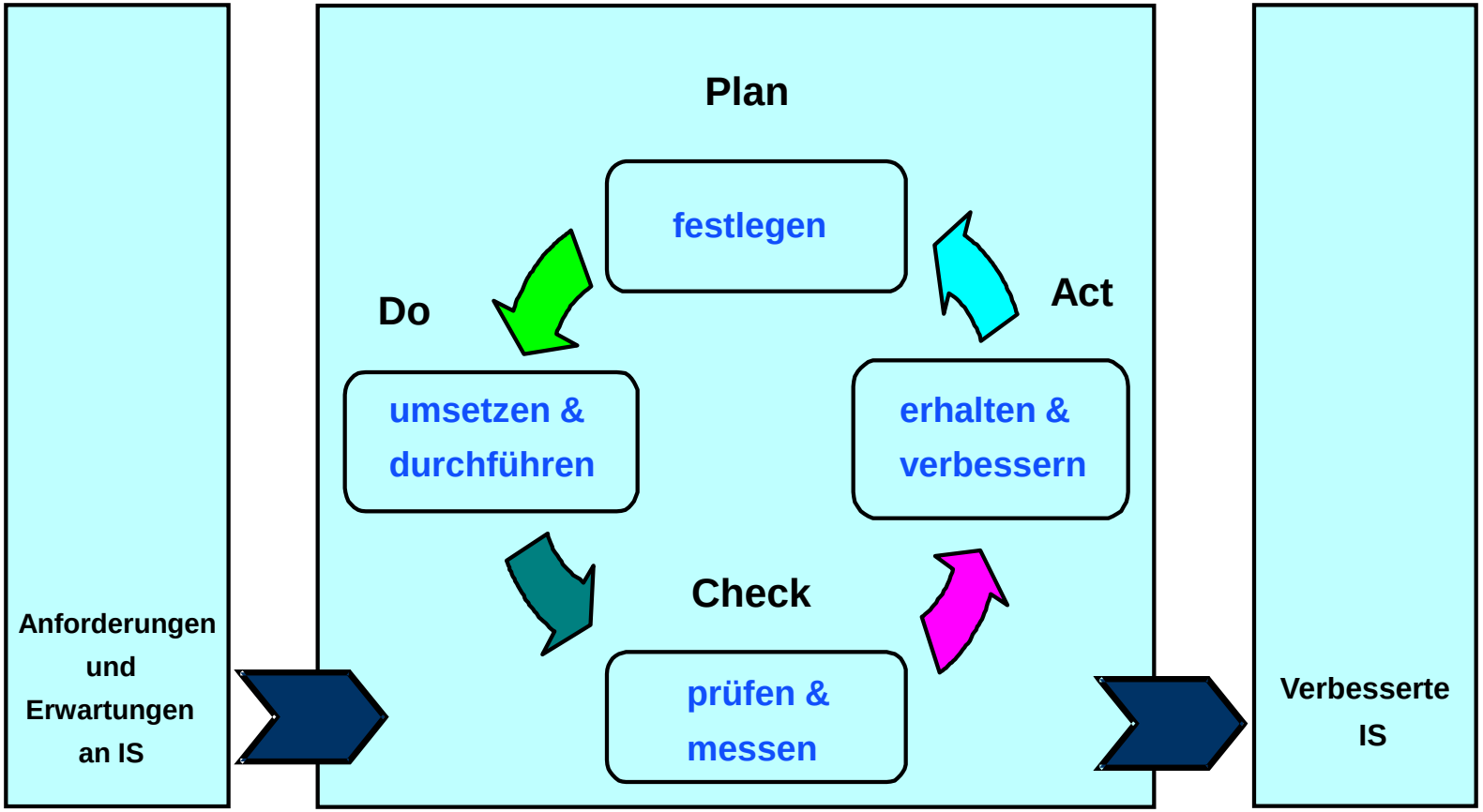
- **die in der ISO 27001 spezifizierten Anforderungen beschränken sich nicht nur auf die IT-Sicherheit als Technologie im engeren Sinne**
- **die formulierten Anforderungen zwingen die Akteure im Prozessgeschehen dazu, sich gleichwertig mit allen Aspekten der Informationssicherheit (IS) zu befassen**
- **die geforderte Einrichtung eines IS-Managementsystems (ISMS) verschafft anhand der Vorgabe eines kontinuierlichen Verbesserungsprozesses zahlreiche systemische Vorteile um die permanent gegebene Herausforderung bei der Informationssicherheit zu bewältigen**

ISO 27001 im Überblick

- **die ISO 27001 überprüft für eine Zertifizierung, ob die IS-relevanten Themengebiete aus der ISO 27002 behandelt sind und auch tatsächlich einem PDCA-Zyklus unterliegen:**
  - Sicherheitsleitlinie
  - Methodik und Durchführung des Risikomanagements
  - Umsetzung von Maßnahmen aus der Risikobetrachtung
  - Kontroll-, Bewertungs- und Reaktionsszenarien
  - IS-Organisation
  - Bewusstseinsbildung, Schulung
  - Ressourcenmanagement
  - Dokumentenmanagement
  - Sicherheitsvorfallmanagement
  - Notfallmanagement
  - etc.

Informationssicherheit PDCA-Zyklus

- **IS PDCA-Zyklus (kontinuierlicher Verbesserungsprozeß)**



ISO 27002 im Überblick

- **die ISO 27002 ist nach folgendem Schema aufgebaut:**
  - sie besteht aus einem 5-teiligen Prolog und 11 thematischen Bereichen („*security control clauses*“)
    - jeder Themenbereich umfaßt dabei Kategorien („*main security categories*“), die für ihn wichtige Themen formulieren (insg. 39 Kategorien über alle Bereiche hinweg)
      - für jede Kategorie werden definiert:
        - Sicherheitszielvorgaben („*security objectives*“)
        - Aufgaben/ Anforderungen („*security controls*“)
          - für die Anforderungen sind Umsetzungsvorschläge („*security implementation guides*“) zur Erfüllung der Zielvorgaben angegeben
- **die ISO 27002 umfasst insgesamt 133 Sicherheitsaufgaben („*security controls*“)**

ISO 27002 im Überblick

- **ein Prolog und elf Themenbereiche der ISO 27002**
  - **Prolog ohne Angabe von Aufgaben („*security controls*“) mit den fünf Abschnitten: „*Introduction*“, „*Scope*“, „*Terms and Definitions*“, „*Structure of This Standard*“ und „*Risk Assessment & Treatment*“**

1. **Weisungen und Richtlinien zur Informationssicherheit / „*Security Policy*“**
2. **Organisatorische Si-Maßnahmen und Managementprozess / „*Security Organization*“**
3. **Verantwortung und Klassifizierung von Informationswerten / „*Asset Classification and Control*“**
4. **Personelle Sicherheit / „*Human Resources Security*“**
5. **Physische und umgebungsbezogene Sicherheit / „*Physical and Environmental Security*“**

ISO 27002 im Überblick

6. **Netzwerk- und Betriebssicherheit (Daten und Telefonie) / *„Communications & Operations Management"***
7. **Zugriffskontrolle / *„Access Control"***
8. **Systembeschaffung, -entwicklung und -wartung / *„System Acquisition, Development & Maintenance"***
9. **Umgang mit Vorfällen bei der Informationssicherheit / *„Information Security Incident Management"***
10. **Sicherstellung des Geschäftsbetriebs – Notfallvorsorgeplanung / *„Business Continuity Management" (BCM)***
11. **Einhaltung von gesetzlichen & sonstigen Vorgaben - Audits / *„Compliance"***

ISO 27001 - Zertifizierung

- **welchen Nutzen bringt eine Zertifizierung?**
  - das Thema Informationssicherheit wird durch eine Zertifizierungs-entscheidung ein wichtiges Anliegen der Geschäftsführung
  - Chance der Organisation auf Verbesserung und Optimierung von Prozessen, nicht nur der IS-spezifischen (Mitnahmeeffekt)
  - deutlich gesteigertes Risikobewusstsein verankert in der Unternehmensleitung, aber auch bei den Mitarbeitern (Transparenz der Risiken)
  - eine günstige Gelegenheit Informationssicherheit ins Mitarbeiter-bewusstsein als Teil der Unternehmenskultur zu integrieren
  - Etablierung von Verbesserungs- und Präventionszyklen im Sicherheitsmanagementsystem (KVPs)
  - effizientere Umsetzung durch externen Druck (ein blamables Ergebnis zur Zertifizierung will unbedingt vermieden werden)
  - verstärkte Integration des Sicherheitsbewusstseins bei Geschäftspartnern
  - eine Möglichkeit sich gegenüber nicht-zertifizierten Mitbewerbern abzuheben

IT-Risikomanagement

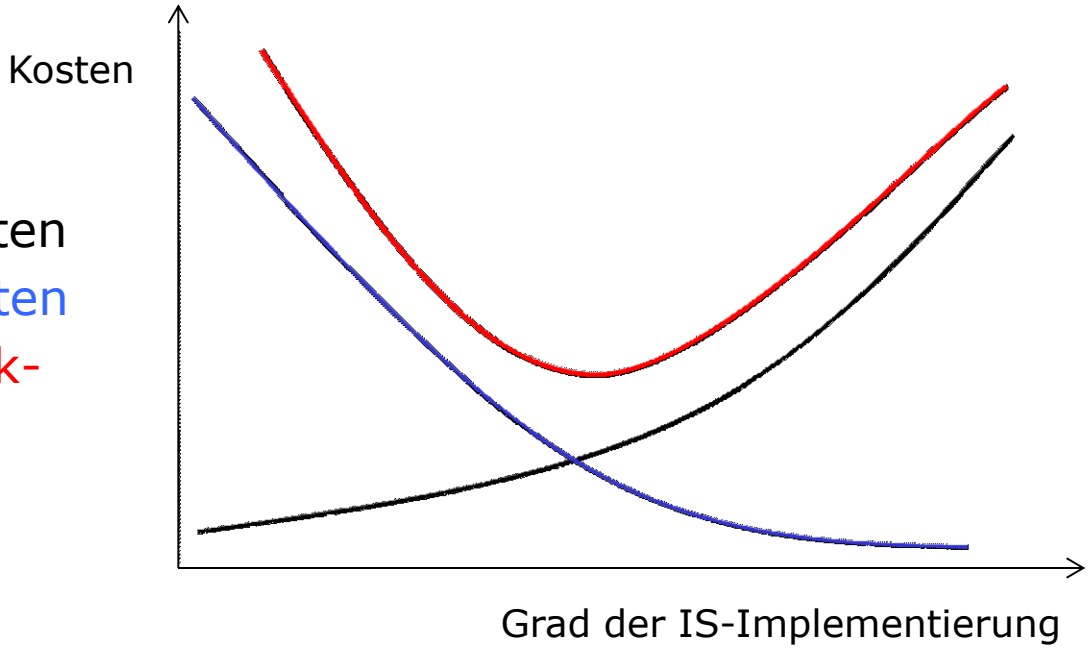
- **Begriffsdefinition „IT-Risikoanalyse“**
  - Analyse von Gefährdungen, Bedrohungen & Schwachstellen
    - und -
    deren Schadensauswirkungen bei Informationen und Geräten zur Informationsverarbeitung
    - und –
    die Wahrscheinlichkeit des Auftretens dieser Risiken

- **Begriffsdefinition „IT-Risikomanagement“**
  - Prozess der *kostenmäßig* vertretbaren Identifizierung, Beschränkung und Minimierung bzw. Elimination von Sicherheitsrisiken, die Informationen und Informations-systeme beeinträchtigen können

IT-Risikomanagement

- **zentrale Aufgabe des IT-Risikomanagements**
  - optimieren der Begegnung von Risiken durch Ausbalancierung von Schadenskosten versus Vorbeugekosten:

- Vorbeugekosten
- Schadenskosten
- Risikenabdeck-kosten



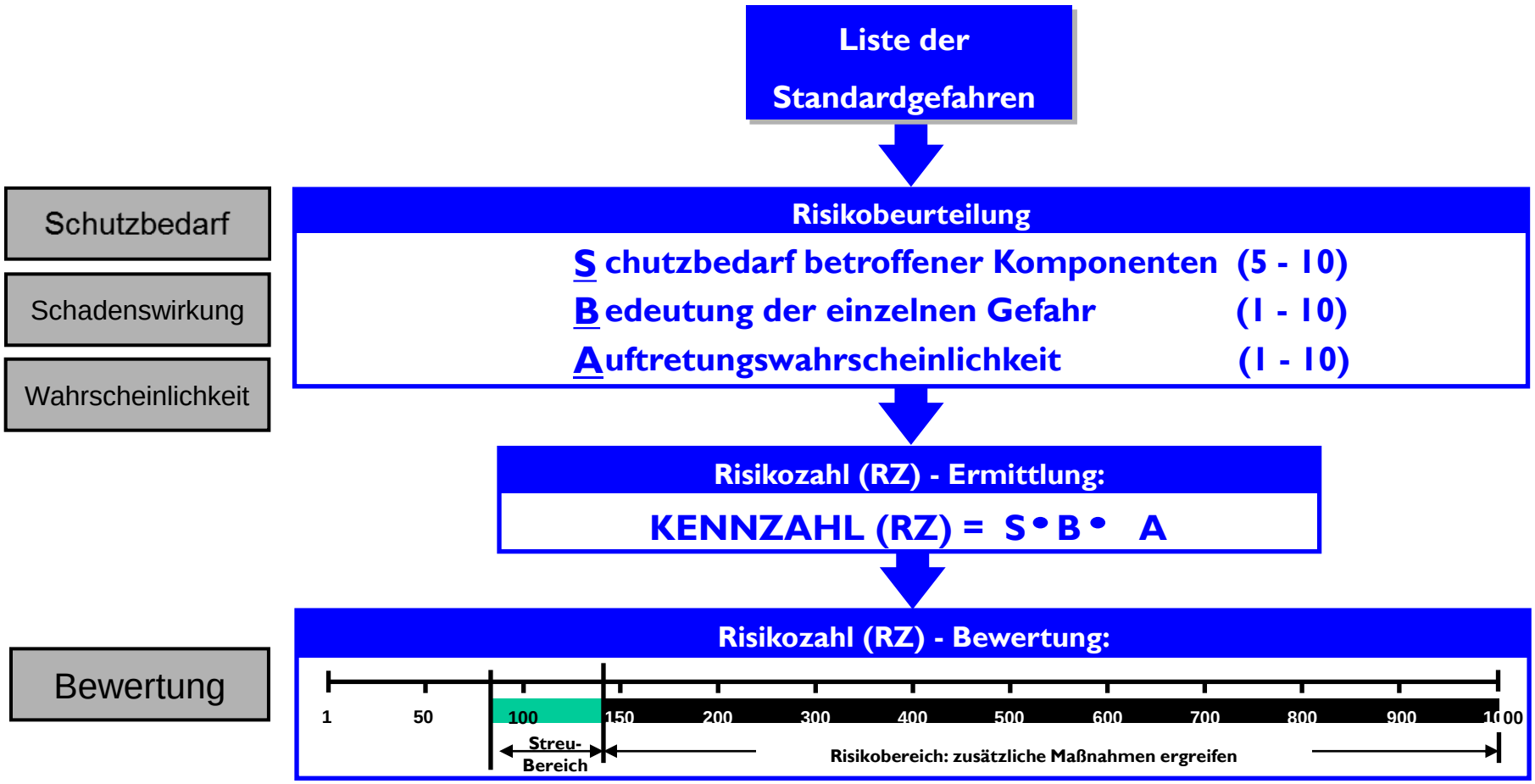
IT-Risikomanagement Prozess
Teilaktivität Risikoanalyse

- **die Risikoanalyse besteht in der systematischen Betrachtung der Punkte:**
  - Schaden für das Geschäft, der unter Berücksichtigung der potentiellen Folgen des Verlusts von
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - Authentizität

    der Informationen und anderer Werte möglicherweise durch einen Sicherheitsausfall (Gefährdungen) entstehen kann
  - realistische Wahrscheinlichkeit, dass ein derartiger Ausfall angesichts der existierenden Bedrohungen und Schwachstellen und der derzeit implementierten Maßnahmen auftritt

IT-Risikomanagement Prozess
Teilaktivität Risikobewertung

- **metrisierte Risikobewertung:**



IT-Risikomanagement Prozess
Teilaktivität Behandlungsmanagement

- **Optionen für die Behandlung von Risiken sind:**
  - Risiko-Vermeidung durch Umstrukturierung von Geschäftsprozessen oder des IT-Verbunds (z.B. durch Vermindern der Komplexität)
  - Risiko-Reduktion durch weitere Sicherheitsmaßnahmen
  - Risiko-Transfer auf eine andere Institution (z.B. durch Abschluß einer Versicherung oder Outsourcing)
  - die verbleibende Gefährdung und damit das daraus resultierende Risiko wird akzeptiert (Risiko-Übernahme)

- **die getroffenen Behandlungsentscheidungen werden im Risikomanagement-Plan dokumentiert**

- **mit dieser Art von Risikomanagement-Plan werden die Risiken transparent gemacht!**

Web-Adressen zu IT-Sicherheit

- **empfehlenswerte Links zum Thema IT-Sicherheit**
  - http://www.bsi.bund.de/grundschutz (BSI IT-Grundschutz)
  - http://www.heise.de/security (News, Basischecks)
  - http://www.sicher-im-netz.de (Fundgrube für KMUs)

bedankt sich für Ihre Aufmerksamkeit
und wünscht Ihnen weiterhin viel Erfolg für Ihre IT-Sicherheit!

www.holliday-consulting.com