> Informationssicherheit

risikoorientiert – betriebsgerecht

Saarbrücken
14. März 2017

> Zur Person

Andreas J. Henke

- Jahrgang 1965 – verheiratet – 3 Kinder
- Dipl. Wirtsch.-Ing.
- Seit 1993 tätig im Bereich Unternehmens- und Managementberatung
- Seit 1997 im Lufthansa Konzern
- Konzeption und Aufbau diverser Managementsysteme
- Beratung in internationalen Projekten
- Lead Auditor ISO/IEC 27001, ITIL V3 Foundation, Foresight Professional
- Senior Manager Information Protection & Business Risk Management

> Agenda

- Motivation
- Informationssicherheit einführen
- Risikoorientierter Ansatz
- Betriebsorientierter Ansatz
- Zusammenfassung und Fazit

Top 10 Geschäftsrisiken

Die 10 wichtigsten globalen Geschäftsrisiken 2017

[Quelle: Allianz Global Corporate & Specialty | Fotos: iSTock Photos]

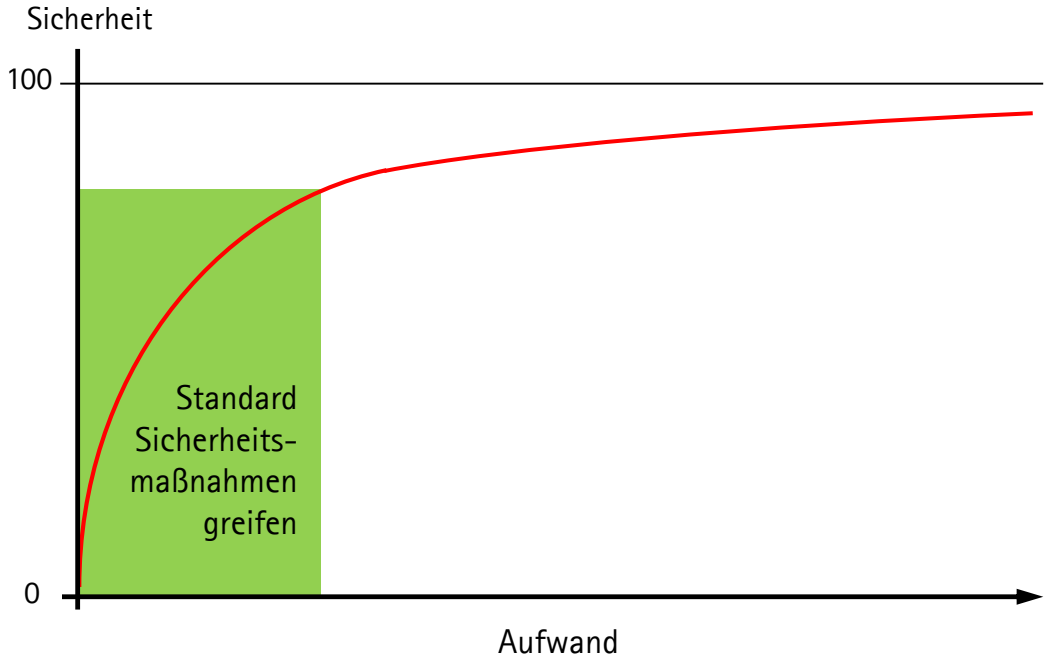
| https://www.risknet.de/themen/risknews/was-sind-die-unternehmensrisiken-2017/03358cda1995f00a2d7ca42f70fd0a81/

Sicht des BSI

- **„Permanent finden in Deutschland Cyber-Attacken statt, die die Leistungsfähigkeit des Standortes massiv beeinträchtigen können**. Die Art der Angriffe stellt sich dabei sehr unterschiedlich dar und es lassen sich Massenangriffe, gezielte sowie skalpellartige Angriffe verzeichnen. Informationstechnik, insbesondere Software, ist aufgrund ihrer Komplexität nicht fehlerlos. Schwachstellen und Verwundbarkeiten gehören daher zur Tagesordnung, auch solche, die aufgrund der Vernetzung der IT-Systeme aus der Ferne ausgenutzt werden können.
- Die **zunehmende Professionalisierung** von Angreifern und Angriffsmethoden führt zudem zu einer dynamischen Gefährdungslage und zu einem permanenten Wettlauf zwischen Cyber-Angriffen und Cyber-Abwehr.
- **Doch es gibt auch gute Nachrichten: Rund 80 Prozent der bekannten Angriffe lassen sich mit Standard-Schutzmaßnahmen abwehren, beispielsweise im Rahmen von IT-Grundschutz.“**

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Allgemeines/Vorwort/vorwort_node.html

Kostenverlauf in der Informationssicherheit



- Hundertprozentige Sicherheit ist auch mit noch so hohem Aufwand nicht zu erreichen
- Mit überschaubarem Aufwand kann jedoch ein Großteil der Angriffe abgewehrt werden

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Fokus_IT-Sicherheit_2013_nbf.pdf?__blob=publicationFile

> Informationssicherheit einführen

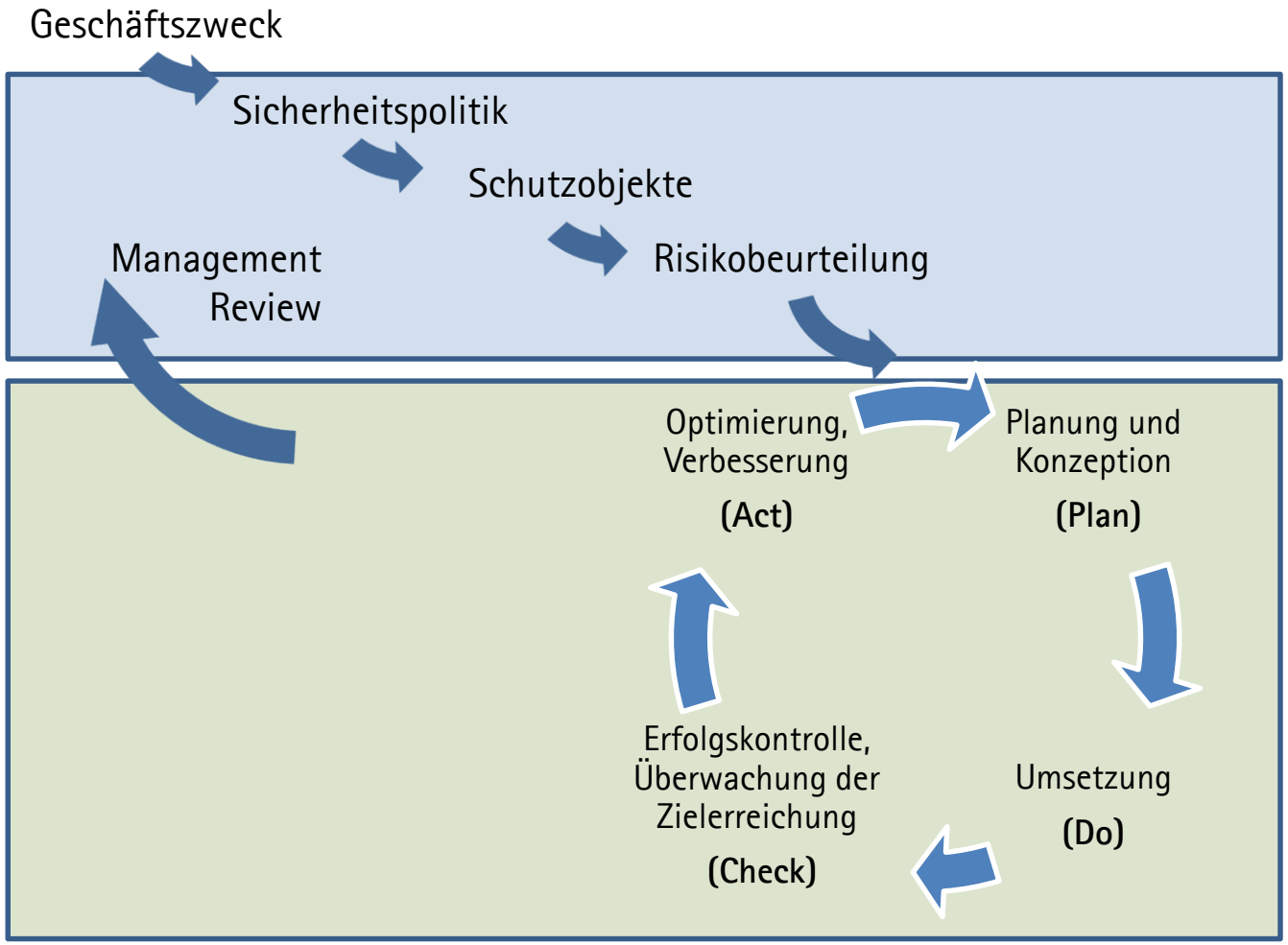
Die Kernaussage in Kürze:

- ➔ Kenne Dein Geschäft
- ➔ Kenne Deine Risiken
- ➔ Handle angemessen danach

InfoSec einführen ist kein Projekt – es ist ein Prozess

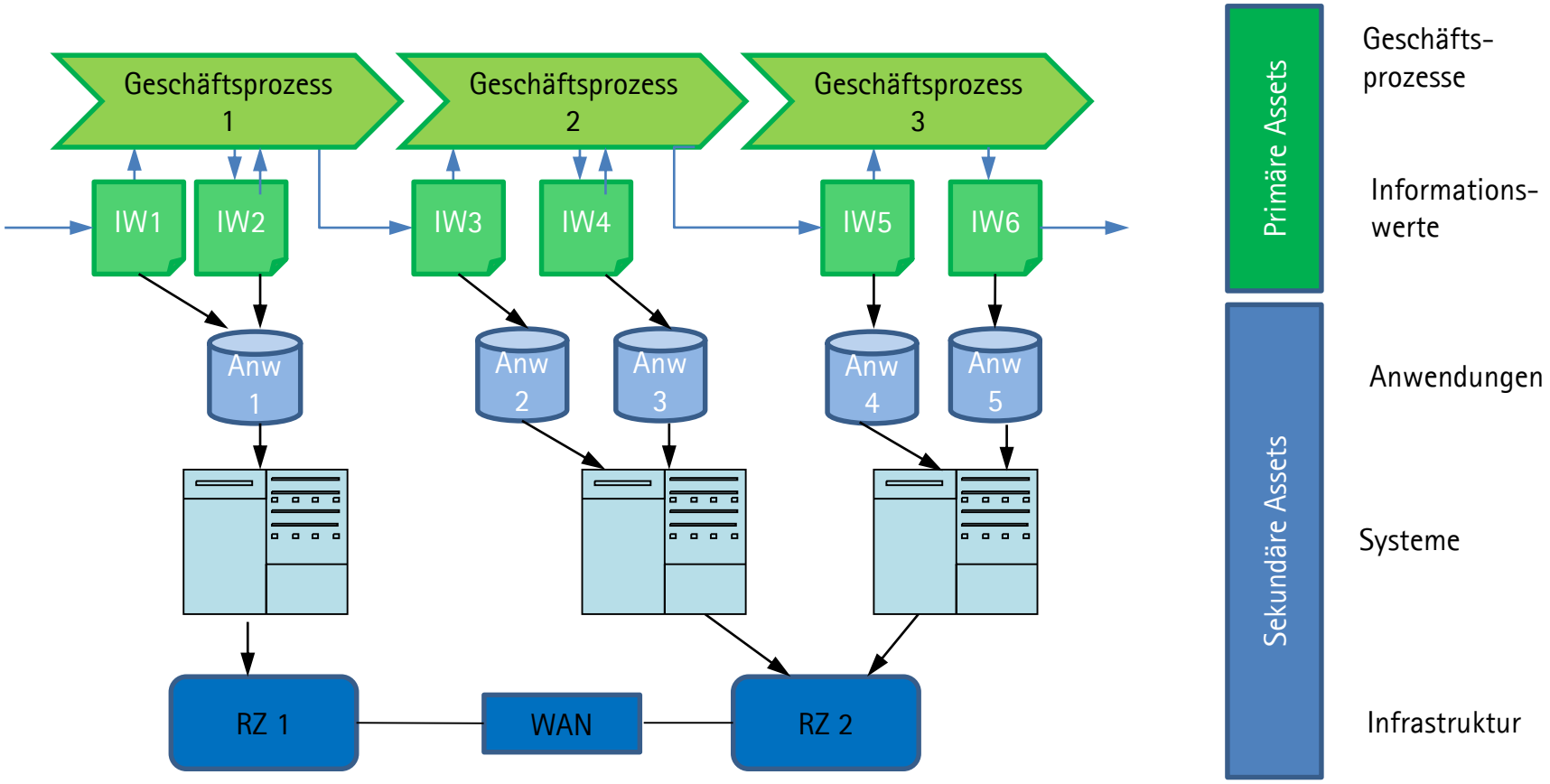
➔Vergleichen Sie es mit Rasenmähen

Der Sicherheitsprozess



Schutzobjekte definieren

Wie sind die essentiellen Prozesse in der IT abgebildet?

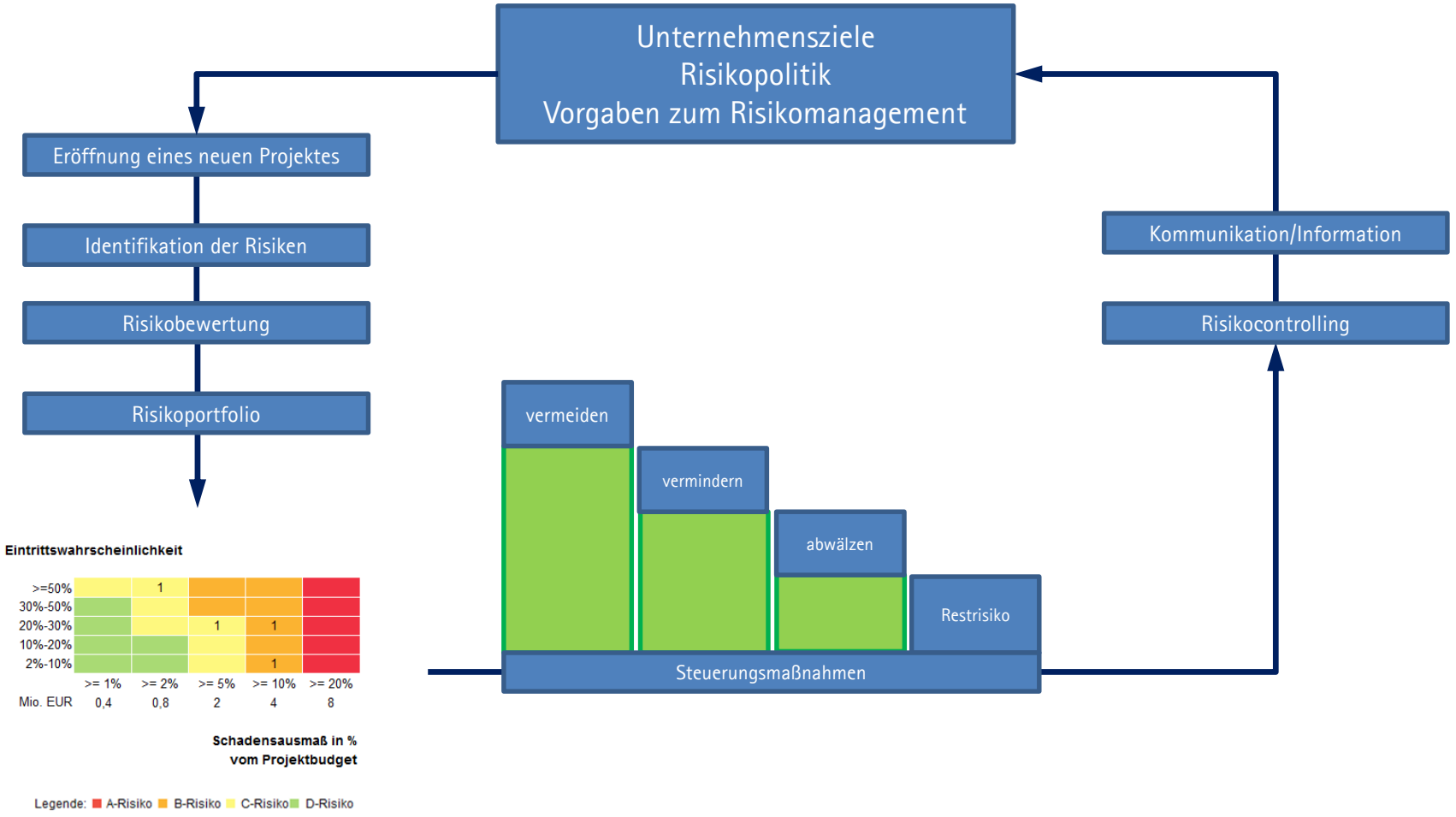


Schutzobjekte definieren – was soll geschützt werden?

Klassifizierung	Gefahrenpotenzial	Erläuterung	Beispiele*
Öffentlich	Informationen, deren Bekanntwerden kein oder ein sehr geringes Risiko darstellt.	Hierbei handelt sich um Informationen, über die alle Mitarbeiter verfügen, die aber ebenfalls gezielt der Öffentlichkeit zur Verfügung gestellt werden.	Produktkataloge, Jahresberichte, Broschüren, Pressemeldungen
Intern	Informationen, deren Bekanntwerden dem Unternehmen Schaden in geringem Umfang zufügen kann.	Über solche Informationen verfügen alle Mitarbeiter des Konzerns.	Geschäftliche Kontaktdaten und Telefonbuch, Organigramme
Vertraulich	Informationen, deren Bekanntwerden dem Unternehmen größeren Schaden zufügen kann bzw. mit Bußgeldern (z.B. aus dem EU-DSGVO) belegt werden kann oder die gesetzlich so klassifiziert werden müssen.	Solche Informationen sind auf Mitarbeiter einer bestimmten Abteilung, eines Bereichs, einer Projekt- oder Arbeitsgruppe, etc. begrenzt.	Unveröffentlichte Geschäftszahlen, vertrauliche Vorlagen und Protokolle, Geschäftsfeldplanung, Personenbezogene Daten, z.B. Personaldaten, Kundendaten, einzelne Kreditkartennummern
Streng Vertraulich	Informationen, deren Bekanntwerden dem Unternehmen erheblichen Schaden zufügen kann bzw. mit Bußgeldern (z.B.aus der EU-DSGVO) belegt werden kann oder die gesetzlich so klassifiziert werden müssen.	Über solche Informationen verfügt i. d. R. eine geschlossene Gruppe und oder die Geschäftsleitung.	Sicherheitsrelevante Informationen, Strategieplanung, Neuentwicklungen i.S. von Erfindungen/Patenten etc., Revisionsberichte, besonders sensible personenbezogene Daten, z.B. Informationen über Religion, medizinische Daten sowie Kombination mehrerer Daten, die eine Profilbildung ermöglichen, Kreditkartendaten

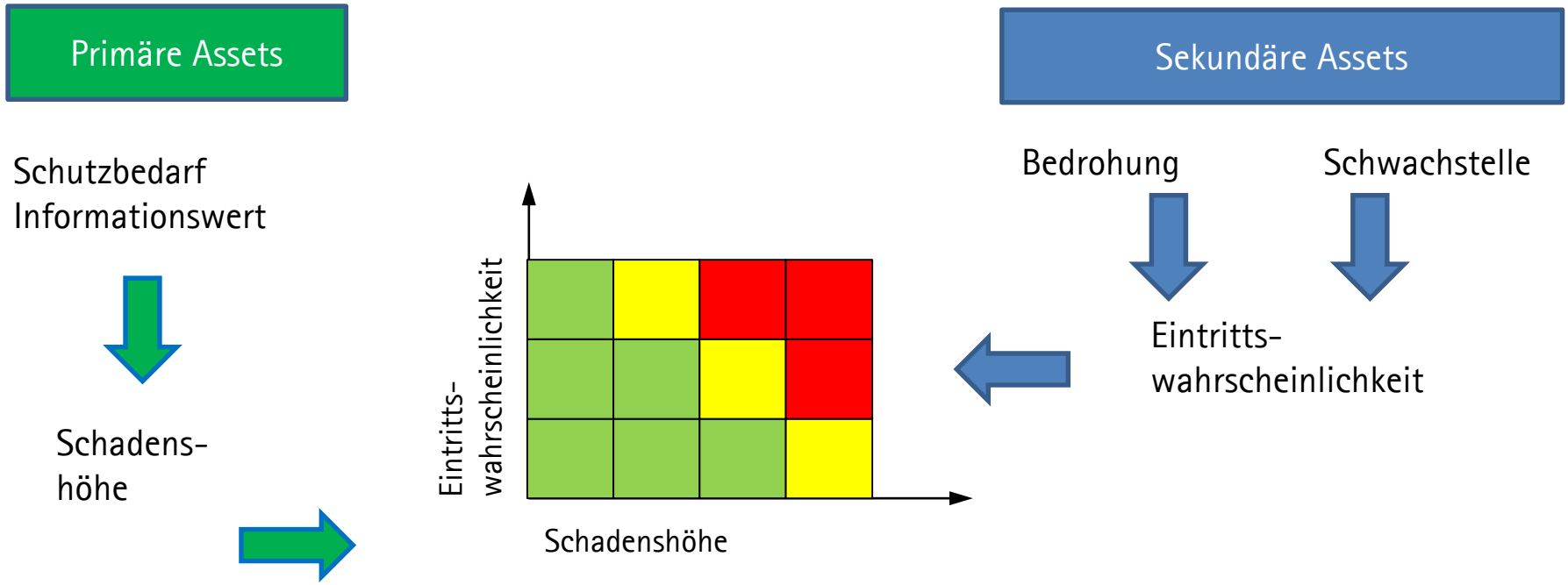
* Abhängig vom Inhalt der Daten, können die Beispiele in ihrer Klassifikation variieren.

Risikobeurteilung - Risikomanagement Prozess

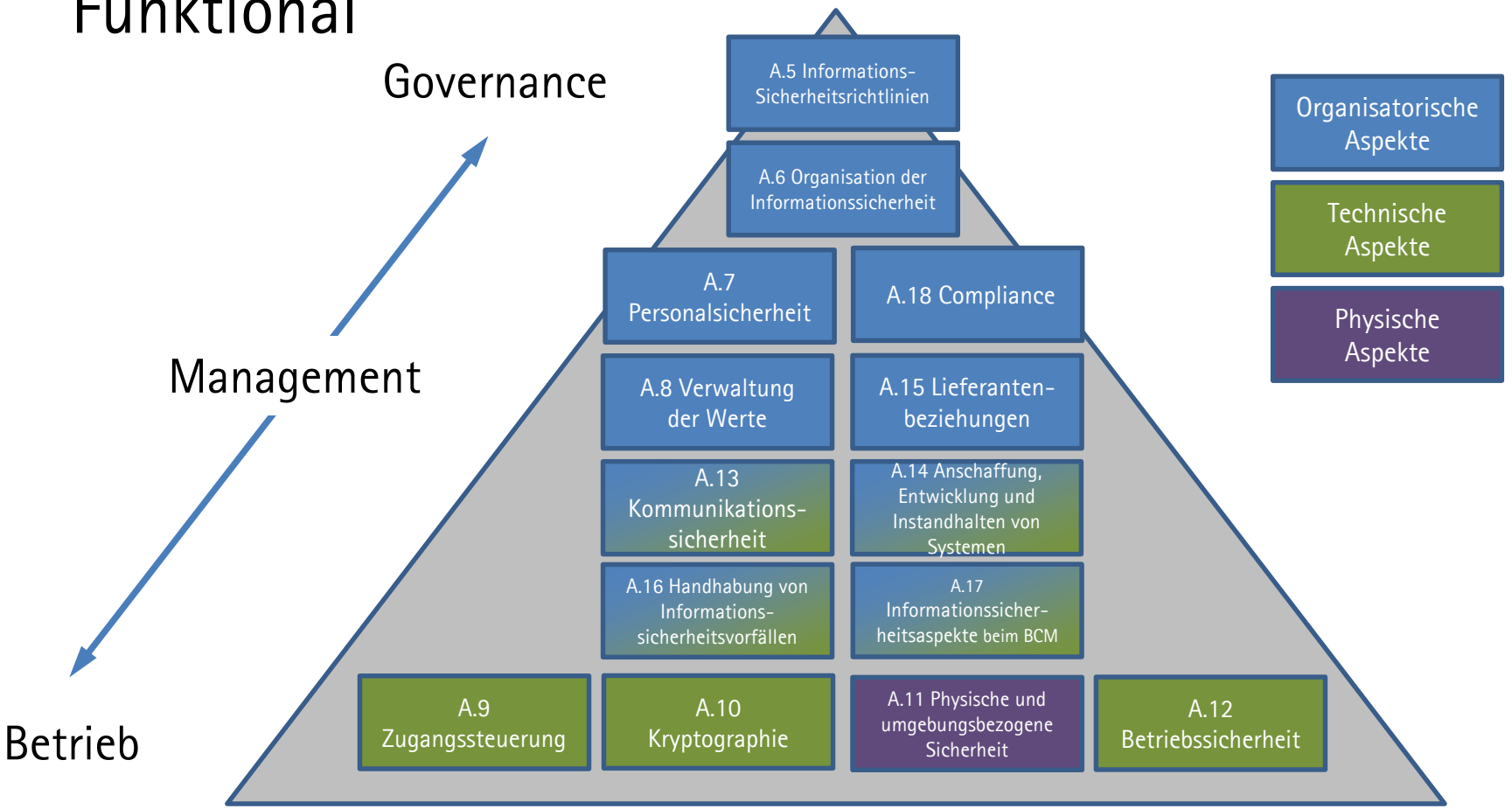


Risikobeurteilung

Risiken identifizieren und analysieren

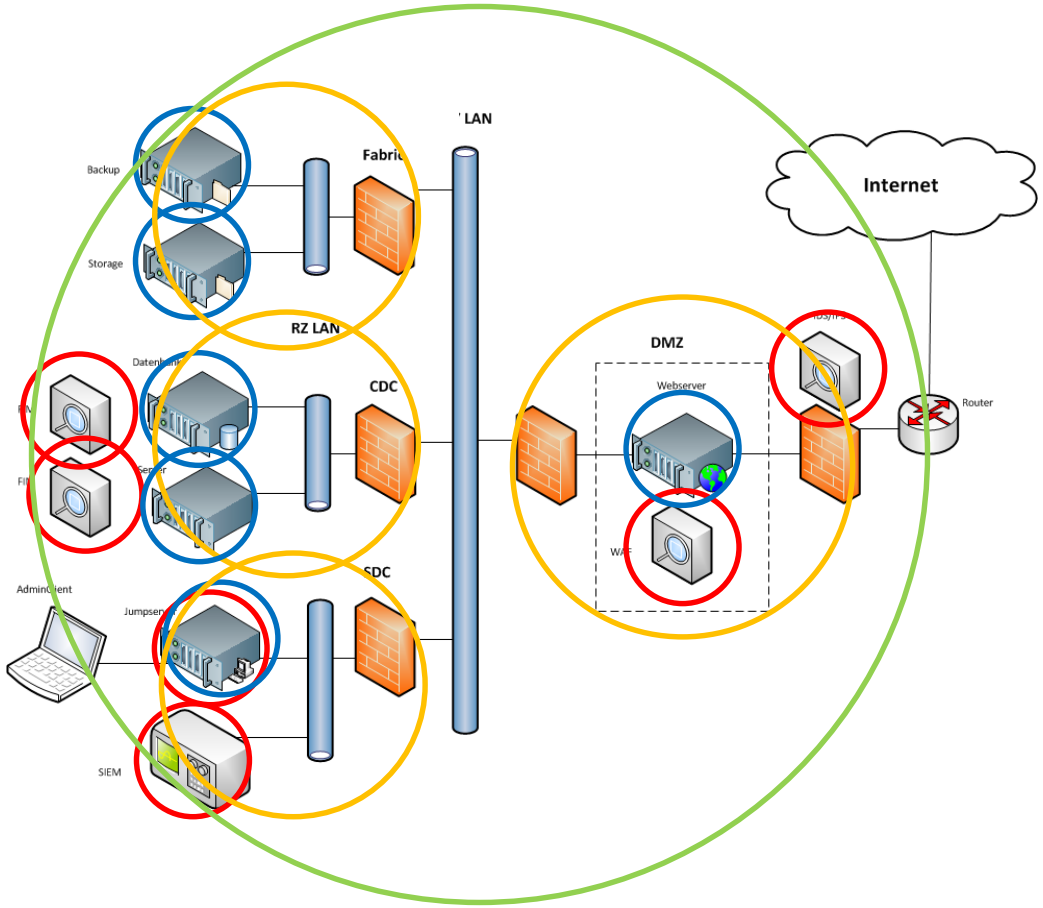


ISO/IEC 27001:2015 Maßnahmen Annex A - Funktional



Eigene Graphik

Ansatzpunkte der Maßnahmen



Schutzziele bei Vertraulichkeit, (Verfügbarkeit) und Integrität werden nur durch **abgestimmte Maßnahmen im gesamten System erreicht**

- Härtung
- Zusätzliche Sicherheitsdevices
- Netzwerk-segmentierung
- Gesonderte Betriebs-, Review und Prüfprozesse

Differenzierung unterschiedlicher Schutzstufen

	normal	hoch	sehr hoch	PCI
Härtung h-sh-PCI		x	x	x
Administrationsprozesse h-sh-PCI		x	x	x
Einsatz von Verschlüsselungstechnologien		x	x	x
Physische Sicherheit	x	x	x	x
Zentrale Protokollierung (SIEM)		x	x	x
File Integrity Monitoring (FIM)		x	x	x
Netzwerk Sicherheitsdevices (IPS, IDS, HIPS, NIPS)		x	x	x
Virenschutz	x	x	x	x
Jump Server zur Administration	x	x	x	x
Netzwerksegmentierung		x	x	x
Netzwerk, Infrastruktur absichern	x	x	x	x
CERT Rufbereitschaft				x
Externe Compliance Audits				x
Technische Audits (Schwachstellenscans)		x	x	x
Regelreview der Firewall		x	x	xx
Schwachstellen Informationsdienst	x	x	x	x
Patch Management	x	x	x	x
Monitoring	x	x	x	x
Service Management Prozesse	x	x	x	x
Organisation des Informationssicherheits-Managements	x	x	x	x

Kriterien für betriebsgerechte Informationssicherheit

- Erkennen Sie Ihre kritischen Geschäftsprozesse
- Definieren Sie nicht zu viele Schutzstufen
- Fassen Sie gleichartigen Schutzbedarf zusammen, segmentieren Sie diese Systeme
- Sichern Sie diese angemessen ab: Sorgfältiger Umgang mit „Kronjuwelen“ – 80% Lösung für den Rest
- Augenmerk auf nichttechnische (Organisatorische) Maßnahmen: z.B. berechtigen Sie Mitarbeiter ausschließlich für notwendige Funktionen

> Vielen Dank für die Aufmerksamkeit!

Andreas J. Henke

- Gerne stehe ich für Ihre Fragen zur Verfügung.
- Bitte kommen Sie vertrauensvoll über Herrn Hallfell – enbiz - auf mich zu (Folgefolie).

Kontaktdaten

Frank Hallfell

hallfell@enbiz.de

0631 3106840