IT-Risk Management in Produktion und Fertigung

Notwendigkeit einer Betrachtung und praktische Umsetzung anhand der ISO 27001 von Informationssicherheit in Produktion und Fertigung

15.04 2008
IT Risk Management Forum 2008
in Düsseldorf

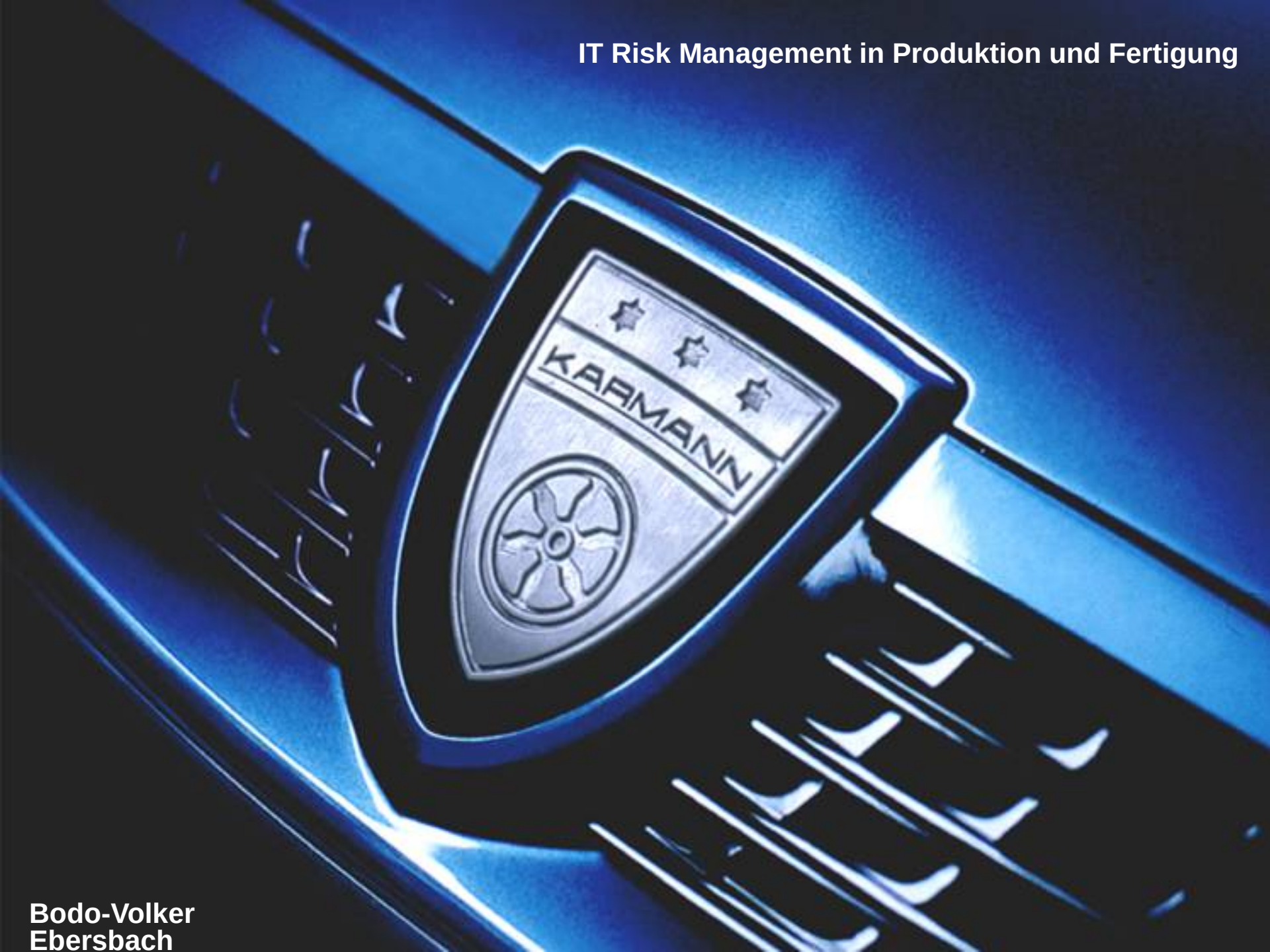
Praxisbericht

Bodo- Volker Ebersbach
CISO/ Leiter IT- Office
Wilhelm Karmann GmbH

IT-Risk Management in Produktion und Fertigung

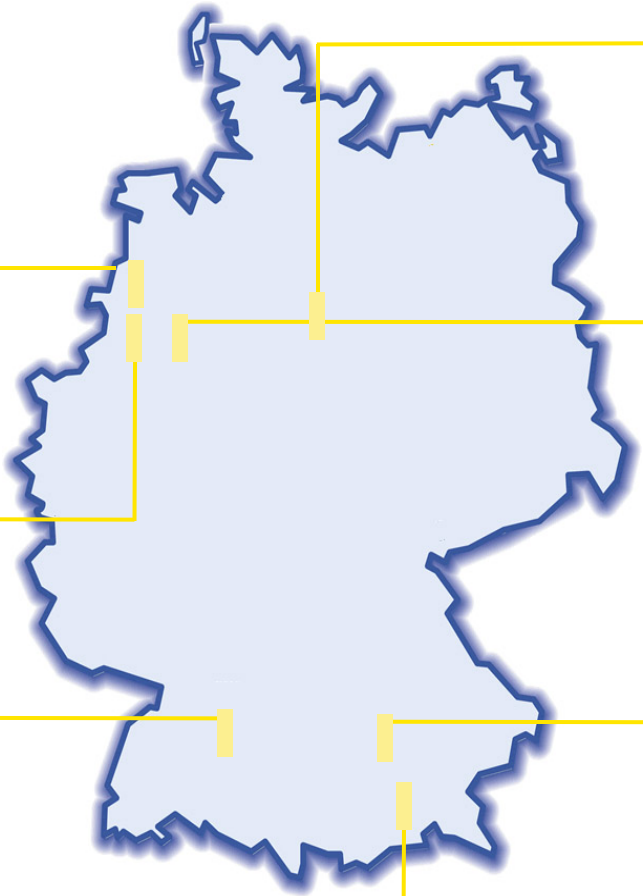
- 16:45 Uhr **Praxisbericht Wilhelm Karmann GmbH**
  - Unsere Zielfestlegung in der Sicherheitspolitik:
    - Sicherheitsmanagement bei Karmann
    - Einführung ISMS nach ISO 27001 inkl. VDA PTS
    - Verantwortlichkeiten in Organisation und Prozessen
    - Vorgehensmethode und Priorisierung von Sicherheitsmaßnahmen aus dem Risikomanagement
  - Risikomanagement
    - Geschäftsprozessliste als Ausgangsbasis
    - Klassifikation der Prozesse aus der Sicht des Business
    - Business BluePrint für das Risk Management
    - Methode zur Risikobewertung
    - Begegnungsplan und Maßnahmenmanagement

IT Risk Management in Produktion und Fertigung



Bodo-Volker Ebersbach

Inlandsstandorte



Wolfsburg
Vertrieb & Technik

ATP Automotive Testing Papenburg GmbH, Papenburg
Prüfgelände

Wilhelm Karmann GmbH Osnabrück
Fahrzeugbau, Entwicklung Produktionstechnologie, Dachsysteme

AGS GmbH, Osnabrück
Logistik-Dienstleistungen

Karmann Rheine GmbH & Co. KG, Rheine
Fahrzeugbau
Dachsysteme

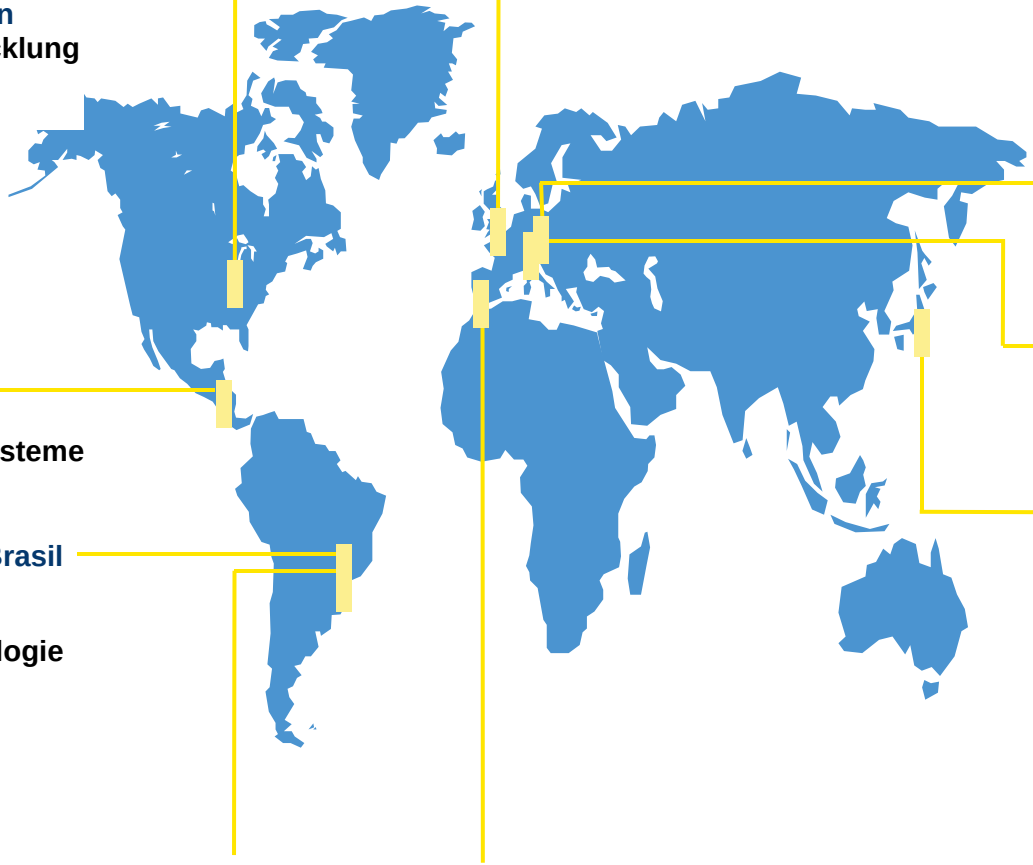
Karmann Engineering Services GmbH Bissendorf
Entwicklung

Sindelfingen
Vertrieb & Technik

Ingolstadt
Vertrieb & Technik

München
Vertrieb & Technik

Globale Standorte



Karmann U.S.A., Inc.
Plymouth, Michigan
Technische Entwicklung
Prototypenbau
Produktion

Karmann-Ghia
de Mexico, Puebla
Produktion Dachsysteme

Karmann-Ghia do Brasil
São Berdinando do Campo
Produktionstechnologie
Presswerk
Fahrzeugbau

Aethra Karmann-Ghia
Carrocerias
Resende
Produktionstechnologie

Karmann-Ghia de Portugal
Vendas Novas
Textilfertigung

Karmann Sunderland
U.K.
Produktion Dachsysteme

Karmann Zary
Polen
Produktion Dachsysteme

Karmann Chorzów
Polen
Produktionssysteme

Karmann Japan
Yokohama
Vertrieb
Engineering

Leistungsspektrum

KARMANN
fast forward

Der Entwicklungs-Dienstleister

Entwicklungs-Know-how

- Entwicklung von Nischenfahrzeugen
- Rohbau
- Dachsysteme
- Integration der Teilsysteme zum Gesamtfahrzeug
- Styling
- Konzepte/Vorentwicklung

Der industrielle Dienstleister

Betriebsmittelbau

- Engineering/Planning
- Werkzeuge
- Produktions Systeme
- Kleinstserie

Dachsysteme

- Soft-top
- Retractable Hardtop
- Dual-top

Fahrzeugbau

- Nischenfahrzeuge
- Abdeckung von Spitzenlasten
- Module

... in Kürze

KARMANN
fast forward

Standorte

GER	Osnabrück	4.376 MA
GER	Rheine	1.023 MA
GER	Bissendorf	70 MA
GER	Papenburg	150 MA
BRA	São Paulo	418 MA
POR	Vendas Novas	281 MA
USA	Plymouth	335 MA
MEX	Puebla	200 MA
UK	Sunderland	40 MA
POL	Chorzow	28 MA
POL	Zary	
JPN	Yokohama	

Umsatz (Karmann Gruppe) 2006

1,9 Mrd. EUR

Produktionszahlen 2006

Audi A4 Cabrio	28.301
MB CLK Cabrio	15.014
Chrysler Crossfire Coupé	1.547
Chrysler Crossfire Roadster	3.258
Renault Mégane II CC (Dachmodul)	32.402
VW New Beetle Cabr. (Dachmodul)	30.009
Pontiac G6 Convertible (Dachmodul)	19.756
Nissan Micra C+C	16.661
MB SLK Roadster (Rohbau)	42.649
MB CLK Cabrio (Rohbau)	5.918

Fachbereiche

Entwicklung
Betriebsmittelbau
Dachsysteme
Fahrzeugbau

Unternehmensbereiche

KARMANN
fast forward

Entwicklung

- Design Studio
- Concept Team
- Karosserie
- Ausstattung + Anbauteile
- Elektrik/Elektronik
- Gesamtfahrzeug
- Versuch & Prototypenbau
- Technische Dienstleistungen

Produktionstechnologie

- Produktionssysteme
- Werkzeugbau & Engineering
- Spezialserie & Module

Dachsysteme

- Entwicklung
- Konstruktion
- Musterbau
- Versuch/Erprobung
- Produktion

Fahrzeugbau

- Presswerk
- Karosseriebau
- Modulfertigung
- Lackiererei
- Fertigmontage

Gesamtfahrzeuge

Produktprogramm: Dachsysteme

KARMANN
fast forward

Audi A4 Cabriolet (Softtop)

Mercedes-Benz CLK Cabriolet (Softtop)

Volkswagen New Beetle Cabriolet (Softtop)

Chrysler Crossfire Roadster (Softtop)

Renault Mégane II CC (Retractable Hardtop)

General Motors Pontiac G6 Cabriolet (Retractable Hardtop)

Nissan Micra Cabriolet (Retractable Hardtop)

Bentley Continental GTC Cabriolet (Softtop)

Chrysler Sebring Cabriolet (Softtop & RHT)

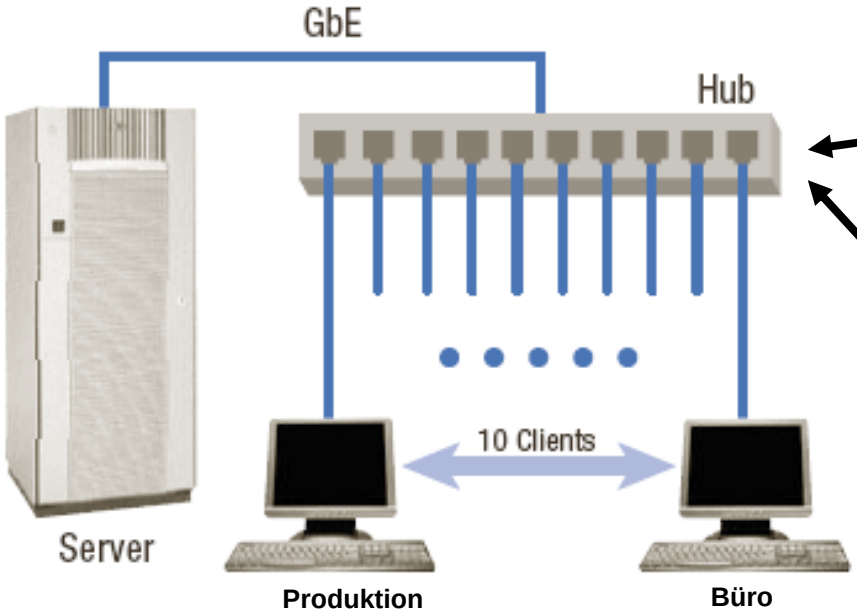
Ford Mustang Cabriolet (Softtop)

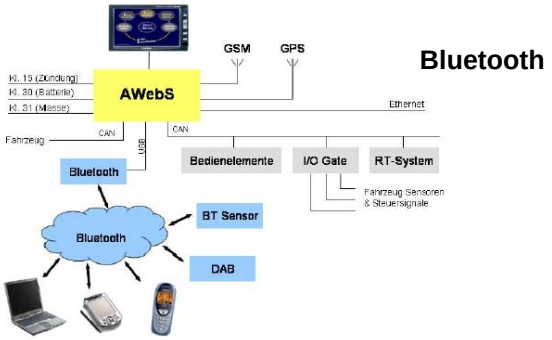
Europäischer OEM

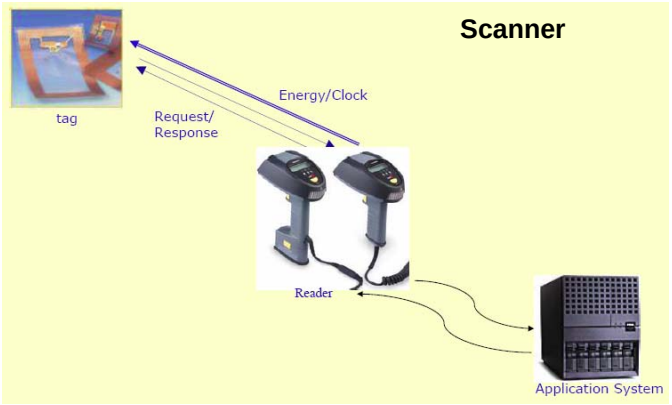
Verschmelzung von Büro- und Produktions- IT Netzwerktopologie in der heutigen Praxis

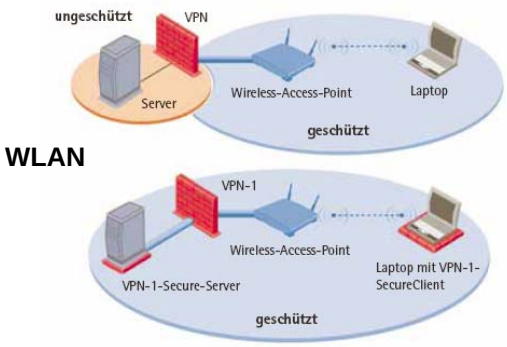
KARMANN
fast forward

- Heutige Netzwerkstruktur mit angekoppelten Insellösungen





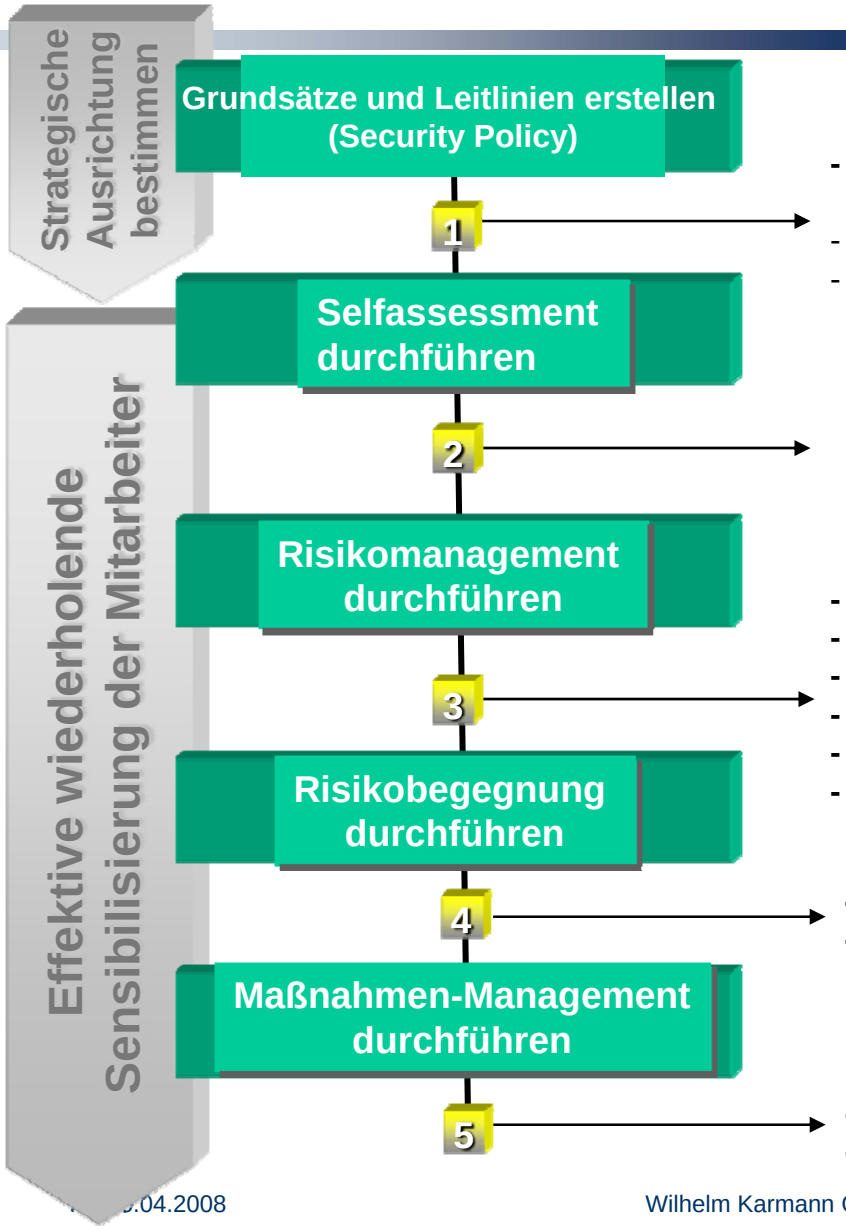




WLAN

Unsere Methode zur Einführung einer ISMS

KARMANN
fast forward



- Geschäftsführungsentscheidung zur konsequenten Sicherheitspolitik
- Ernennung eines Sicherheitsbeauftragten auf Managementebene
- Einführung von Grundsätzen und Leitlinien

- Implementierung der ISMS-Organisation
- Technik geprüft und bewertet (Vulnerability Assessment)
- Ressourcen und Prozesse zugeordnen und bewertet
- Produktschutz nach VDA PTS bewertet

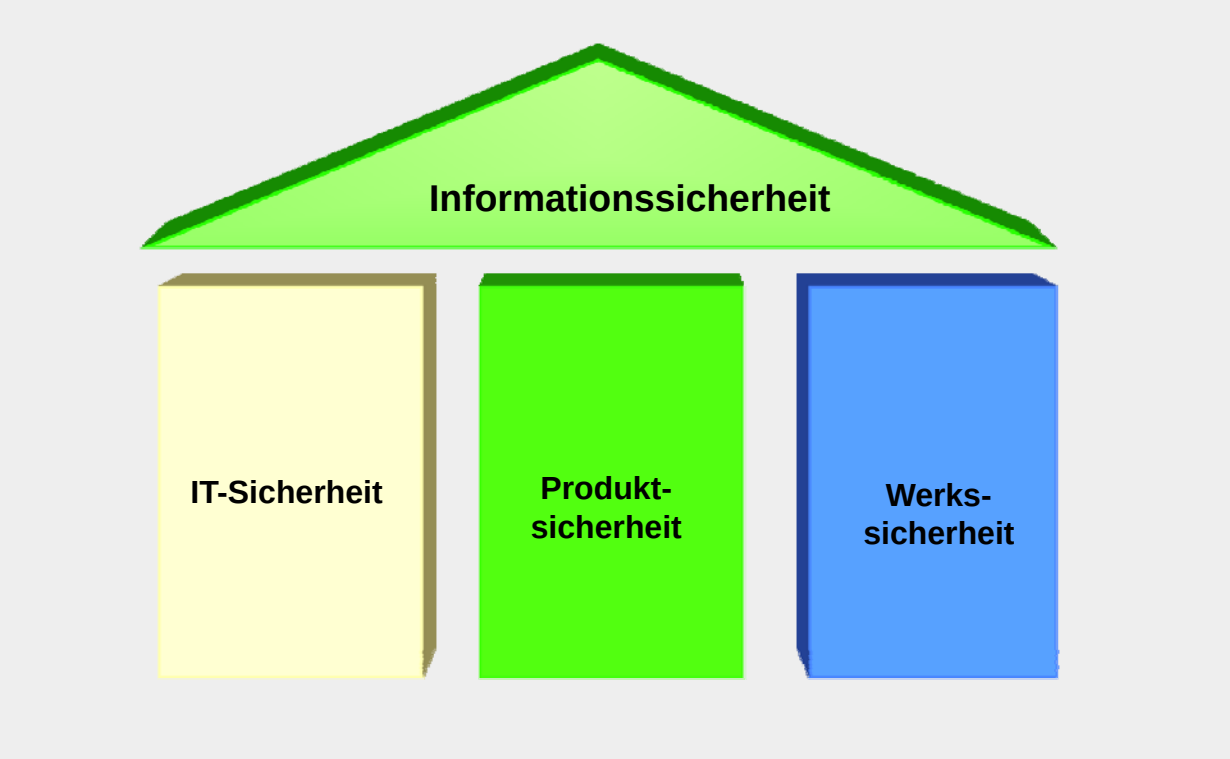
- Beurteilung der Prozesse nach „Business-Kritikalität“
- Erstellung eines Business-Blueprints der Systemlandschaft
- Ermittlung der Assetwerte zur Bildung eines Kennzahl-Systems
- Bedrohungs- und Schwachstellenanalyse der Systemlandschaft
- Bewertung der möglichen Risiken
- Erstellung eines Risiko-Begegnungsplanes

- Akzeptanz und Abstellung der Risiken
- Durchführung von Sicherheitsmaßnahmen

- Terminieren und Aufsetzen der notwendigen Projekte
- Überprüfung der eingeleiteten Maßnahmen

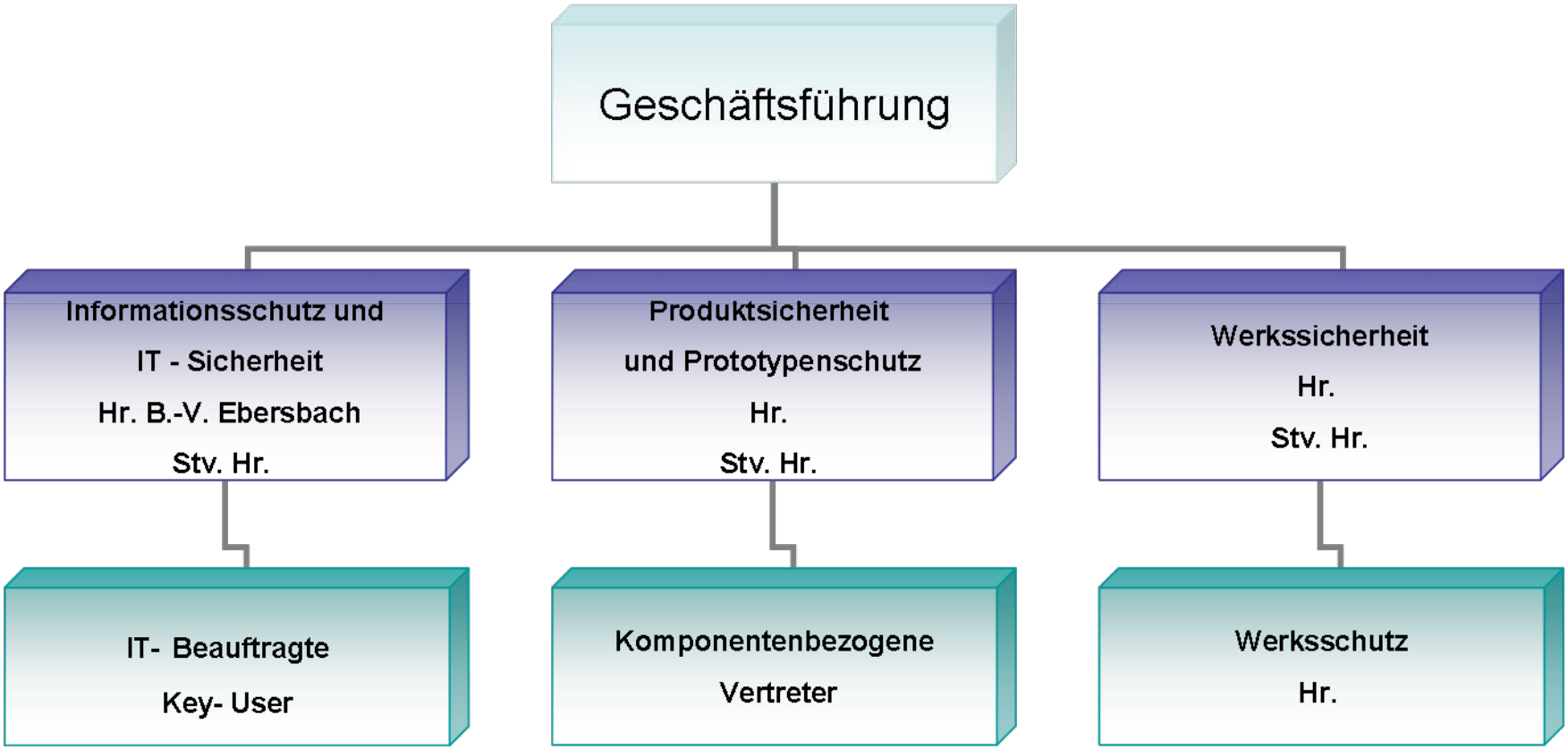
Informationssicherheit bei Karmann (3 Säulen)

- Informationssicherheit schützt das Know How und damit die Wettbewerbsfähigkeit
- Die erfolgreiche Zertifizierung ist ein Teil der Basis für neue Aufträge (Vertraulichkeit)



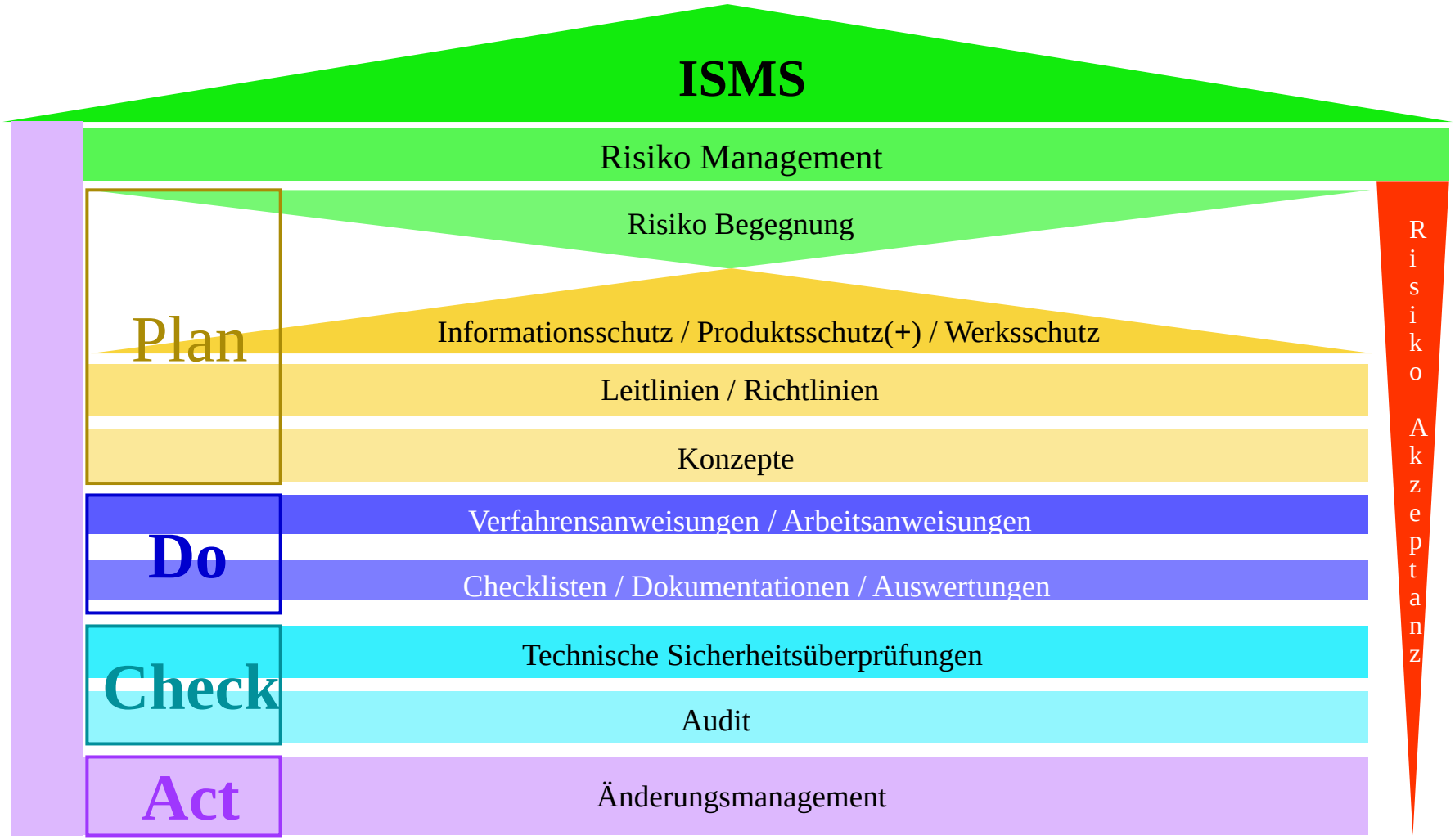
- Die Herausforderungen der Zukunft erfordern ein zentrales Sicherheitsmanagement
- Der dazu notwendige geordnete Sicherheitsprozess muß Teil unserer Aufgabenabwicklung werden (keine zusätzliche Administration)

Organigramm ISMS



Einrichtung eines Sicherheitsmanagements und Zertifizierung nach ISO/IEC 27001:2005 +

KARMANN
fast forward



Planung und Einführung eines ISMS
Teilprojekte und Control Clauses

KARMANN
fast forward

Teilprojekte nach den Control Clauses der ISO 27001

TP A 5 Sicherheitsrichtlinie
TP A 6 Organisation Informationssicherheit
TP A 7 Asset Management
TP A 8 HR Sicherheit
TP A 9 Physikalische Sicherheit
TP A 10 Kommunikations- u. betriebliches Management
TP A 11 Zugriffskontrolle
TP A 12 IT-Syst. Anschaffung, Entwicklung und Wartung
TP A 13 Incident Management
TP A 14 Business Continuity Management
TP A 15 Einhaltung von Richtlinien
A. Risiko Management
B. Produktsicherheit
C. Technische Überprüfungen

Terminologie

TP = Teilprojekt

A 5, A 6 .... = Appendix 5, ...

Entspricht den Control Clauses der

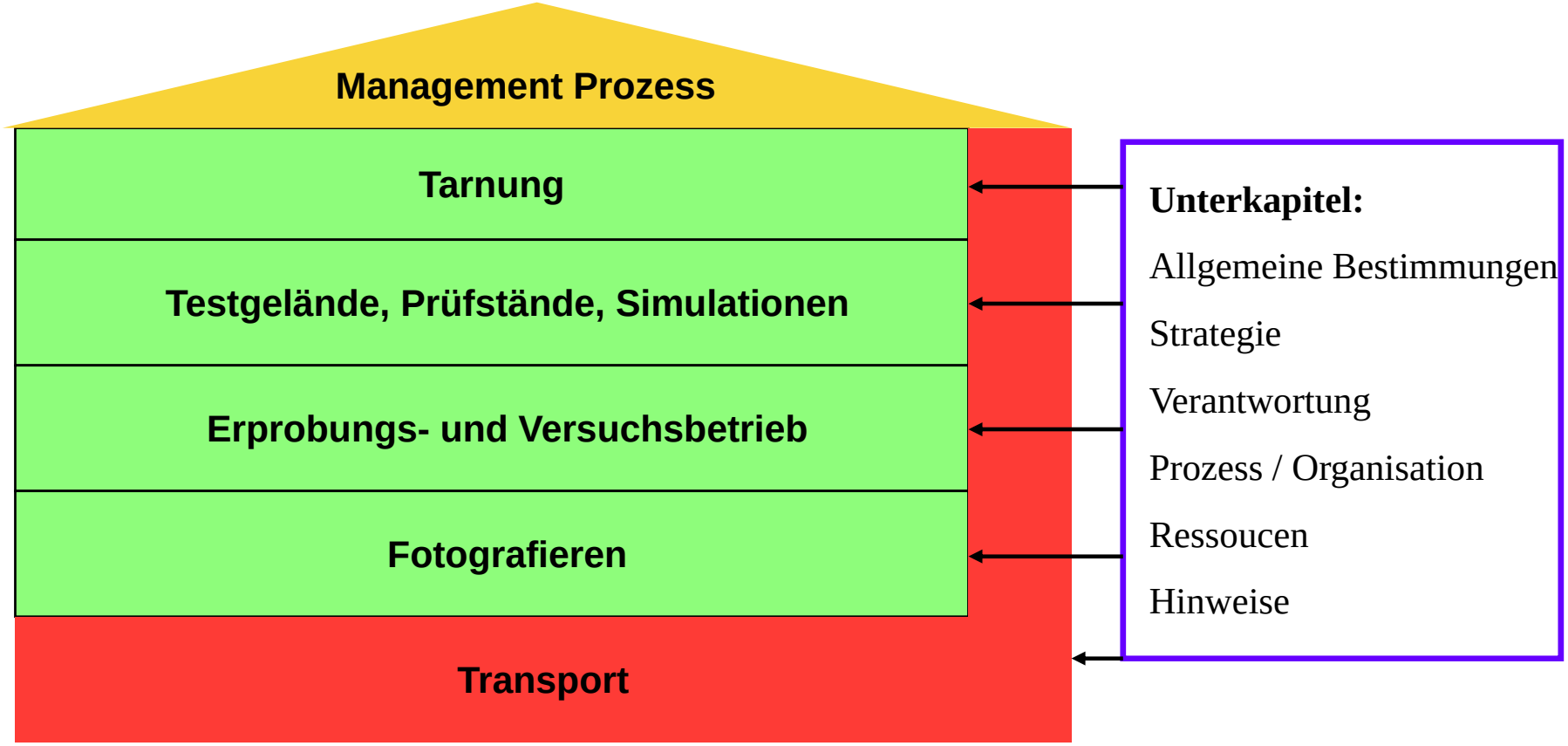
ISO 27001

Control = Sicherheitsregelung

Control Objective = Sicherheitsregelungsziel

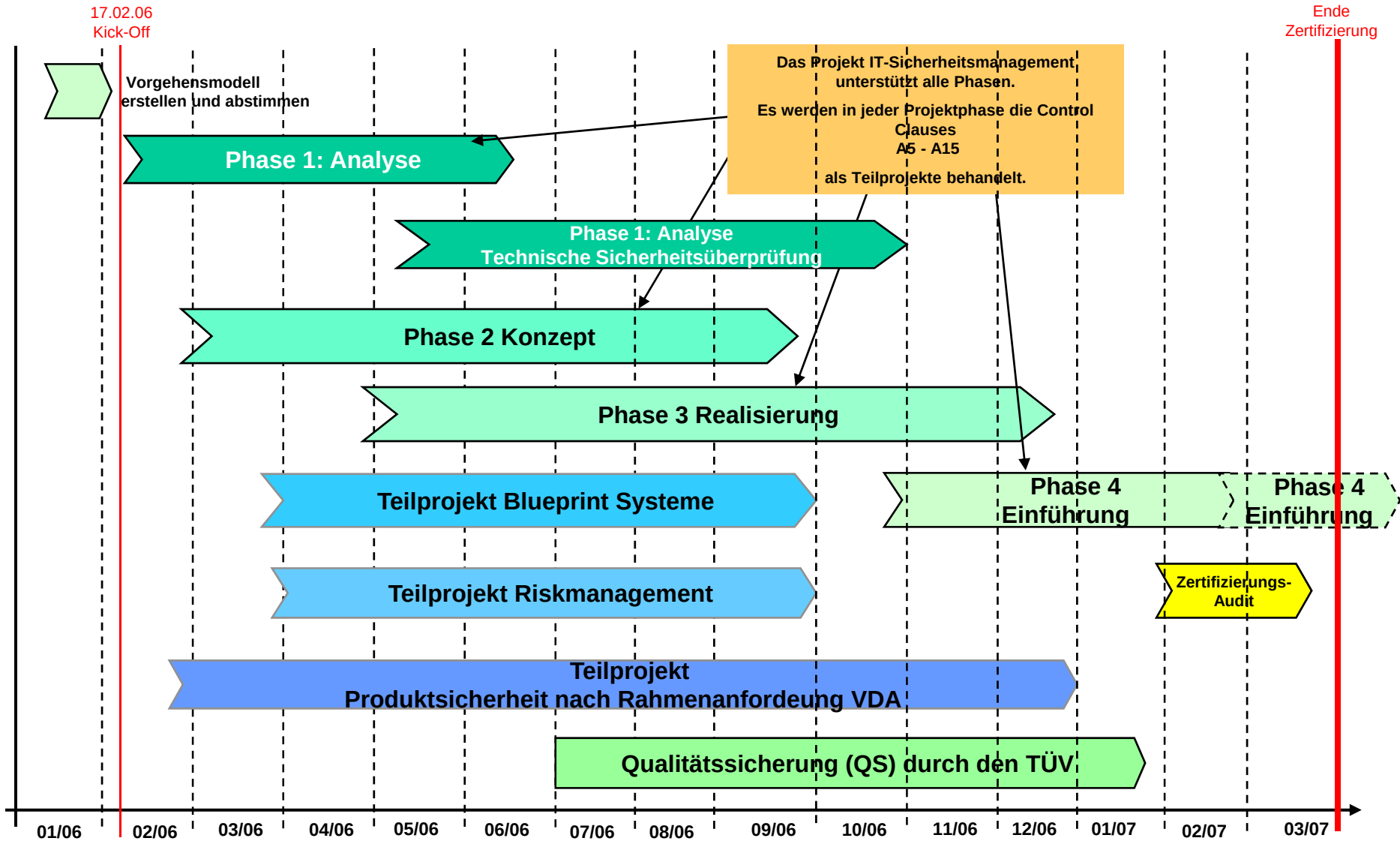
Control Clause = Sicherheitsregelungsabsatz

Teilbereiche Produktsicherheit aus der Rahmenanforderung VDA



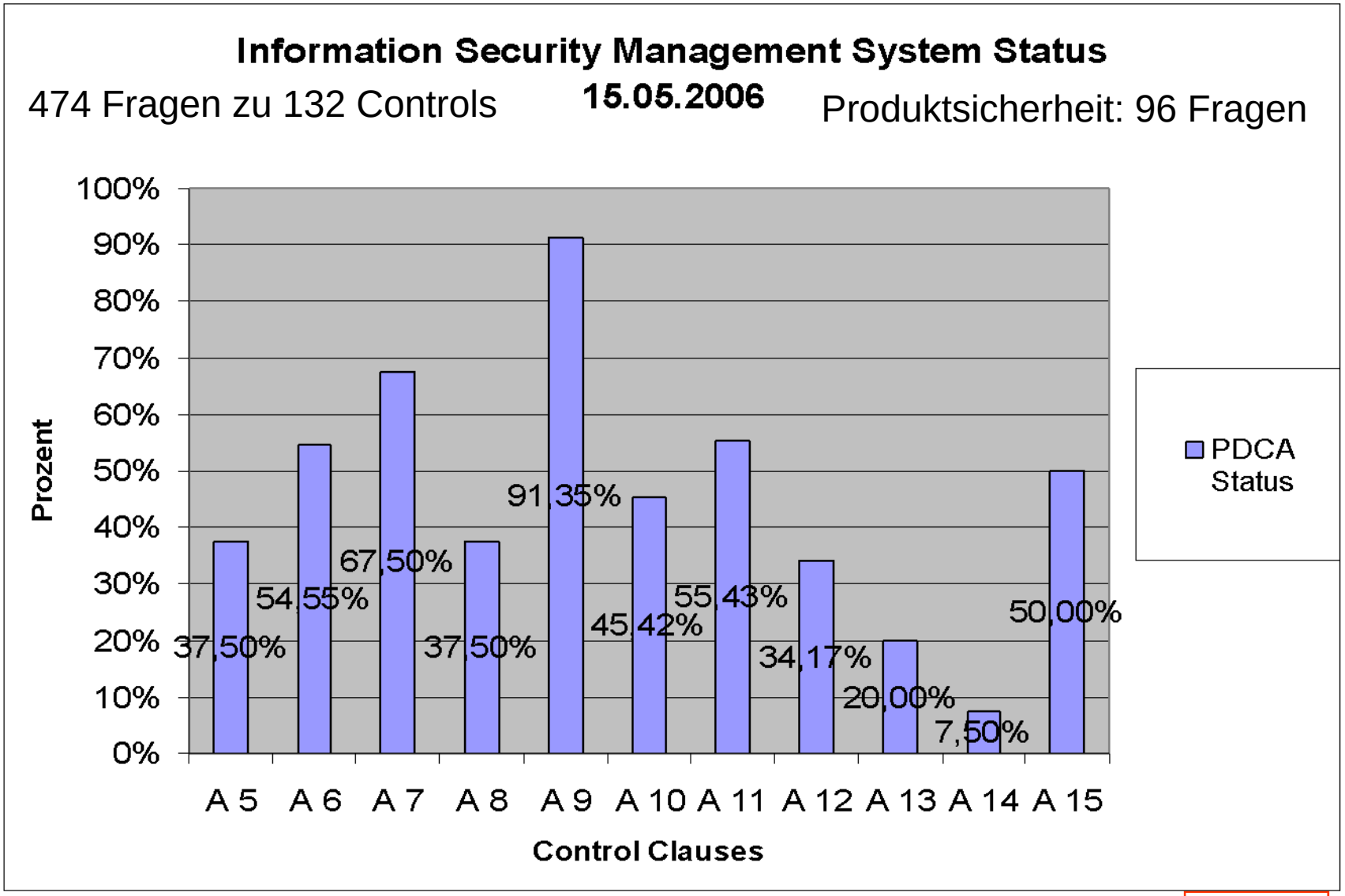
Die ISMS- Datenbank enthält alle wichtigen Informationen ISMS DB

Ablaufplan
Auditierung nach ISO 27001



Selfassesment Stand Vorbereitung 2006

(Expertendatenbank von WMC eingesetzt)



Selfassesment Maßnahmen-Bericht
(Auszug aus der Expertendatenbank)

KARMANN
fast forward

Control 5.1.1

Dokument zur Informations-Sicherheitsleitlinie

Plan	**1**
Do	**1**
Check	**1**
Act	**-1**
Status	**2**

Aufwand_PD	**10**
Auwand_CA	**2**
Ziel_PD	**KF**
Ziel_CA	**MF**

Bemerkung:

Die derzeitigen IT- Grundsätze und Leitlinien enthalten nicht alle Formalitäten, wie sie von der Norm definiert werden. Z.B. fehlen Absätze zu Review ISMS, Rollendefinition und Informationssicherheit (es wird nur IT-Sicherheit behandelt).

Maßnahme:

Erstellung einer Information Security Policy :
Gemäß den IT-Grundsätzen und Leitlinien eine Information Security Policy erstellen, die alle Aspekte der ISO 27001 abdeckt

Abstimmen der neuen Policy mit der Geschäftsleitung, dem Policy Datenschutzbeauftragten, der Rechtsabteilung und dem Betriebsrat.

Freigabe durch die Geschäftsleitung und interne Veröffentlichung.
Bereitstellen der Policy in HR und an allen Pförtnerbesetzten Geländezutrittspunkten.

(Auszug aus der Expertendatenbank)

Projekt-Maßnahmenliste

1 Information Security Policy

Erstellung des Dokumentes

Verantwortlicher Herr Ebersbach

M-ID	*Maßnahme*	*Text*
1	Erstellung einer Information Security Policy	Gemäß den IT-Grundsätzen und Leitlinien eine Information Security Policy erstellen, die alle Aspekte der ISO 27001 abdeckt
2	Abstimmung der Information Security Policy	Abstimmen der neuen Policy mit der Geschäftsleitung, dem Datenschutzbeauftragten, der Rechtsabteilung und dem Betriebsrat.
3	Freigabe und interne Veröffentlichung	Freigabe durch die Geschäftsleitung und interne Veröffentlichung. Bereitstellen der Policy in HR und an allen Pförtnerbesetzten Geländezutrittspunkten.
4	Review Prozess der Information Security Policy	Review Prozess definieren. Hierzu definieren, welche Daten zwischen den einzelnen Reviews zu sammeln sind, um sie im Review auszuwerten. Festlegen wer in welchen Zeitabständen die Reviews durchzuführen hat. Festlegen ob und in welchen Zeitabständen ein unabhängiges Review durchgeführt wird.
29	Disziplinarmaßnahmen in den Richtlinien bzw. der Policy nennen.	Aufnahme eines Durchsetzungsabsatzes in die Information Security Policy. Aufnahme in die Senisbilisierungsmaßnahmen.

Agenda

- Unsere Zielfestlegung in der Sicherheitspolitik:
  - Sicherheitsmanagement bei Karmann
  - Einführung ISMS nach ISO 27001 incl. VDA PTS
  - Verantwortlichkeiten in Organisation und Prozessen
  - Vorgehensmethode und Priorisierung von Sicherheitsmaßnahmen aus dem Risikomanagement

- Risikomanagement
  - Geschäftsprozessliste als Ausgangsbasis
  - Klassifikation der Prozesse aus der Sicht des Business
  - Business BluePrint für das Risk Management
  - Methode zur Risikobewertung
  - Begegnungsplan und Maßnahmenmanagement

KARMANN
fast forward

Bewertung von Risiken

Wofür?

- Risiko erkennen, messen
- Entscheidungsgrundlage für eine Begegnung
- Liefert Informationen für Business Continuity Management
- Liefert Informationen für Incident Handling

Was bewerten?

- Asset Werte
- Bedrohungen
- Schwachstellen
- Vorhandene Sicherheitsmaßnahmen
- resultierendes Risiko

Wer?

- Risk Manager
- Business Prozess Owner
- System Owner
- Application Owner
- IT-Sicherheitsbeauftragter

Wie?

- Bewertung qualitativ mit der Hilfe von Tabellen

KARMANN
fast forward

Bewertung von Risiken

Übergeordnete Bewertung

- Assets anhand der Wichtigkeit für die Geschäftprozesse bewerten (niedrig, mittel, hoch)
- Hoch -> detaillierte Risiko Analyse
- Niedrig und Mittel -> Basis Bewertung

Asset bewerten

- Finanzelle Asset Werte
- Notwendigkeit für Vertraulichekeit
- Notwendigkeit für Integrität
- Notwendigkeit für Verfügbarkeit
- (0,1,2,3,4) Höchste Zahl = Bewertung

Bedrohung

- Bedrohungsliste
- Zuordnung zu Assetgruppen
- Qualitative Einschätzung der Eintrittsmöglichkeit der Bedrohungen
- (niedrig, mittel, hoch)

Schwachstellen

- Schwachstellenliste
- Zuordnung zu Assetgruppen
- Qualitative Einschätzung der Gefährdungsstufe
- (niedrig, mittel, hoch)

KARMANN
fast forward

Bewertung von Risiken

	Bedrohung Level	Niedrig			Mittel			Hoch		
	Schwachstellenlevel	Niedrig	Mittel	Hoch	Niedrig	Mittel	Hoch	Niedrig	Mittel	Hoch
Wert der Assets	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Risiko nicht akzeptabel, Begegnung notwendig

KARMANN
fast forward

Begegnung von Risiken / Auswahl der Sicherheitsmaßnahmen

Methoden der Begegnung

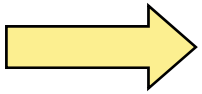
- Akzeptanz
- Transfer auf Kunden/Lieferanten
- Transfer auf Versicherungen
- Sicherheitsmaßnahmen

Akzeptanz ?

- Geschäftsleitung trägt das Risiko bewusst
- Es existiert ein unterschriebenes Dokument
- Beschreibung des Risikos
- Bestätigung der Akzeptanz durch die Geschäftsleitung

Sicherheitsmaßnahmen

- Welchen Risiken wird wie begegnet
- Welche Controls sind eingeführt
- Welche Controls werden eingeführt
- Welche Controls werden nicht eingeführt und warum



Statement
of
Applicability

Risk Management in der Praxis

KARMANN
fast forward

Für ein unternehmensweites Risiko Management sind folgende Kern-informationen aus den einzelnen Teilbereichen des Unternehmens essentiell:

- Geschäftsprozessliste
- Klassifikation der Prozesse
- Identifikation der Abhängigkeiten der betrieblichen Prozesse von den sie unterstützenden IT- Systemen, Klassifikation der IT- Systeme und Applikationen auf Basis der Prozesse
- Verfügbarkeits- Integritäts- Vertraulichkeitsanforderungen basierend auf den Bedürfnissen der Geschäftsprozesse und gesetzlichen Bestimmungen
- Identifikation und Bewertung der möglichen Bedrohungen und Schwachstellen der IT- Systeme

Die Klassifikation erfolgt aus der Sicht des Business. Allgemein ist zu beantworten, welche Prozesse maßgeblich zum Erfolg des Unternehmens beitragen, und welche Bedrohungen das Potential haben den Geschäftsertrag negativ zu beeinflussen.

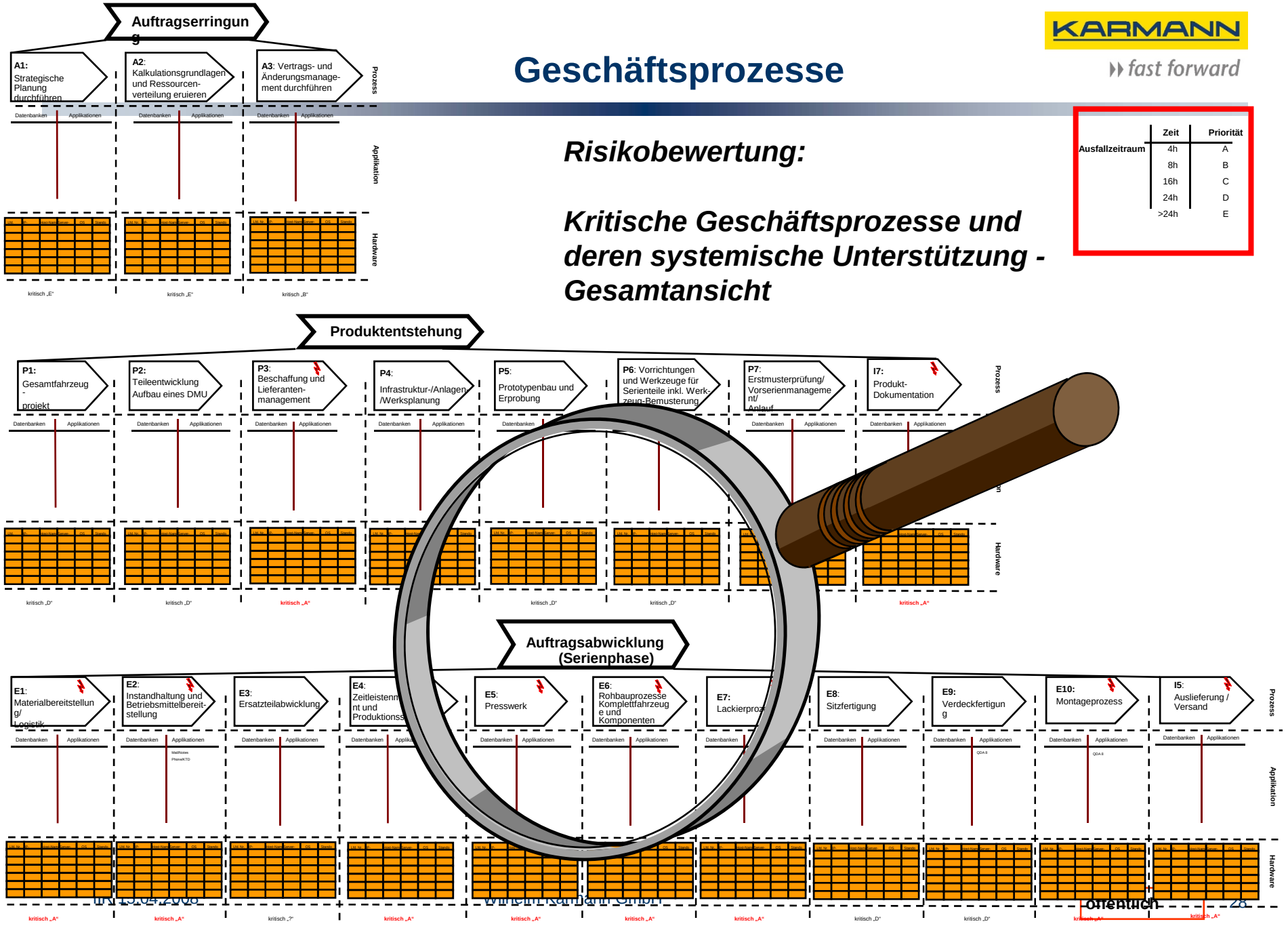
Geschäftsprozesse

KARMANN
fast forward

Ausfallzeitraum	Zeit	Priorität
	4h	A
	8h	B
	16h	C
	24h	D
	>24h	E

Risikobewertung:

Kritische Geschäftsprozesse und deren systemische Unterstützung - Gesamtansicht



Risikobewertung: Kritische Geschäftsprozesse und deren systemische Unterstützung - Ausschnitt

KARMANN
fast forward

Ausfallzeitraum	Zeit	Priorität
	4h	A
	8h	B
	16h	C
	24h	D
	>24h	E

Prozess

Auftragsabwicklung (Serienphase)

E5: Presswerk

E6: Rohbauprozesse

E7: Lackierprozesse

Applikation

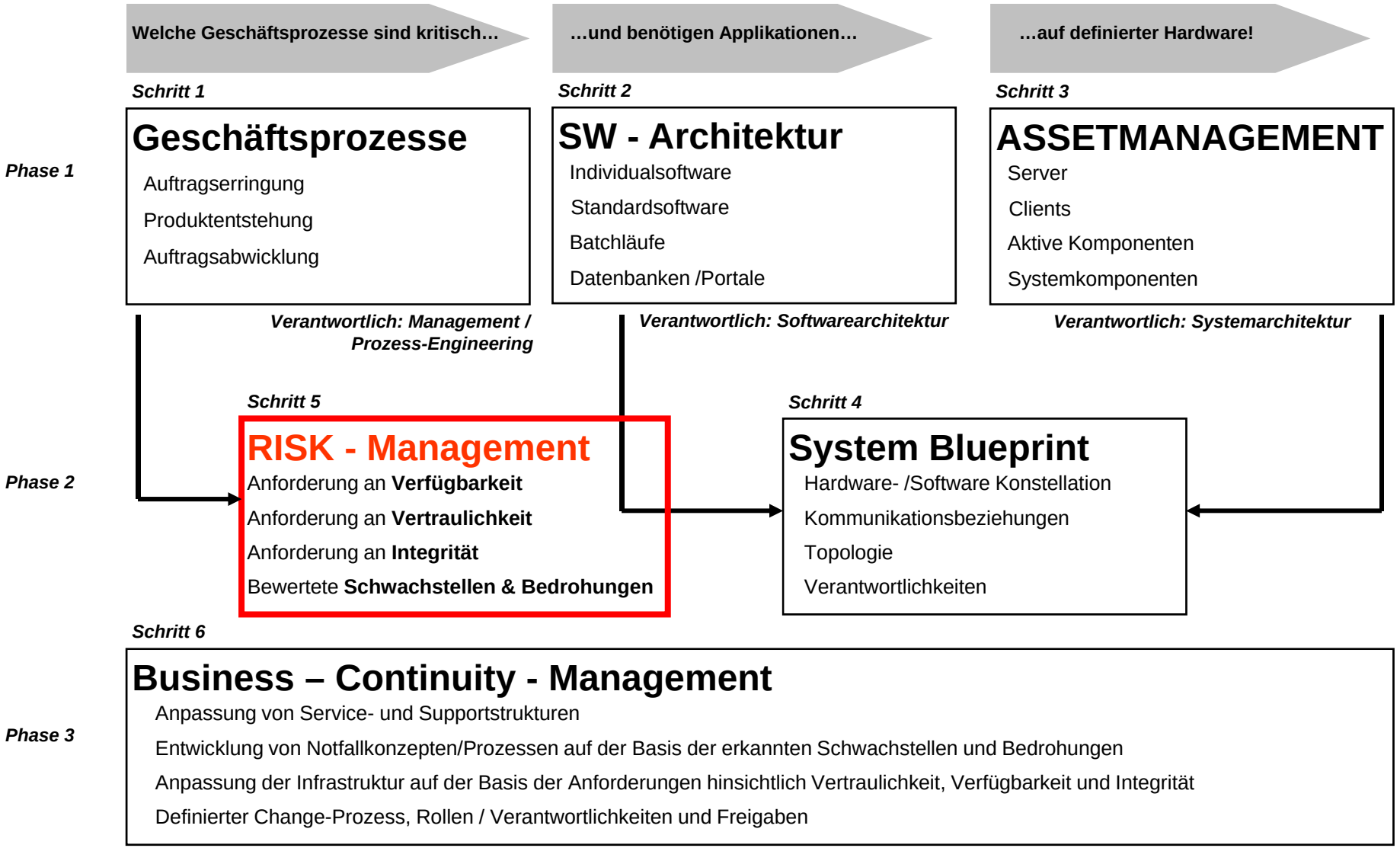
Datenbanken/ Middleware	Applikationen
- DB-Instanzen - VM-Ware - Webserver	Applikation 1

System

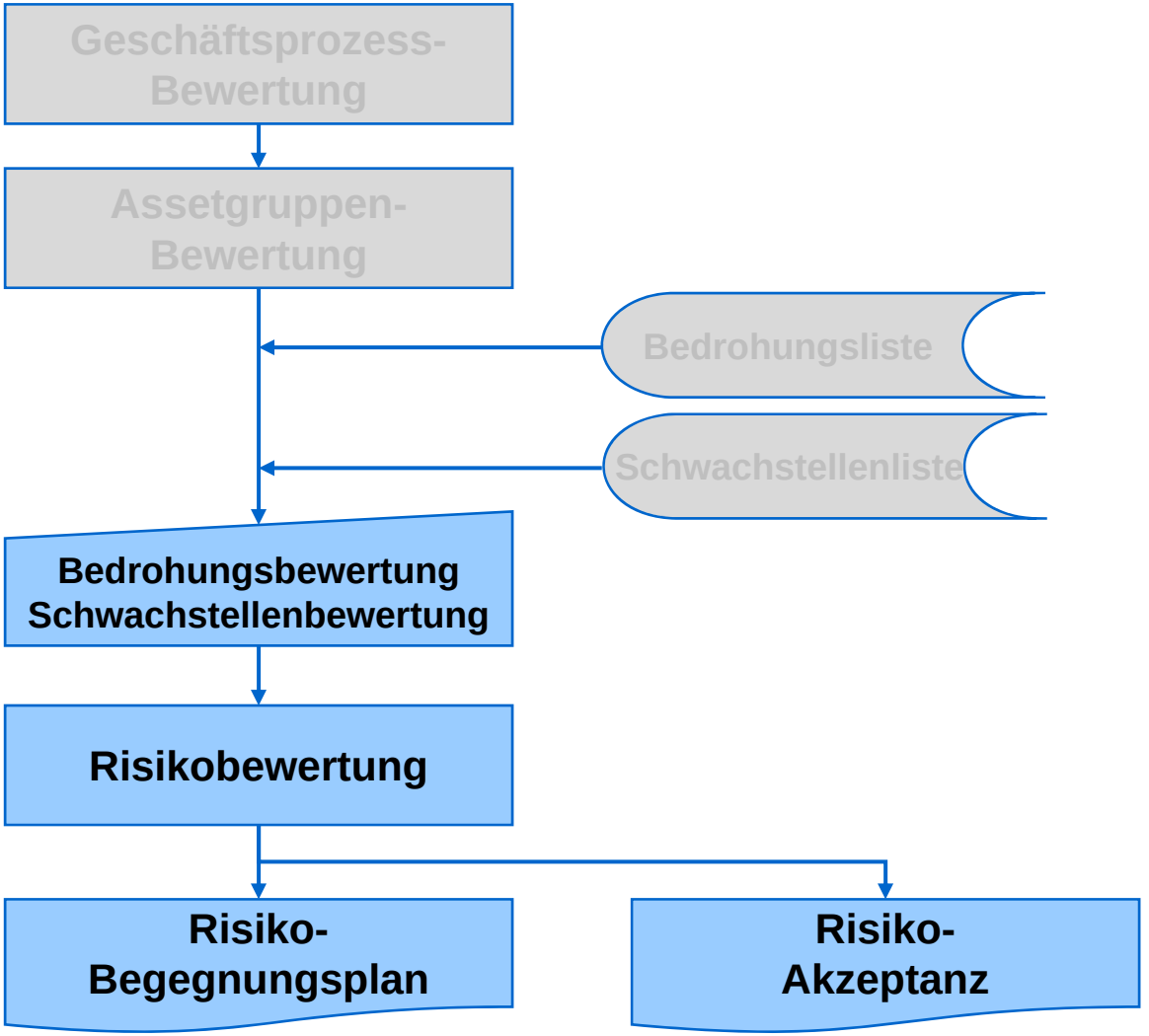
Host-Name	IP-Adresse	Server-Typ	Standort
App01	177.777.777	Cray II	RZ
…	…	…	…
…	…	…	…

Der Weg zum systemgestützten System-Blueprint

KARMANN fast forward



Methode zur Risikobewertung



Beispiele aus dem RA (Geschäftsprozessbewertung)

GP-ID	Geschäftsprozess	geschäfts-kritisch	Bemerkung
A1	Strategische Planung / strategische Projekt-Auswahl	niedrig	Basiert auf personenbezogenem Know-how und ist reproduzierbar.
A2	Angebotserstellung - Kalkulationsgrundlagen und Ressourcenverteilung	hoch	Zielgerichtete Angebotserstellung mit dem Ziel der Auftragserringung (Treffergenau) Eine integere Datenbasis bei der Offertenerstellung ist zwingend erforderlich.
A3	Vertrags- und Änderungs-Management	niedrig	
P1	Gesamtfahrzeugprojekt	Hoch	Gilt als Kernkompetenz und höchstes „Asset“ des Unternehmens
P2	Teileentwicklung – Aufbau eines DMU	mittel	Digitale Produkt-Entwicklung: Datenaustausch mit OEMs und Dienstleistern zur Bildung des Digital-MockUp.
P3	Beschaffung und Lieferantenmanagement	hoch	a) Beschaffung gem. der Philosophie des Product-Livecycle-Management, Erstbemusterung, Nachalten und Pflege des QM-Status auf Teileebene, b) Lieferantenmanagement im Sinne der strategischen Ausrichtung und nach den Anforderungen der Qualitäts-Sicherung (und Einbindung in die Notfallplanung gem. BCM)
P4	Infrastruktur-/Anlagen-/Werksplanung	niedrig	
P5	Prototypenbau und Erprobung	Niedrig	

Beispiele aus dem RA (Asset-Gruppen Bewertung 1)

KARMANN
fast forward

AG- ID	GP-ID	IT-Funktions (Gruppe)	Beschreibung	Unterstütztes Unternehmensziel	Bewertung nach Abhängigkeit des Geschäftsbetriebes	Kosten für Ersatz
10		SAP R3	FI/CO/MM, Schnittstellen zu HOST-System, PVR	Internes/externes RW	niedrig	**2 Mio. €**
20		SAP-SRM	Elektronische Beschaffung für NPM	Effizienter Beschaffungspro-zess	niedrig	**1 Mio. €**
30		SAP-HR	Personalmgt.		niedrig	**1 Mio. €**
40		SAP-BW	Controlling-/Planungsinstru-ment (light)	Integrierte Unternehm. Planung	niedrig	**1 Mio. €**
50		PVR	Produktionssteuerung (G-Fz)	Effiziente Auftrags-Abwicklung	hoch	**5 Mio. €**
60		- Fahrzeug-DB			niedrig	**0,2 Mio**
70		Lackleit-rechner			hoch	**0,5**
80		- FABS			Hoch (bei Fakrurierung)	**0,2**
90		Spider	Asset, Contract, Purchase, Licence		Hoch	**0,5**

Beispiele aus dem RA Asset-Gruppen Bewertung 2

KARMANN
fast forward

AG ID	Asset Name	Vertraulich-keit	Integrität	Verfügbarkeit	Finanzieller Wert	Bem.	A-Bewertung
10	SAP R3	3	4	3	3	C: Buchhaltung	4
20	SAP-SRM	2	4	1	2	Zu D: Gebote der Lieferanten schützen	4
30	SAP-HR	4	4	1	2		4
40	SAP-BW	3	4	1	2		4
50	PVR	2	4	4	3		4
60	- Fahrzeug-DB	2	2	2	1	internes Tool zur Auswertung	2
70	Lackleitrechner	2	4	1	1		4
80	- FABS	2	4	1	1		4
90	Spider	2	2	2	1		2
100	**Host (+ Subsysteme)**	2	4	4	4		4
105	**-Varix**	0	0	0	0	Fremdsystem	0

Beispiele aus dem RA Bedrohungs-Bewertung

KARMANN
fast forward

	AG-Name	SAP R3	SAP-SRM	SAP-HR	SAP-BW	PVR
	AG-ID	**10**	**20**	**30**	**40**	**50**
Bed-ID	**Bedrohung Wertebereich: niedrig=0, mittel=1, hoch=2 (n.a.=-2)**					
10	Erdbeben	-2	-2	-2	-2	-2
20	Überflutung	-2	-2	-2	-2	-2
30	Sturm	0	0	0	0	0
40	Blitz	0	0	0	0	0
50	Bombe	0	0	0	0	0
60	Waffengebrauch	0	0	0	0	0
70	Feuer	1	1	1	1	1
80	Sabotage	0	0	0	0	0
90	Stromausfall	1	1	1	1	1
100	Wasserausfall	0	0	0	0	0
110	Ausfall der Klimaanlage	0	0	0	0	0
120	Hardware Fehler	1				
130	Stromschwankungen					
140	Hohe Luftfeuchtigkeit oder Temperatur					
150	Staub					
160	EM-Einstrahlung					
170	Elektrostatische Entladung					
180	Diebstahl					

Beispiele aus dem RA Schwachstellen-Bewertung

KARMANN
fast forward

	AG-Name	SAP R3	SAP-SRM	SAP-HR	SAP-BW	PVR
	AG-ID	**10**	**20**	**30**	**40**	**50**
S-ID	**Schwachstelle Wertebereich: niedrig=0, mittel=1, hoch=2 (n.a.=-2)**					
	Umgebung und Infrastruktur					
5	Unterbringung in Einsturz gefärdetem Begäude	-2	-2	-2	-2	-2
10	Fehlender physikalischer Schutz von Gebäuden, Türen und Fenstern	0	0	0	0	0
20	Unangemessene oder nachlässige Verwendung von Zutrittskontrollmechanismen					
30	Unstabile Stromversorgung					
31	Unstabile Wasserversorgung					
35	Fehlender Überspannungsschutz					
36	Fehlender Blitzableiter					
37	Fehlende Stichprobenuntersuchung von Personen und KFZ durch den Werksschutzes					
40	Platzierung in einer Umgebung mit erhöhter Überflutungsgefahr	0				
50	Fehlende Feuermelder und Löschvorrichtungen					

Begegnungsplan

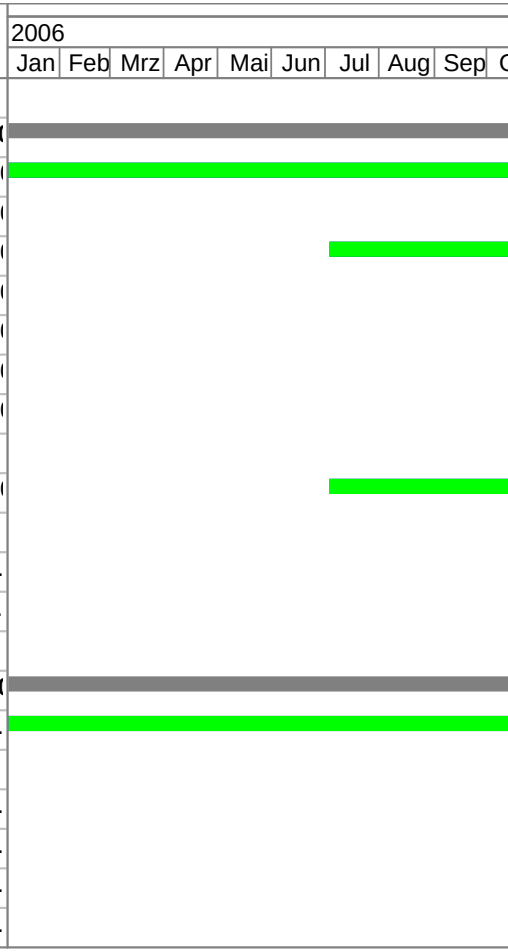
NR	Risiko	Gegenmaßnahme	Status	Risk Acceptance
4	Ungenügende Einweisung oder Schulung in spezielle Aufgabengebiete, Ungenügendes Sicherheitstraining, Fehlende Überwachungsmechanismen 3.7.12 3.8.12 3.7.7	Ein Sensibilisierungskonzept ist erstellt und Maßnahmen zur Sensibilisierung der Benutzer sind angefahren. Weitere Schulungen und Sensibilisierungen stehen noch aus. (User, Admin, Entwickler). Dies geschieht durch Präsentationen, Flyer und Artikel in der Karmann Post. Eine spezielle Sicherheitsschulung für die IT-Beauftragten wurde begonnen und soll vertieft werden.	in Umsetzung, Teile umgesetzt, spezielle Schulungen noch notwendig Sensibilisierung der Anwender wird online geschehen. Quiz zur Motivation/Messung geplant.	
5	Fehlerhafte Bewilligung/Einstellung von Zugriffsrechten 3.7.3	Dieses Organisatorische Thema wird durch die bestehende Org-Richtlinie 170abgedeckt.	umgesetzt	
6	Übertragung von unverschlüsselten Passworten 3.7.5	Im Rahmen der netzwerkbasierten Schwachstellenuntersuchung wurden alle Anmeldedienste, welche unverschlüsselte Passworte entgegennehmen identifiziert. Ein Projekt für deren Ablösung ist in Planung.	Pnr. 659 Ziel: 31.07.2007 Verantwortlich Hr.xy	
7	Ungeschützte Netzwerkverbindungen in öffentliche bzw. nicht vertrauenswürdige Netze, Einwählverbindungen 3.7.11 3.8.1	Die vorhandenen Modems, welche für Fernwartungen an speziellen Systemen implementiert wurden, sind nun durch eine organisatorische Regelung geschützt. Die Modems werden nur noch auf Zuruf des Fernwartenden eingeschaltet. Details sind in der Anweisung zur Modemnutzung festgelegt. Mittelfristig wird Fernwartung nur noch über ENX ermöglicht.	Umgesetzt ENX-Umstellung in Umsetzung	

Maßnahmenmanagement

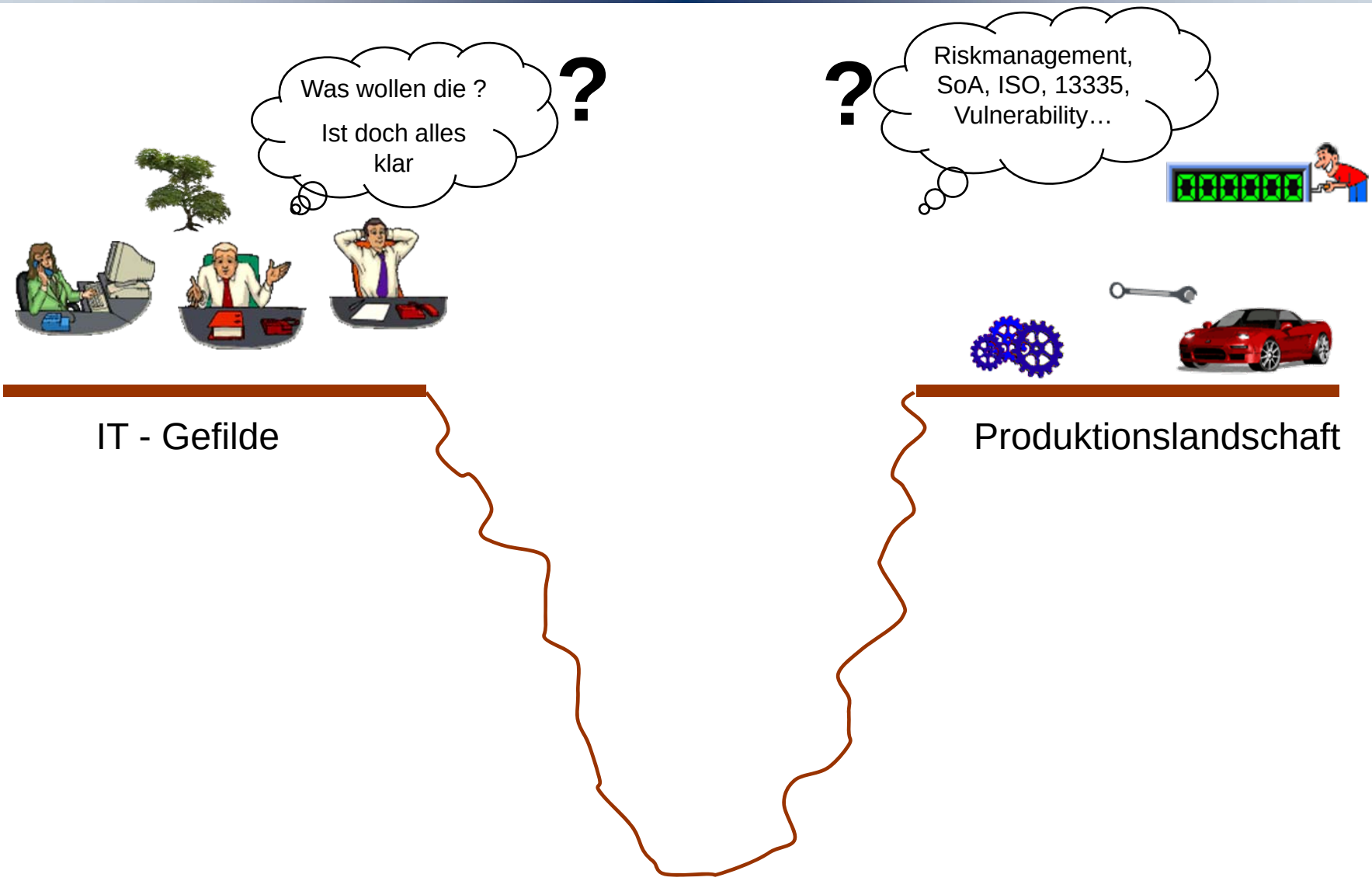
KARMANN
fast forward

1. **Kritische Sicherheitslücken sofort abstellen**
2. **Bündeln der Maßnahmen in Projekte bzw. in ein Programm**
3. **Plan-Do-Ckeck-Act beachten**

Nr.		Statu	Abt.	Verantw	Vorgangsname	Dauer	Anfang	Ende
1								
2					**ISMS**	**565 Tag**	**Mo 02.01.(**	**Fr 29.02.(**
3		F	OF	Ebersba	596 - IT-Sicherheitsmanagement	260 Tag	Mo 02.01.	Fr 29.12.(
4		L	SV	Wessel	594 - EMP - Restumfänge 2006	151 Tag	Fr 01.12.(	Fr 29.06.(
5		Z	BP	Pohlma	611 - SAP - Kompetenz Netzwerk - Konzeption und E	195 Tag	Mo 03.07.	Fr 30.03.(
6		L	SE	Sensse	647 - Aufbau Entwicklungs-und Produktivumgebunge	326 Tag	Fr 01.12.(	Fr 29.02.(
7					Genehmigung	1 Ta	Fr 01.12.(	Fr 01.12.(
8					GoLive Entw.-Umgebung	1 Ta	Fr 15.06.(	Fr 15.06.(
9					GoLive Prod.-Umgebung	1 Ta	Fr 29.02.(	Fr 29.02.(
10		L	IN	Leyman	659 - Passwortrichtlinie für Server	195 Tag	Mi 01.11.	Di 31.07.
11		L	IN	Gurtma	749 - DL-Auswahl für nat. und internat. Datenverbindu	305 Tag	Mo 03.07.	Fr 31.08.(
12		L	SV	Moenke	750 - BSC - Optimierung der Prozesse	142 Tag	Mo 15.01.	Di 31.07.
13		L	OF	Ebersba	808 - Sicherheitszertifizierung - Folgeprojekte	238 Tag	Do 01.02.	Mo 31.12.
14		P	IN	Sporled	814 - AntiVirus Client Update	109 Tag	Fr 01.06.(	Mi 31.10.
15		L	IN	Kruse	827 - Upgrade Software-Firewall-Systeme	109 Tag	Do 01.03.	Di 31.07.
16					**BCM**	**521 Tag**	**Mo 02.01.(**	**Mo 31.12.(**
17		L	OF	Ebersba	599 - Vorbereitung der Betriebsabsicherung (BCM	521 Tag	Mo 02.01.	Mo 31.12.
18		P	SV	Tann	598 - BSC - SLA-Umsetzung	87 Tag	Mo 02.07.	Di 30.10.
19		P	OF	Ebersba	806 - Change Management Prozesse	152 Tag	Fr 01.06.(	Mo 31.12.
20		P	OF	Ebersba	807 - Incident Management - Strategie/Kompeten	152 Tag	Fr 01.06.(	Mo 31.12.
21		P	OF	Ebersba	809 - Configuration-/Patchmanagement	152 Tag	Fr 01.06.(	Mo 31.12.
22		P	OF	Ebersba	810 - Betriebshandbuch und Synchronisation der	152 Tag	Fr 01.06.(	Mo 31.12.

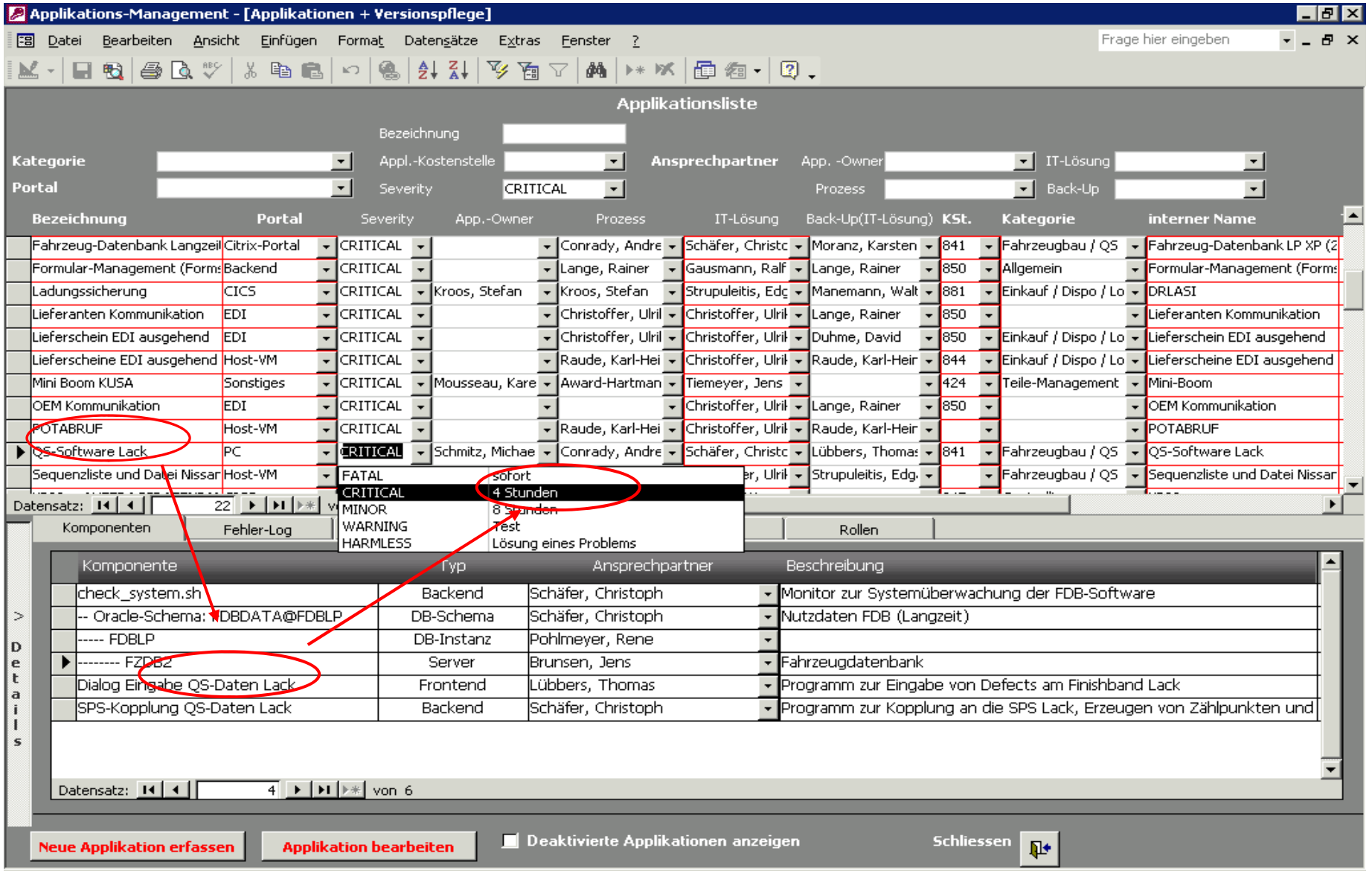


Der Graben zwischen IT und Produktion

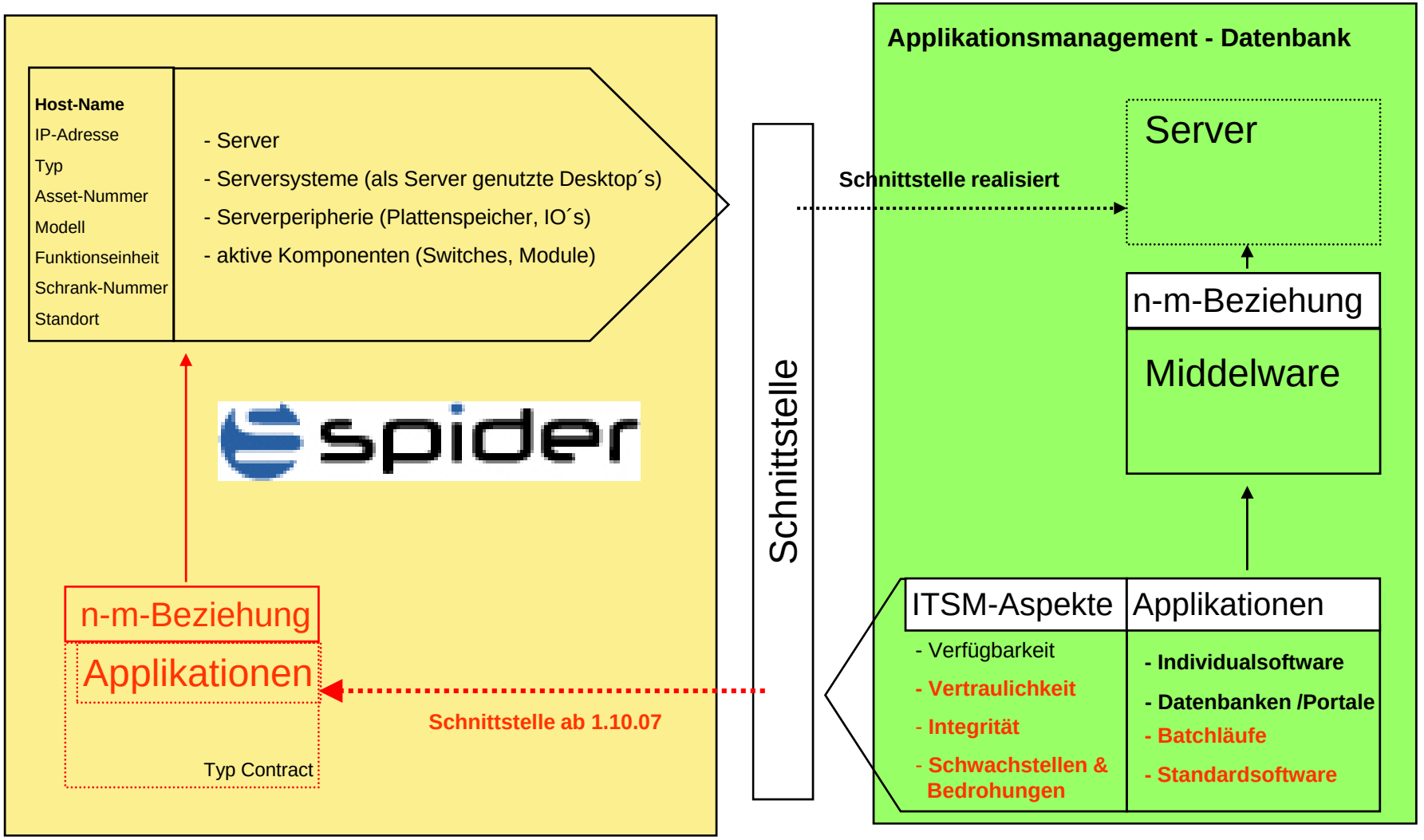


Angewandtes Applikationsmanagement:
Kopplung der SPIDER-Assets mit Karmann-Applikationen

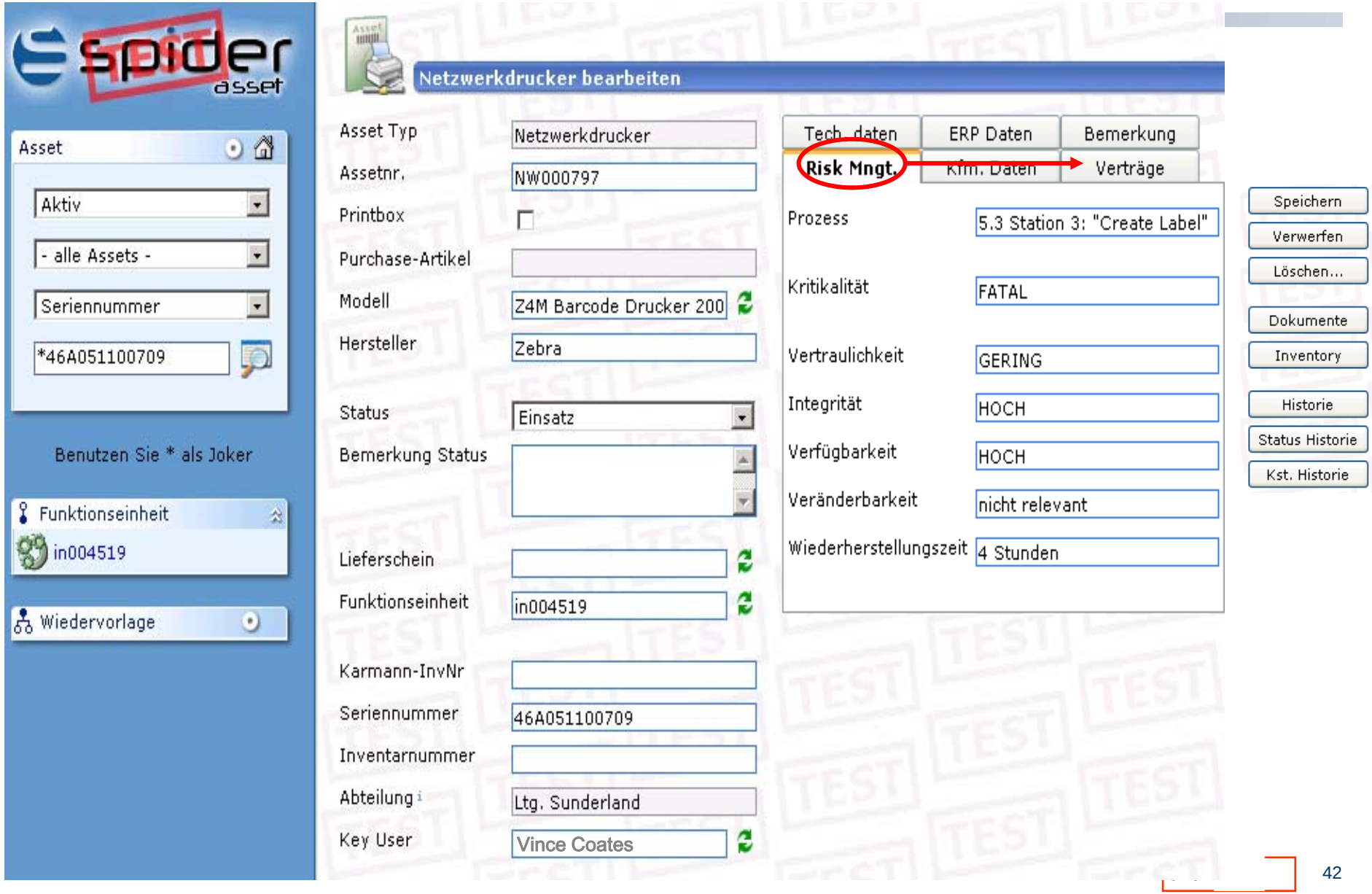
KARMANN
fast forward



Kopplung SPIDER und Applikationsmanagement

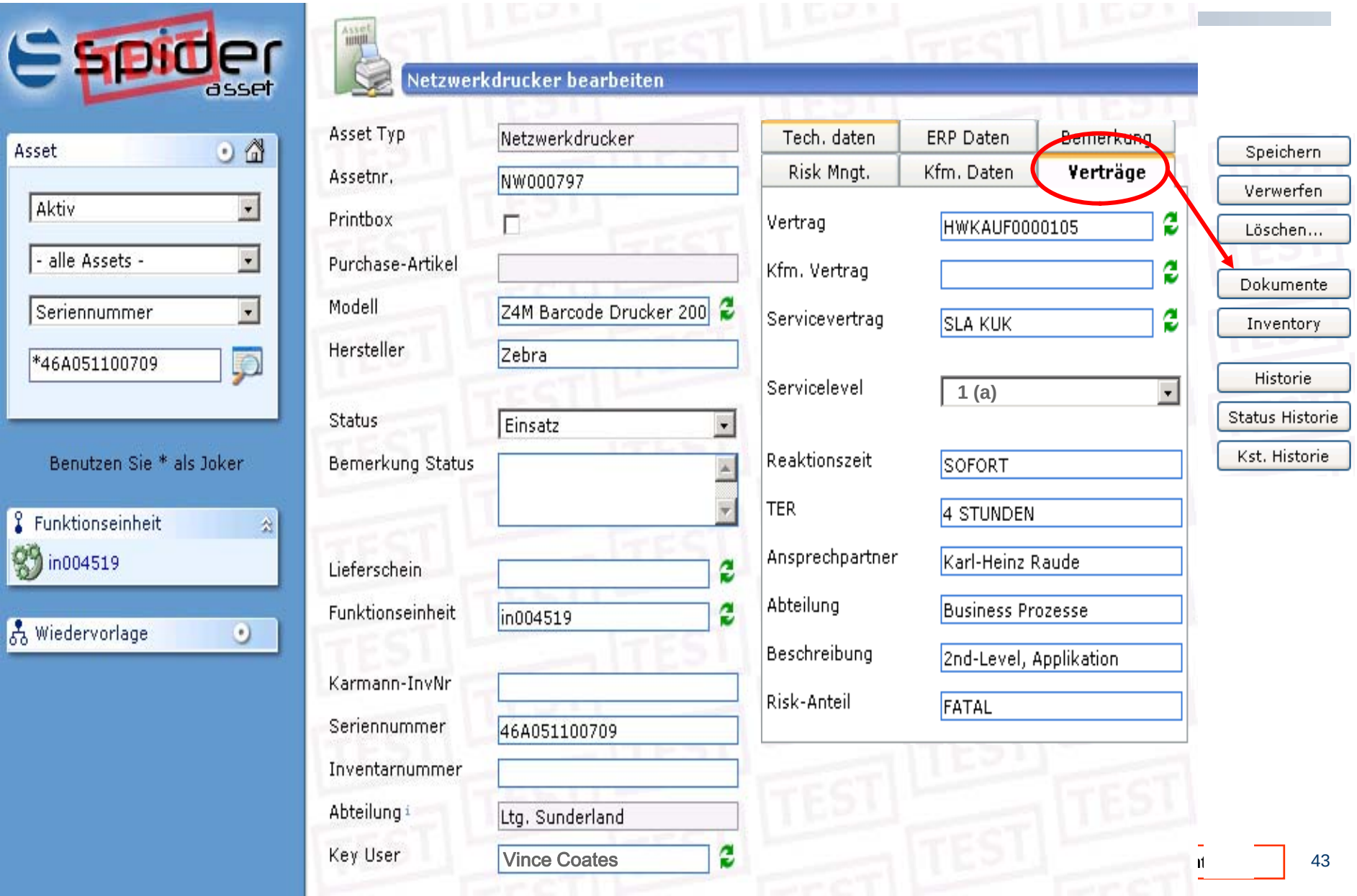


Asset-Kritikalität: Beispiel Labeldrucker Sunderland – RISK



Asset-Kritikalität: Beispiel Labeldrucker Sunderland - SLA

KARMANN
fast forward



Übersicht zugeordneten Dokumenten

Prozessbeschreibung (1)

Dokument	Dateiname	Angelegt am	Bearbeitet am	
5.3. Station 3: Create Label	Microsoft Word - Entwurf_Emergency_Concept_KUKIT__doc.pdf	15.08.2007	15.08.2007	Details

KARMANN

fast forward

5.3 Station 3: "Create Label"

Kurzbezeichnung:	Create Label		
Zugehöriger Geschäftsprozess:	P_03		
Prozessunterstützer:	Supervisor (Vince Coates)		
Akteure/Rolle:	Manufactoring Operator		
Location Code:	15		
Eingesetzte Applikationen:	Acces-Label-Creator		
Eingesetzte Assets: (Changes nachhalten!)	PIII Stand-Alone Desktop	in004519	Print-Applikation KRITISCH! (siehe SLA)
	Dragon-Funk-Scanner	Keine Angabe	
	Zebra LP 2844-Z	46A051100709	KRITISCH! (siehe SLA)
	Ersatz-(Backup) PC		im Zulauf
	Kabel Scanner Backup		im Ersatzteillager
	Kabel-Verlängerung 3m Kabel		im Ersatzteillager
Kurzbeschreibung:	vertraulich		

Input/Vorbedingungen Prozess: Datentechnisch:	vertraulich
Ablauf:	vertraulich 3. Scan: Farbe (Entsprechender Farb-Barcode ist auf der Vorderseite des Schrankes angebracht)
Alternative Abläufe (optional):	Keine alternativen Abläufe möglich
Fehlerfall:	F_1: Ein Scan ist nicht möglich wegen defektem Stand-Alone-PC F_5: Ein Scan ist nicht möglich wegen defektem Scanner F_4: Monitor ist defekt F_7: Zebra Drucker ist defekt
Sofortmaßnahmen:	Solution F_1: Fehler an die WI melden, Verkabelung des Stand-Alone-PC lösen und das Gerät durch das im Schrank befindliche Ersatzgerät ersetzen. Solution F_5: Scanner durch im Schrank befindliches Ersatzgerät ersetzen, Stand-Alone-PC neu booten. vertraulich Solution F_4: WI informieren, Monitor austauschen und Tausch an BSC melden (Lagerort Monitor: Hochregallager) Solution F_7: Fehler an die WI melden, Verkabelung des Zebra-Drucker lösen und das Gerät durch das im Schrank befindliche Ersatzgerät ersetzen. vertraulich
Präventivmassnahmen:	Ersatzgeräte befinden sich im Schrank, nur die Verkabelung und ein Reboot muss neu durchgeführt werden. Verbrauchsmaterial (Labels) befinden sich ebenfalls bereits im Schrank.
Output/Nachbedingungen:	Das Label wurde erzeugt und am Dach angebracht

Vom Management zur Tagesarbeit

KARMANN
fast forward

- **Bei Ausfall der Applikation kann die Hardware sofort zugeordnet werden.**
- **Die Hardware ist nach Risk-Management-Kriterien bewertet und in der Asset-DB visualisiert.**
- **Bei Ausfall einer Hardware können betroffene Prozesse und Applikationen sofort zugeordnet werden.**
- **Der Prozess ist nach Risk-Management-Kriterien bewertet und an der Applikation visualisiert.**
- **Betroffene Prozesse und deren Kritikalität sind dem Asset zugeordnet.**
- **Durch hinterlegte SLA´s, Prozessverantwortliche und 2nd-Level wird der Supportbedarf sofort ersichtlich.**
- **Änderungen sowohl in der App.-DB (z.B. Middleware) oder in der Asset-DB (z.B. Umzug eines virtuellen Servers auf eine andere Hardware) werden durch das Referenzobjekt nachgezogen und täglich automatisch aktualisiert.**

Zusammenfassung / Status Quo bei Karmann

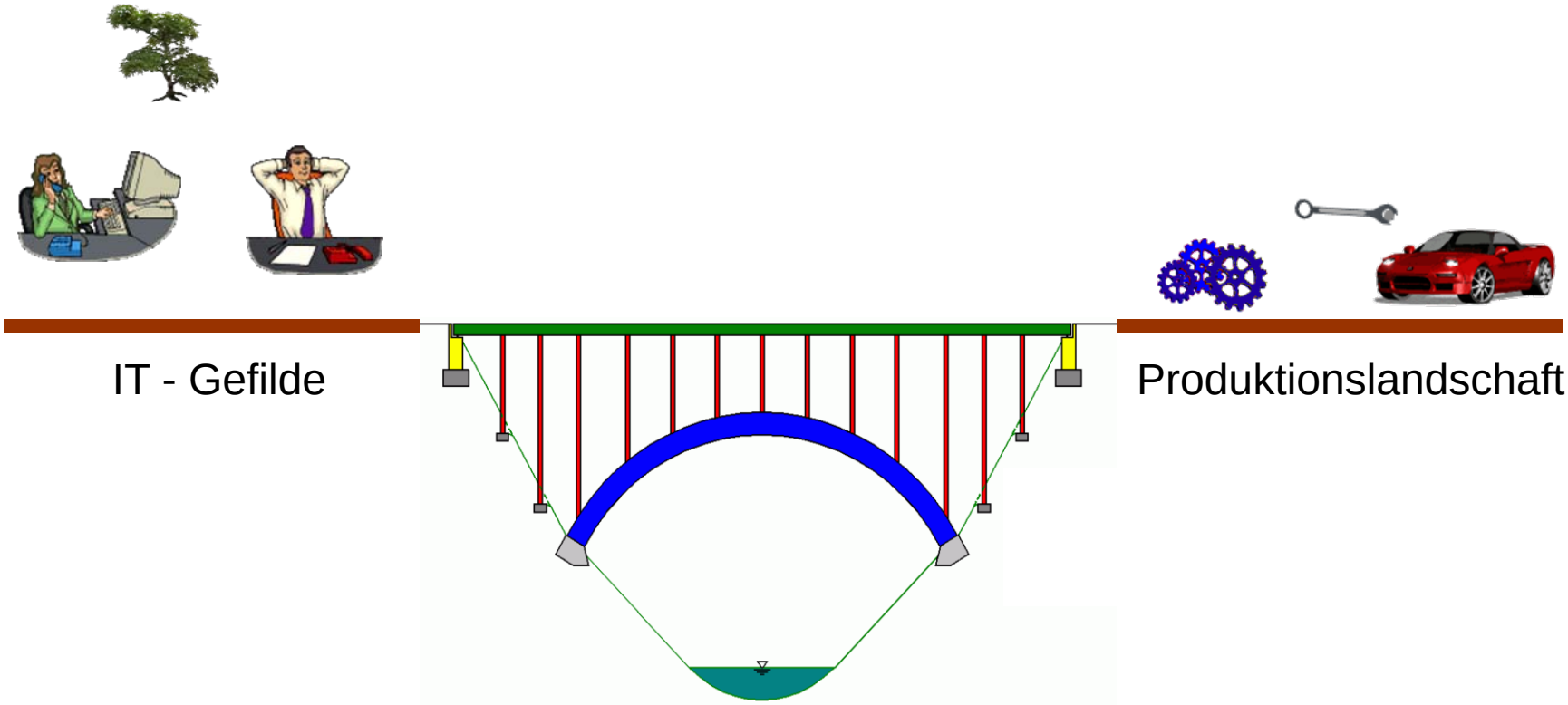
KARMANN
fast forward

Produktionssystem mit Business verbunden

Prozesse, Applikationen und Assets sind inkl. Risikoeinschätzung logisch in einer zentralen Datenbank dokumentiert

Business Continuity Management eingeführt

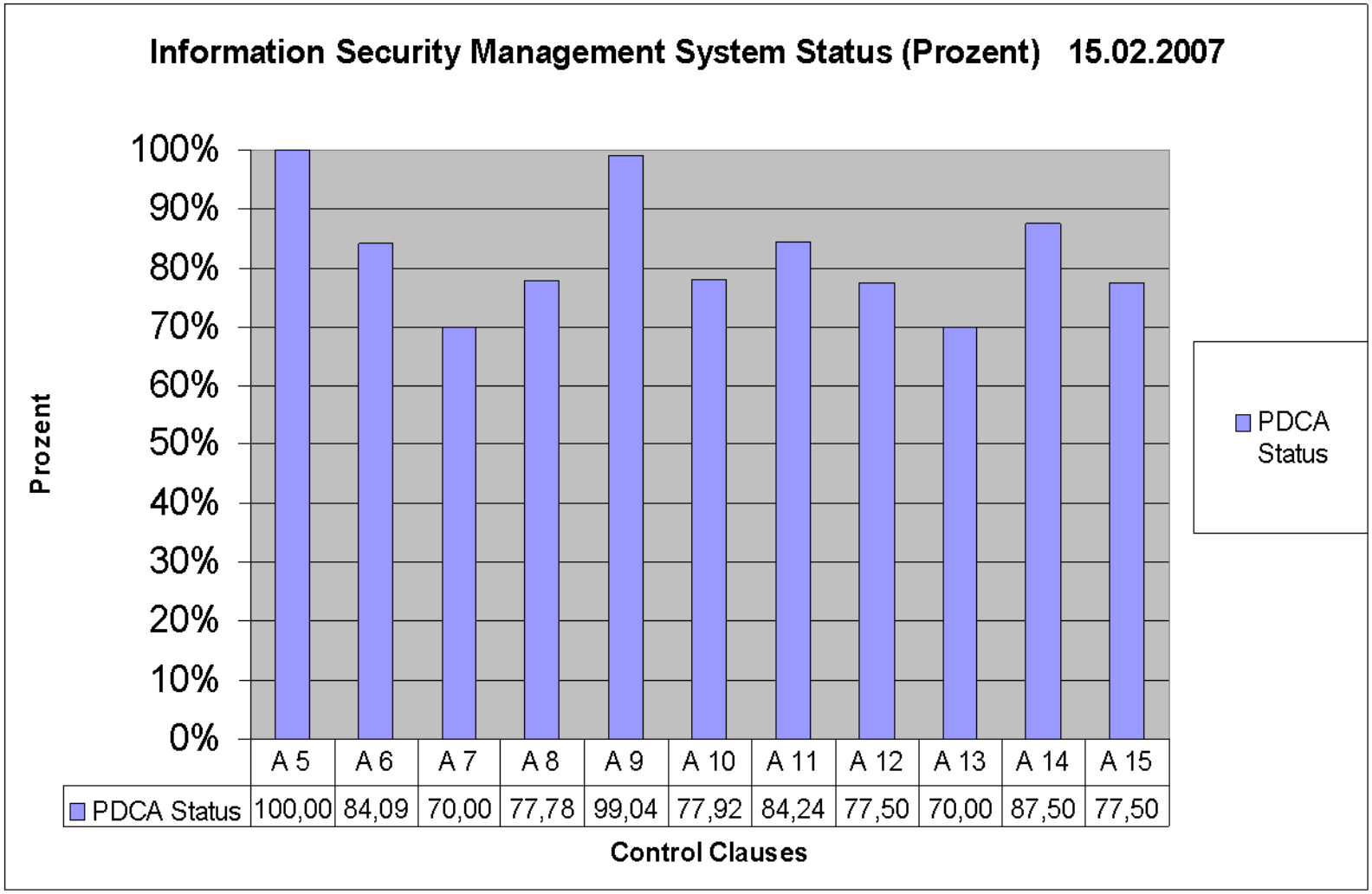
Produktions- und Büro-IT mit Risk Management verbunden



Stand März 2007 (Zertifizierung)

474 Fragen zu 132 Controls

Produktsicherheit: 96 Fragen



Danke

Vielen Dank für Ihre Aufmerksamkeit !