PERSICON

ALTERNATIVE ANSÄTZE IM SICHERHEITSMANAGEMENT

Knut Haufe

- Diplom-Wirtschaftsinformatiker
- Master in Commercial Law (LL.M.)

- Mitautor BSI IT-Grundschutzhandbuch/BSI IT-Grundschutzkataloge
- Zertifizierter ISO 27001 Auditor/Auditteamleiter (TÜV und BSI)
- Zertifizierter IS-Revisions- und IS-Beratungsexperte (BSI IS-Revisor)

- Certified Information System Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise Information Technology (CGEIT)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information System Security Professional (CISSP)
- Geprüfter Datenschutzbeauftragter (SGS TÜV)
- EuroPriSe Technical and Legal Expert (ULD)
- Project Management Professional (PMP)

- Kontakt: khaufe@persicon.com

PERSICON

- Spezialist für IT-Sicherheit und Datenschutz
- Besondere Expertise im BSI IT-Grundschutz
  - Mitgestaltung BSI IT-Grundschutz und ISO 27001
  - Ausbilder der BSI Auditoren
- 60 Mitarbeiter
- Hauptsitz: Friedrichstraße 100, 10117 Berlin, weitere Büros in Düsseldorf und Kiel

Staatlich akkreditierte Zertifizierungs- und Sachverständige Prüfstelle für Datenschutz und IT-Sicherheit

Anerkennung als sachverständige Prüfstelle

Datenschutz-Gütesiegel Schleswig-Holstein

Beim ULD anerkannte sachverständige Prüfstelle für IT-Produkte (rechtlich / technisch)

Die

PERSICON cert AG

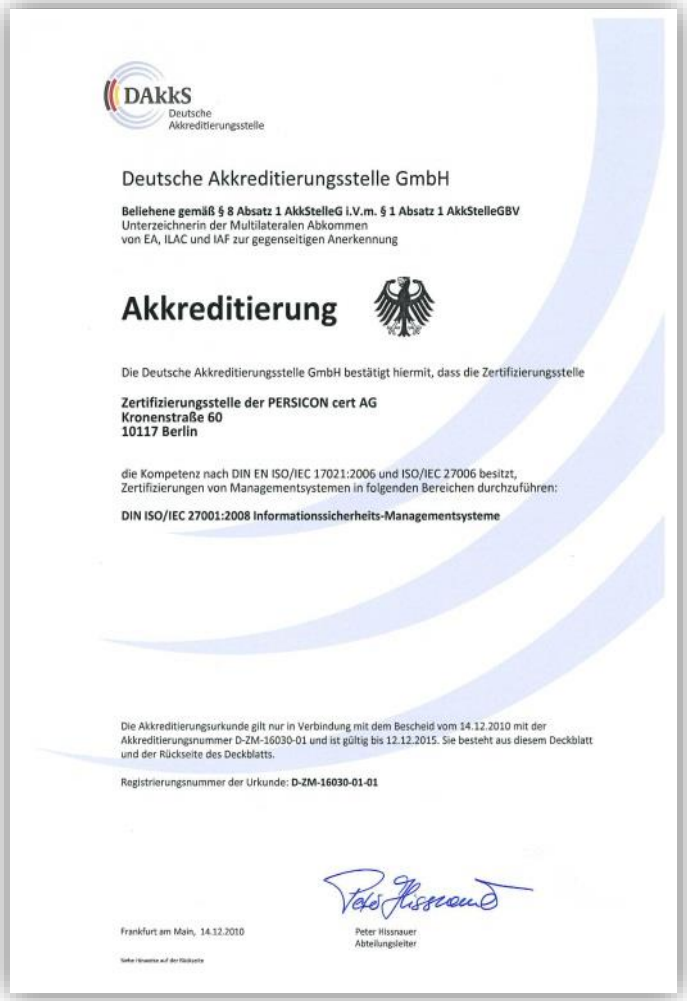
wurde am 23. Juni 2011 vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein als sachverständige Prüfstelle gemäß § 4 Abs. 2 LDSG SH i. V. m. § 3 Abs. 1 der Datenschutzauditverordnung (DSAVO) vom 18. November 2009 für die Bereiche Recht und Technik anerkannt. Aufgrund der Anerkennung ist sie berechtigt, bei ihrer gutachterlichen Tätigkeit die Bezeichnung

„Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte sachverständige Prüfstelle für IT-Produkte (rechtlich/technisch)"

zu führen.

Weitere Informationen unter www.datenschutzzentrum.de/guetesiegel/

Dr. Thilo Weichert



DAkkS Deutsche Akkreditierungsstelle

Deutsche Akkreditierungsstelle GmbH

Beliehene gemäß § 8 Absatz 1 AkkStelleG i.V.m. § 1 Absatz 1 AkkStelleGBV
Unterzeichnerin der Multilateralen Abkommen
von EA, ILAC und IAF zur gegenseitigen Anerkennung

Akkreditierung

Die Deutsche Akkreditierungsstelle GmbH bestätigt hiermit, dass die Zertifizierungsstelle

Zertifizierungsstelle der PERSICON cert AG
Kronenstraße 60
10117 Berlin

die Kompetenz nach DIN EN ISO/IEC 17021:2006 und ISO/IEC 27006 besitzt, Zertifizierungen von Managementsystemen in folgenden Bereichen durchzuführen:

DIN ISO/IEC 27001:2008 Informationssicherheits-Managementsysteme

Die Akkreditierungsurkunde gilt nur in Verbindung mit dem Bescheid vom 14.12.2010 mit der Akkreditierungsnummer D-ZM-16030-01 und ist gültig bis 12.12.2015. Sie besteht aus diesem Deckblatt und der Rückseite des Deckblatts.

Registrierungsnummer der Urkunde: **D-ZM-16030-01-01**

Frankfurt am Main, 14.12.2010

Peter Hissnauer
Abteilungsleiter

PERSICON

Referenzen (Auszug)

Öffentlicher und Nicht-öffentlicher Sektor

- Bundesministerium der Finanzen
- Bundesministerium des Inneren
- Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
- Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben
- Wasser- und Schifffahrtsverwaltung des Bundes
- Deutsche Post, Deutsche Telekom, Versatel
- HOCHTIEF, Pfizer
- E.ON, RWE, diverse Stadtwerke
- Bertelsmann, arvato
- Rolls Royce, MAN Nutzfahrzeuge
- Talanx Versicherungsgruppe/HDI Gerling
- Microsoft, IBM, Nokia, Sennheiser

Bundesamt für Sicherheit in der Informationstechnik (BSI)

PERSICON unterstützt das BSI seit Jahren konstant bei der Weiterentwicklung von Sicherheitsstandards und Softwarelösungen. Unter anderem zählen hierzu folgende Projekte:

- Strategiekonzept für die Weiterentwicklung der IT-Sicherheitsprodukte des BSI,
- Ausbildung der BSI-Auditoren (Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz" und IS-Revisoren),
- Erstellung des Bausteins „Windows Server 2003” für die BSI IT-Grundschutz-Kataloge und
- Erstellung des Bausteins „Client unter Windows 7” für die BSI IT-Grundschutz-Kataloge.

Bundesamt für Sicherheit in der Informationstechnik

PERSICON

Informationssicherheitmanagement

BSI IT-Grundschutz

PERSICON

BSI IT-Grundschutz (1)

- Verpflichtende Anwendung gemäß UPBund
- Nationaler Standard für Informationssicherheitsmanagement mit „weitgehender“ Kompatibilität zur internationalen Norm ISO 27001
- Herausgeber ist das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Nachschlagewerk und Vorgehensmodell

- *Kontrollziele:*
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit

- Zertifizierungsfähig, Zertifizierungsstelle ist das BSI


Bundesamt für Sicherheit in der Informationstechnik

Lizenzierung

Die Bundesrepublik Deutschland
vertreten durch das Bundesministerium des Innern
dieses vertreten durch den Präsidenten des
Bundesamtes für Sicherheit in der Informationstechnik
bestätigt hiermit, dass

Knut Haufe
Weichbergerstr. 34, 99425 Weimar
PERSICON Information Risk Management GmbH
Friedrichstr. 188, 10117 Berlin

die Kompetenz besitzt und befugt ist,
Audits nach
ISO 27001 auf der Basis von IT-Grundschutz
durchzuführen. Er ist berechtigt, den Titel
Lizenzierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz
zu führen.

Die Gültigkeit dieser Lizenz beginnt am 29.05.2008 und endet am 29.05.2013.
BSI-Registriernummer: BSI-IGL-0180-2008

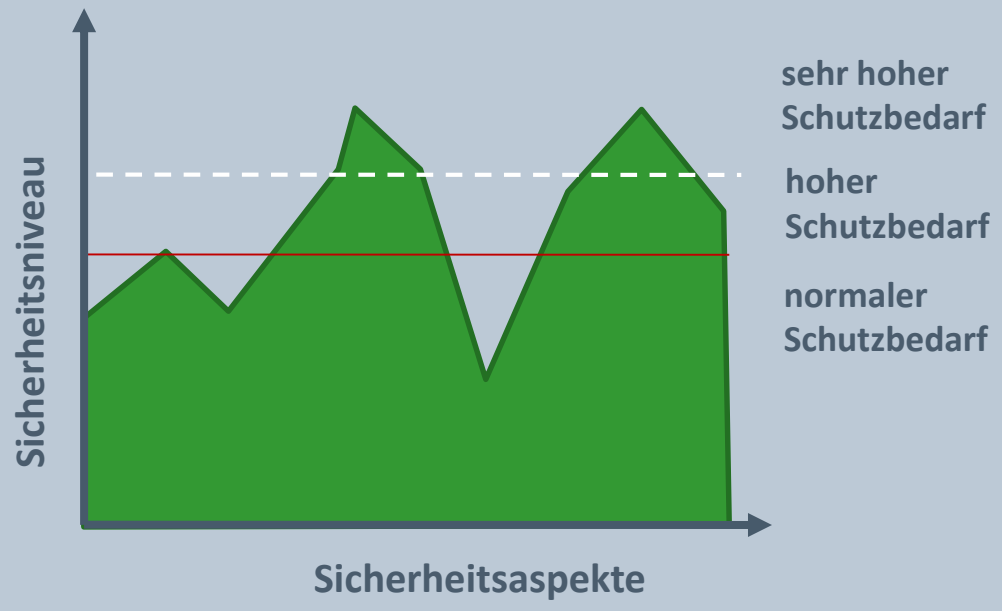
Bonn, den 29.05.2008
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag
Bernd Kowalski
Abteilungspräsident

PERSICON

BSI IT-Grundschutz (2)

- Standardsicherheitsmaßnahmen für typische IT-Umgebungen
- Personelle, technische, organisatorische und infrastrukturelle Aspekte
- Initialer Verzicht auf eine detaillierte Risikoanalyse
- Risikoanalyse für Objekte für Objekte mit Schutzbedarf „normal“ nicht notwendig, da bereits vom BSI vorgenommen und von Maßnahmen abgedeckt

- *Drei Schutzbedarfskategorien:*
  1. normal
  2. hoch
  3. sehr hoch



PERSICON

Struktur und Anwendung der BSI-Standards

BSI-Standards zur Informationssicherheit Bereich „Informationssicherheitsmanagement“

BSI Standard 100-1
ISMS: Managementsysteme für Informationssicherheit

BSI Standard 100-2
IT-Grundschutz-Vorgehensweise

BSI Standard 100-3
Risikoanalyse auf der Basis von BSI IT-Grundschutz

BSI Standard 100-4
Notfallmanagement

Zertifizierung nach ISO 27001 auf der Basis von BSI IT-Grundschutz, Prüfschema für ISO 27001-Audits

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

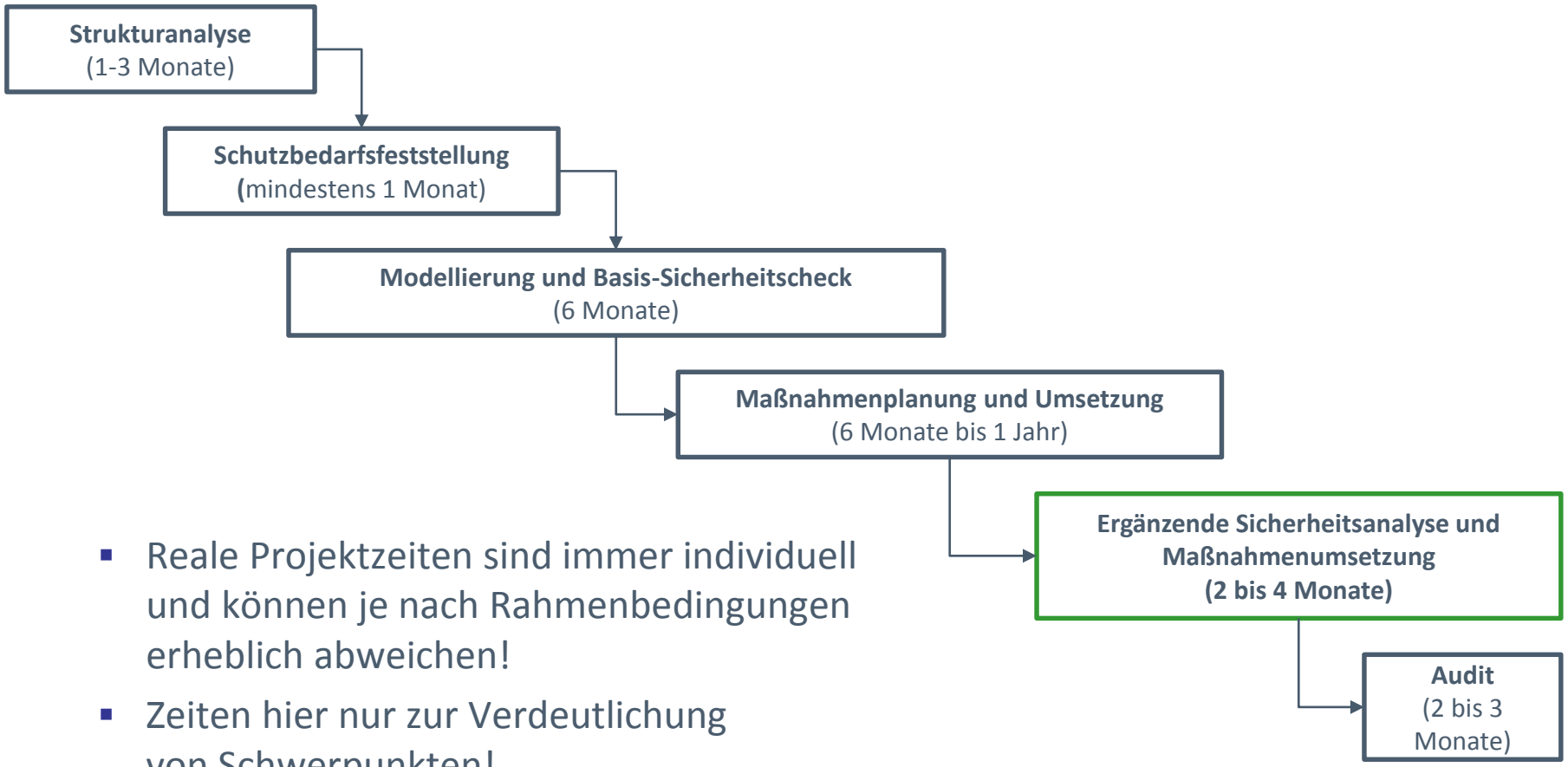
Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

- **Bausteine-Kataloge**
  - **Kapitel B1:** Übergreifende Aspekte
  - **Kapitel B2:** Infrastruktur
  - **Kapitel B3:** IT-Systeme
  - **Kapitel B4:** Netze
  - **Kapitel B5:** IT-Anwendungen
- **Gefährdungskataloge**
- **Maßnahmenkataloge**

Erstellung eines Sicherheitskonzeptes nach BSI IT-Grundschutz – zeitliche Planung



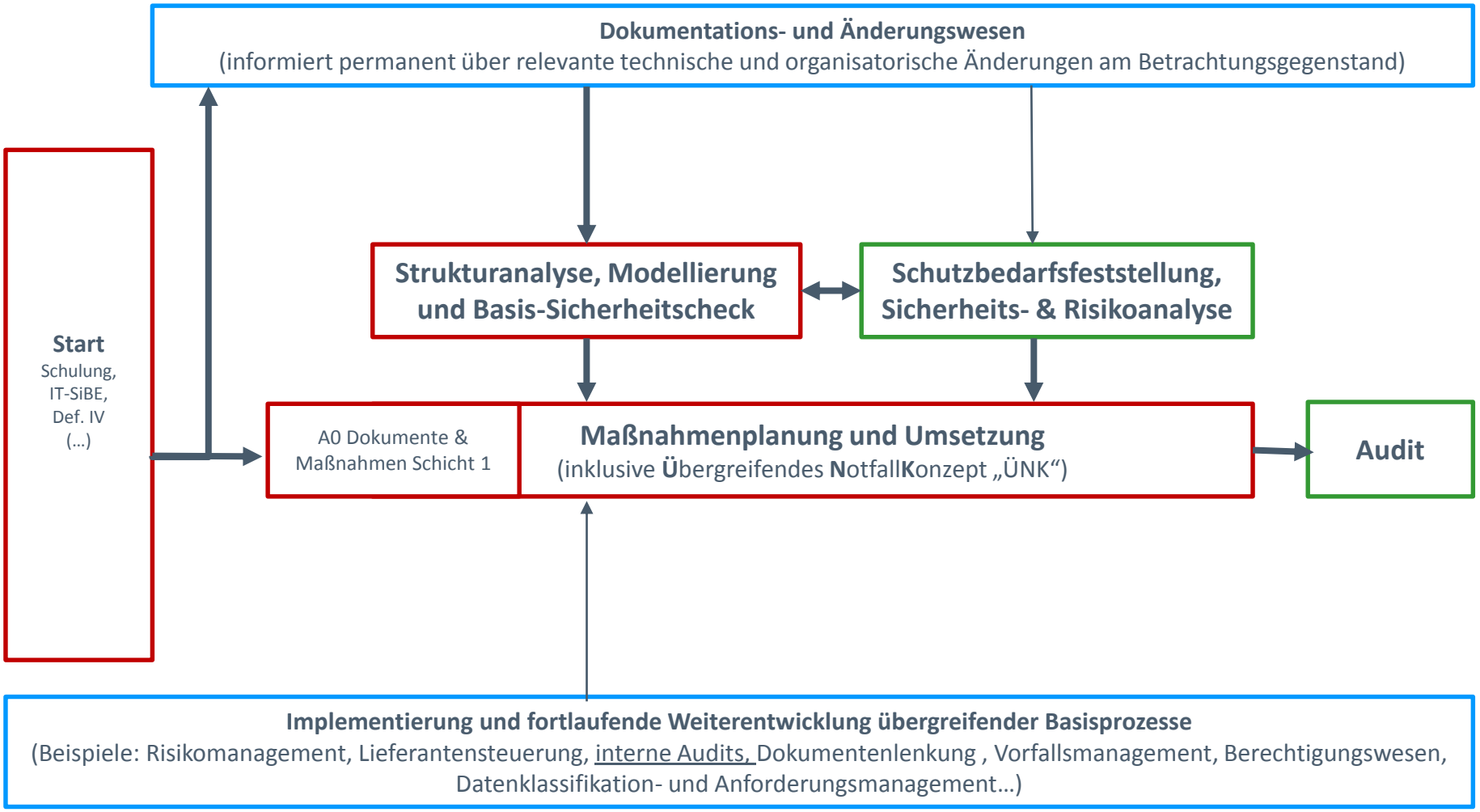
- Reale Projektzeiten sind immer individuell und können je nach Rahmenbedingungen erheblich abweichen!
- Zeiten hier nur zur Verdeutlichung von Schwerpunkten!

PERSICON

Praktische Erfahrungen, typische Schwierigkeiten sowie häufige Probleme

- Hoher Analyse-Aufwand und zeitlicher Vorlauf bis erste konkrete Maßnahmen umgesetzt werden
- Hoher Dokumentationsaufwand
- Unzureichende Anpassung der Maßnahmen an individuelle Rahmenbedingungen und Anforderungen
- Risikoakzeptanz ist unbekannt
- Umfang der Grundschutzkataloge
- Redundanzen und zu hohes Sicherheitsniveau
- ISMS steuert die Umsetzung aller Maßnahmen beziehungsweise setzt selbst um
- Maßnahmen teilweise ungeeignet für KMU
- (Aktualität der Bausteine)

Alternative Vorgehensweise



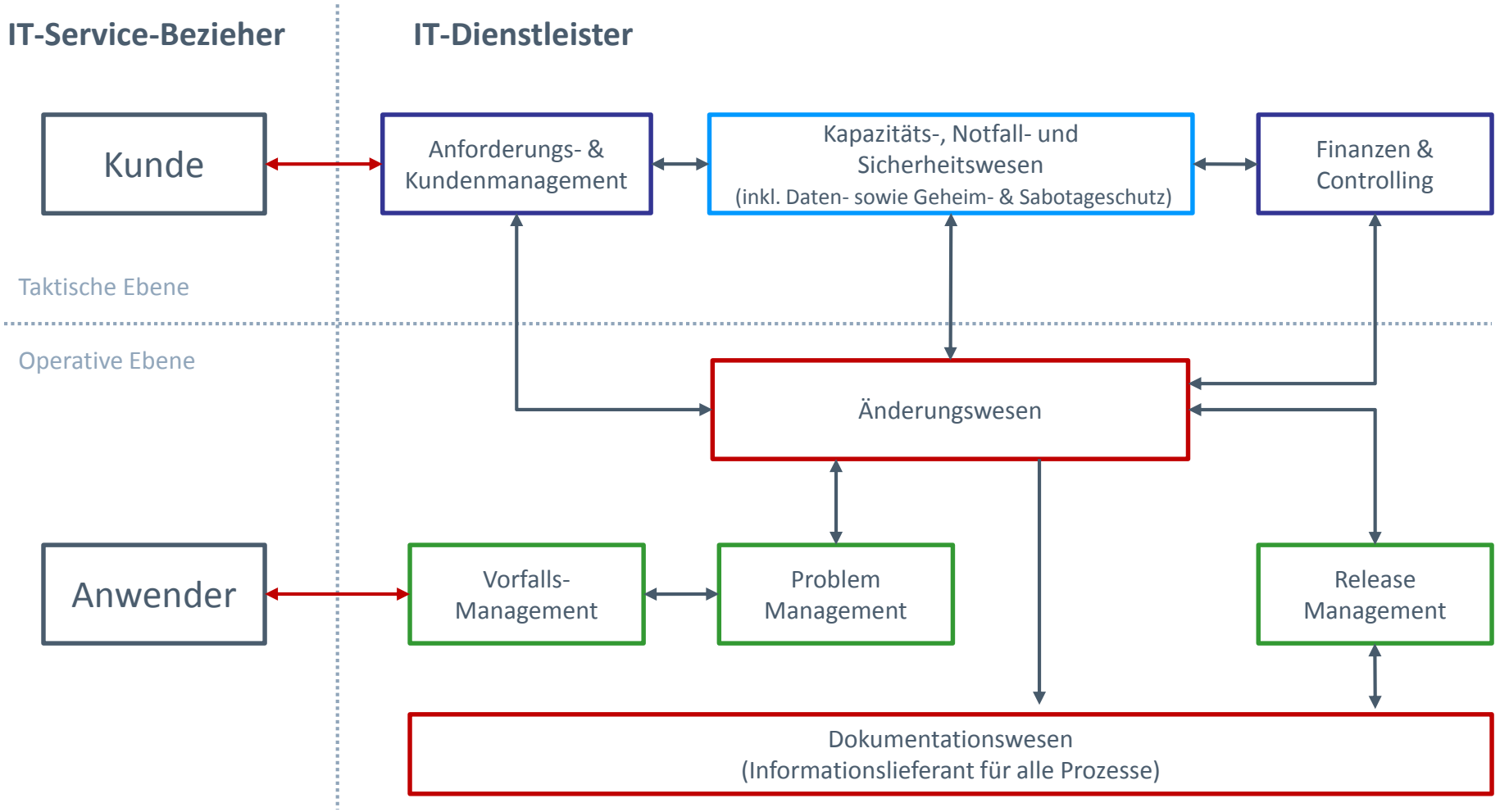
PERSICON

Kernpunkte der alternativen Vorgehensweise

- Prozessorientierung (ein zentraler Prozess statt dezentraler und redundanter Maßnahmen)
- Betriebs- statt Projektfokus
- Parallelisierung von Aufgaben statt Wasserfallmodell
- Synergien zu ITIL durch gemeinsames Vorgehens- und Prozessmodell
- Qualitätssteigerung und Kostensenkung durch Verlagerung von Aufgaben aus dem Sicherheitsmanagement in den Regelbetrieb
- Kritischer Erfolgsfaktor ist ein zentrales Dokumentations- und Auskunftssystem (CMDB) mit nativer Schnittstelle zum ISMS-Tool (z.B. GSTOOL) sowie ein funktionierendes Änderungswesen
- Synergieeffekte UPBund/IT-Grundschutz/Datenschutz nutzen um Aufwände zu senken
- Reife des Technik-Betriebs konstant erhöhen – wo sinnvoll

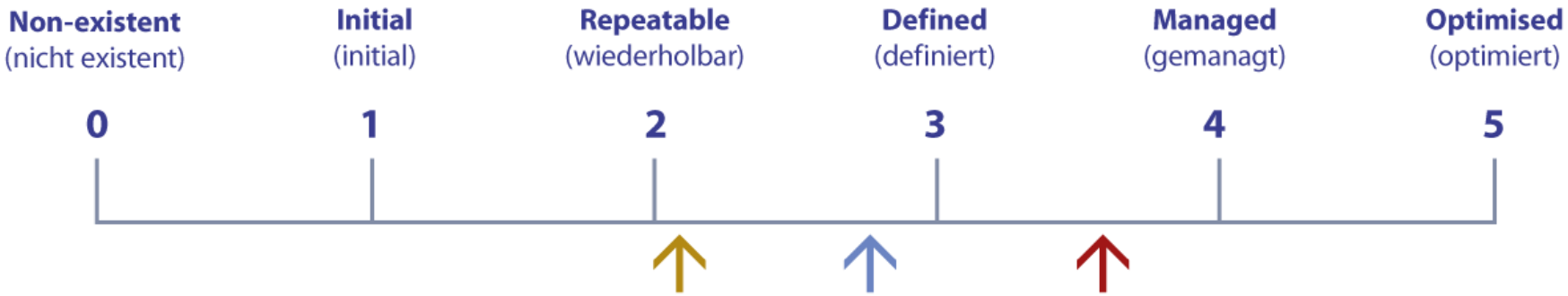
Achtung: Wenn Modellierung und Basis-Sicherheitscheck vor der Schutzbedarfsfeststellung durchgeführt werden, dann ist es wichtig ggf. Skalierbarkeitsbedarf der Maßnahmen hinsichtlich des Schutzbedarfes zu identifizieren und insb. B1.7 Krypto-Konzept darf nicht vergessen werden!

Beispiel eines vereinfachten Prozessmodells für den Technik-Betrieb



PERSICON

Prozess-Reifegradmodell



Derzeitiger Status

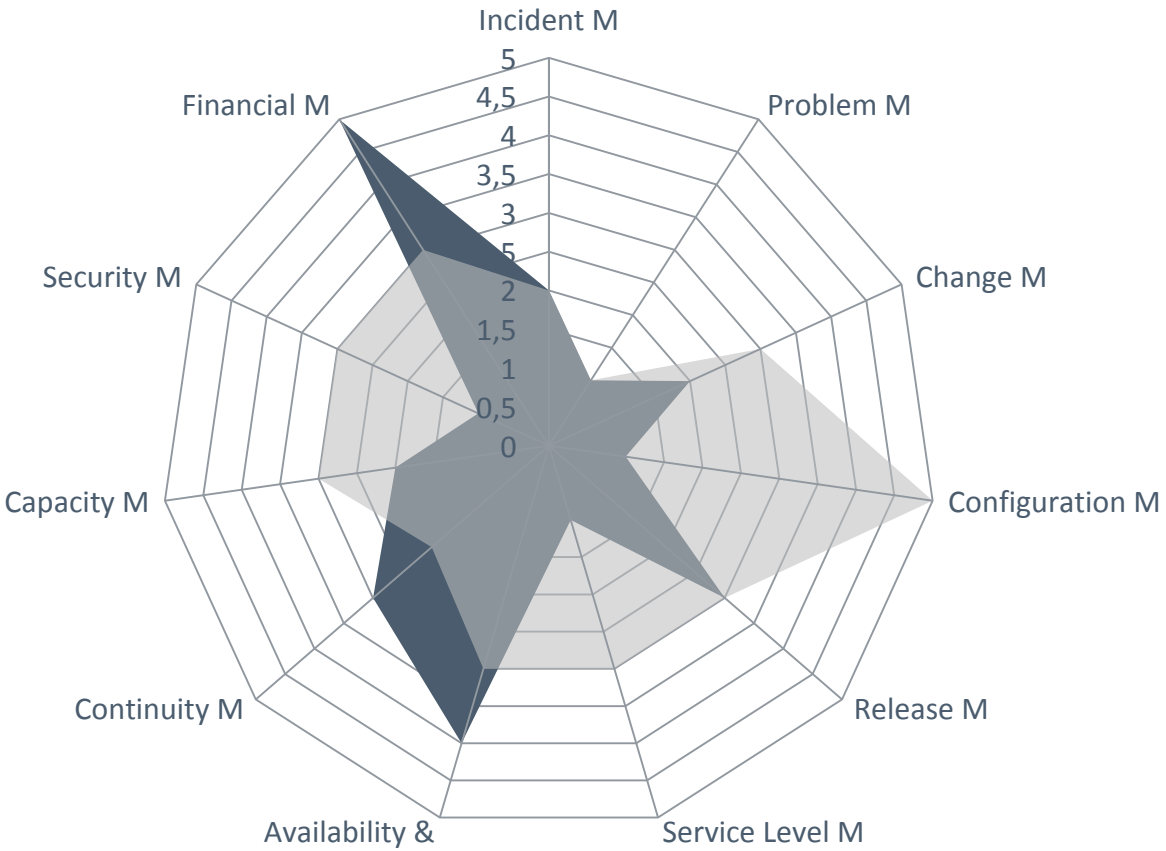
Durchschnitt der Industrie

Unternehmensziel

Niveaus

0 – Managementprozesse werden nicht angewandt
1 – Prozesse sind ad-hoc und unorganisiert
2 – Prozesse folgen einem regelmäßigen Muster
3 – Prozesse sind dokumentiert und kommuniziert
4 – Prozesse sind gemonitort und gemessen
5 – Good Practices werden angewandt und automatisiert

Beispielhafte Visualisierung der Prozessreife



Einsatzbereiche/Nutzen:

- Überblick gewinnen
- Delta-Analyse (Soll-Ist)
- Organisationsleitung und sonstige Beteiligte leichter mitnehmen
- Identifikation von „Quick Wins“
- Unterstützung bei Prioritätensetzung
- Bestimmung von Umsetzungsreihenfolgen
- (…)

PERSICON

Ausblick

- Vereinfachung – Vorgehensweise
- Verschlankung – Grundschutzkataloge
- Fokussierung auf KMU und auf CISO / CIO
- Grundschutz-Profile

Vielen Dank für Ihre Aufmerksamkeit

khaufe@persicon.com
Friedrichstraße 100 | 10117 Berlin
www.persicon.com

Tel: +49 (30) 6881988-80
Fax: +49 (30) 6881988-99
Mobil: +49 (1522) 25353-02