

Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten

Bernd Donabauer



**Workshop
IT-Sicherheitspflicht als Chance
26.04.2007
CAST e.V.
Darmstadt**

COMPETENCE CENTER FOR
APPLIED SECURITY TECHNOLOGY



CAST

Bernd Donabauer

IT Management and Resources

Rodauer Str. 20
64372 Ober-Ramstadt
Germany

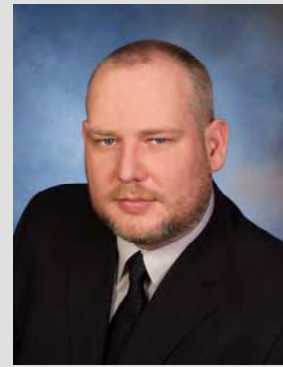
fon: (+49) 06154 575264

fax: (+49) 06154 575265

mobile number on request

Mail: info@it-mare.com

www.it-mare.com

**Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten**

Die IT-Infrastruktur eines Unternehmens ist längst ein unverzichtbares Mittel für die betriebliche Leistungserstellung. Bei einer Störung der Verfügbarkeit oder mangelnder Funktionalität sind diese in ihrer Existenz bedroht.

So verwundert es nicht, dass in den letzten Jahren eine Vielzahl von Regularien für den Bereich Informationssicherheit entwickelt wurden.

Dennoch wird die normative Kraft von Gesetzen, Normen und Standards der Informationssicherheit von vielen Fachleuten überschätzt. In der Praxis fehlt es den Unternehmen an einem Anreiz oder schlicht an den Ressourcen diese anzuwenden.

Daher kommt es wesentlich darauf an, die vorhandenen Geschäftsprozesse in einer vorgelagerten Projektphase auf die Einführung neuer Standards vorzubereiten.

Unter welchen Voraussetzungen Normen und Standards erfolgreich eine Anwendung finden und Unternehmen Vorteile aus strategischen Investitionen in die Informationssicherheit generieren können, beschreibt aus der Sicht eines aktiven Projektleiters der praxisorientierte Vortrag.

Certified Examiner under
ISO/IEC 17024:2003Designated by Cert-IT. According
to the Regulations of the Document
No. 2003-1009.ITIL: Foundation
Certificate in IT Service
ManagementZertifiziert by TÜV Akademie.
According to the Regulations of the
Document No. 0402#310388944**Werdegang**

Berufliche Ausbildung, Studium der Soziologie, BWL und Recht an der TU-Darmstadt.

5 Jahre Berufserfahrung als Baustellenleiter.

12 Jahre Berufserfahrung als Mitarbeiter und Projektleiter in verschiedenen IT Projekten. Davon 4 Jahre als Leiter Marketing und Human Resources in einem IT-Unternehmen.

Member of

**Aktivitäten**

Mitglied des Förderpreiskomitees des (CAST e.V.) seit 2000.

Ehrenamtlicher Prüfer der IHK Darmstadt.

Vertreter der BITKOM und der IG Metall bei Fachveranstaltungen.

Mitglied in verschiedenen ISO-Normungsgremien.

Partnership in
TECHNISCHE
UNIVERSITÄT
DARMSTADT

Die kommentierte Fassung steht Ihnen auf dem CAST-Mitgliederbereich oder unter www.it-mare.com zur Verfügung.

Quellennachweis:

Donabauer, Bernd: Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten. Kommentierte Fassung. Vortrag zum Workshop des CAST e.V. IT-Sicherheitspflicht als Chance. 26.04.2007, CAST e.V., Darmstadt. Veröffentlicht unter www.it-mare.com/sources/070426_vortrag_cast.pdf, Stand 26.04.2007.

Erklärung der Kommentarsymbole

Lieber Leser,

wieder einmal hat mich eine CAST-Veranstaltung zu einer Idee angeregt. Der CAST e.V. stellt Inhabern eines CAST-Leistungspaketes die Vorträge aus den CAST-Workshops kostenlos als Datei zur Verfügung. Dies ist auch ein für mich wertvolles Fach-Archiv, dass ich rege nutze. Für einen Referenten stellt sich im Sinne der bestmöglichen Dienstleistung gegenüber dem Kunden ein grundsätzliches Problem. Optimiert er seine Unterlagen für den Lernertrag während des Vortrages, ist es im späteren Studium der Unterlagen schwer jeden Gedankengang in vollem Umfang nachzuvollziehen – es fehlt der mündliche Beitrag. Optimiert er hingegen die Unterlagen für das spätere Studium, ist der Lernertrag während des Vortrages gefährdet, weil die Vortragsfolien mit zusätzlichen Detailinformationen überbordnet werden.

Als Ergebnis meiner Überlegung finden Sie nun hier ein kommentierte PDF-Version des Vortrages. So können die Folien, optimiert für den Vortrag, im Original erhalten und dennoch mit Detailinformationen, wie Kommentare des Referenten, Zusatzinformationen, Quellennachweisen und weiterführenden Links versehen werden.

Mit den besten Grüßen

Bernd Donabauer

Erklärung der Kommentarsymbole

Nachfolgend finden Sie eine Erklärung der verschiedenen Kommentarsymbole. Sie können die Kommentare einblenden, indem Sie mit dem Mauszeiger darauf deuten. Mit einem einfachen Linksklick werden diese geöffnet, so dass Sie eigene Anmerkungen hinzu fügen oder den Kommentartext über die Zwischenablage kopieren können.

- **Inhaltlicher Kommentar des Autors**
- **Ergänzende Information**
- **Quellennachweis**
- **Weiterführender Link**



„Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten“

Workshop IT-Sicherheitspflicht als Chance

26.04.2007, CAST e.V., Darmstadt

Bernd Donabauer

Vorstellung des Referenten

Der Referent

- **Bernd Donabauer**
IT Management and Resources
- **Seit 1994 Tätigkeit als freier Consulter in verschiedenen IT-Projekten mit dem Schwerpunkt Informationssicherheit**
- **12 Jahre Berufserfahrung als Mitarbeiter und Projektleiter in verschiedenen IT Projekten im In- und Ausland**
- **Davon 4 Jahre als Leiter Marketing und Human Resources in einem IT-Unternehmen**
- **ITIL zertifiziert**
- **Master Examiner under ISO 17024:2003**
- **Mitglied in verschiedenen Normierungsgremien**
- **Vertreter von BITKOM und IG Metall**
- **Aktives Mitglied des CAST e.V. (CAST-Forum) seit dem Jahr 2000**

Partner

Organisationen und Unternehmen

„Die Informationstechnologie ist eine betriebliche Querschnittsfunktion. Die Entwicklung und Einführung von sicheren und effizienten IT-Prozessen erfordert das Zusammenführen verschiedenster Experten in einem schlagkräftigen Team.“

- Technische Universität Darmstadt
Public Privat Partnership
- Cert-IT GmbH
Akkreditierte Personalzertifizierungsstelle
- CAST e.V.
Kompetenznetzwerk IT Sicherheit



Agenda

Vorstellung

Teil I

Normative Kraft oder Papiertiger? Gesetze, Normen und Standards aus Sicht der Unternehmen

Teil II

Entscheidungsgründe: Das Primat der Wirtschaftlichkeit von Informationssicherheitsprojekten

Teil III

Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten

Teil IV

Die Bedeutung des Projektmarketing am Beispiel eines Kredit-Ratings nach Basel II

Ausblicke



Kontakt

Teil I

Normative Kraft oder Papiertiger? Gesetze, Normen und Standards aus Sicht der Unternehmen






Gesetze Normen und Standards

Begriffsdefinition und Wirkungsweisen: Gesetze

- Von einem staatlichen Organ erlassene, verbindliche Rechtsnormen, die in eine Hierarchie eingebunden sind
- I.a.R. mit Sanktionen bewehrt
- Verfolgungsdruck durch Exekutive
- Gesetze sind aus Sicht der Unternehmen das Rahmenwerk des wirtschaftlichen Handelns
- In hochentwickelten, international vernetzten Volkswirtschaften können sie nicht, direkt oder indirekt wirken
- Sie wirken nicht, wenn der Verfolgungsdruck fehlt 
- Direkt durch Sanktionen bei nicht konformen Handeln
- Indirekt als Instrument der Marktöffnung oder Marktschließung 

Gesetze Normen und Standards

Begriffsdefinition und Wirkungsweisen: Normen und Standards

- Normen sind nur solche Standards, die durch nationale oder Internationale Normierungsorganisationen veröffentlicht wurden 
- Nationale DIN (Deutsches Institut für Normung), Internationale ISO (International Organization for Standardization), u.w. 
- Sie beinhalten die unabhängige Zertifizierung einer Methode, eines Produktes, einer Organisation oder einer Person
- ITIL/ ISO 20000, BSI Standard 100-1/ ISO 27001, CISSP/ ISO 17024 
- Entscheidend bei der privatwirtschaftlich geregelten Umsetzung und Anwendung ist die organisatorische, wirtschaftliche und politische Trennung der akkreditierten Organisationen und Personen 
- Normen und Zertifizierungen sind aus Sicht der Unternehmen Prüfungsinstrumente der Qualität
- Primäres Ziel ist die internationale Vergleichbarkeit
- Sie bewirken für die Unternehmen eine Marktöffnung oder eine Marktschließung 

Gesetze Normen und Standards

Beispiel Normenumsetzung in der Personalzertifizierung IT Security Coordinator/ ISO 17024



Gesetze Normen und Standards

Wirkungsbereiche – Quantitative Schlaglichter

- **Anzahl der Unternehmen in Deutschland mit 1-49 Mitarbeitern**
1.943.716
- **Anzahl der Unternehmen in Deutschland mit 50-499 Mitarbeitern**
79.754
- **Anzahl der Unternehmen mit 500 und mehr Mitarbeitern**
4.689

Quelle: Bundesagentur für Arbeit, Stand 30.06.2006



- **Anzahl der Unternehmen mit BSI „ISO 27001-Zertifikat auf der Basis von IT-Grundschutz“**
8

Quelle: Bundesamt für Sicherheit in der Informationstechnik, Stand 19.04.2007



Gesetze Normen und Standards

Wirkungsbereiche – Qualitative Schlaglichter

- Auf viele Unternehmen treffen Gesetze aufgrund ihrer Rechtsform oder ihres Tätigkeitsfeldes nicht zu
- Die Risiken bei Missachtung von Gesetzen sind für persönlich haftende Unternehmer nur einige von vielen Risiken
- Der Verfolgungsdruck ist bei verschiedenen Gesetzen quasi nicht vorhanden
- Für lokal handelnde Unternehmen sind Normen oft genug ohne jede Bedeutung 
- Für viele Unternehmen entsteht kein Wettbewerbsvorteil durch die Anwendung von Standards 
- Langfristig sind wir alle tot: Unternehmen sind aufgrund fehlenden Kapitals nicht in der Lage strategische Investitionen in die Informationssicherheit zu tätigen
- Unternehmen sind nicht in der Lage die notwendigen Humanressourcen zu entwickeln oder am Markt zu akquirieren

Teil II

**Entscheidungsgründe:
Das Primat der Wirtschaftlichkeit von
Informationssicherheitsprojekten**

Entscheidungsgründe

„Das Ziel eines jeden Informationssicherheitsmanagements ist es, die für die Leistungserstellung notwendigen Prozesse zu gewährleisten und zu optimieren“

Bernd Donabauer, 2002



Entscheidungsgründe

Technik	Steigende Komplexität Steigendes Projektvolumen Unternehmensweite Integration Zunehmende Automatisierung Öffnung in unsichere Netze Dynamische Entwicklung der Gefahrenpotentiale
Organisation	Globalisierung der Geschäftstätigkeit Unternehmensübergreifende Produktion Neue Arbeitsformen Abhängigkeit bei der Leistungserstellung Abhängigkeit von der Verfügbarkeit Dynamik der Märkte IT als Wettbewerbsvorteil
Recht	Steigende Anforderungen des Gesetzgebers KonTraG BASEL II Datenschutz Informationssicherheit Lizenz-, Wettbewerbs- und Urheberrecht

Quelle: Eigene Darstellung.

Entscheidungsgründe

Entscheidungsgründe in der Praxis

- **Der Impact**
Man bezahlt mindestens einmal für Informationssicherheit: Davor oder danach
- **Die Erweiterung der Geschäftsfelder** 
War da nicht noch was?
- **Die Prozessoptimierung** 
Das Kosten- Nutzenverhältnis für die IT Services steht in keinem Verhältnis mehr
- **Der Marktzugang**
Ohne Norm-Zertifizierung kann ich nicht mal mehr mit Zitronen handeln

In der Praxis zählt der Nutzen von Normen und Standards nur im Hinblick auf die Anwendbarkeit zur Optimierung der Leistungserstellung. Die Frage einer abschließenden Zertifizierung ist ergebnisoffen und fast immer mit der Frage des Marktzuganges verbunden

Teil III

Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten

Die Umsetzung im Praxisprojekt

Praxisorientierte Kategorien der IT-Systeme



- **Primäre Systeme:**
Technische Ressourcen zur Abbildung der Geschäftsprozesse über IT-Services in der Wertschöpfungskette
- **Sekundäre Systeme:**
Technische Ressourcen zur Absicherung der Funktion der primären Systeme, jedoch ohne originäre Aufgabe bei der Wertschöpfung
- **Tertiäre Systeme:**
Organisationsstrukturen und Ressourcen, die für den Betrieb, die Wartung und die Erweiterung verantwortlich sind

Die Umsetzung im Praxisprojekt


Praxisorientierte Kategorien der IT-Systeme

Management	Organisation, Personalentwicklung, Recht, Systemdokumentation, Audit, Hard- und Softwaremanagement, Budget-Planung, Projektmanagement, Riskmanagement, Notfallkonzepte, Datenschutz
Infrastruktur	Passive und aktive Netzkomponenten, Versorgung, Serverraum, Arbeitsplatz
IT-Systeme	Server- Client-Hardware, Server- Client-OS, TK-Anlage, mobile Geräte
Netze	Netzmodell, heterogene Netze, verteilte Standorte, Anbindung, Netz- und Systemmanagement, Backup-Geräte, Backup-Systeme, Test-Systeme
Anwendungen	Serveranwendungen, Clientanwendungen, Internetanwendungen, Anwenderdaten in Dateiform, programmgebundene Anwenderdaten (z.B. Database)
Sicherungssysteme	Firewall, AV-Software, SPAM-Filter, IDS, VPN, Verschlüsselung, Signatur, Biometrie, DRS, Gebäudesicherheit
Tertiäre Systeme	Primäre Systeme Sekundäre Systeme

Quelle: Eigene Darstellung.

Die Umsetzung im Praxisprojekt

Schlussfolgerungen

- Jede der drei Kategorien von Systemen ist für die Abbildung der betrieblichen Prozesse notwendig und daher als Produktivsystem Teil der Wertschöpfung 
- Jedes primäre System benötigt eine Absicherung durch sekundäre Systeme
- Jedes primäre und sekundäre System benötigt eine Absicherung durch tertiäre Systeme
- Hieraus entstehen erhebliche Folgekosten und ggf. nicht zu schließende Investitionslücken

Die Umsetzung im Praxisprojekt





Forderungen

- **Genaue Erfassung, Bewertung und Optimierung der betrieblichen Kernprozesse**
- **Eliminierung der für die Wertschöpfung irrelevanten Prozesse**
- **Genaue Erfassung, Bewertung und Optimierung der Abbildung der Geschäftsprozesse auf den primären Systemen**
- **Eliminierung der für die Abbildung der betrieblichen Kernprozesse irrelevanten Systeme**
- **Genaue Erfassung, Bewertung und Optimierung sekundären und tertiären Systeme**
- **Eliminierung der überflüssig gewordenen sekundären und tertiären Systeme**
- **Re-Investitionen der frei gewordenen Ressourcen in die vorhandenen Systeme**
- **Ziel: Verringerung der Komplexität**
- **Methode: Qualitätsmanagement der IT Services**



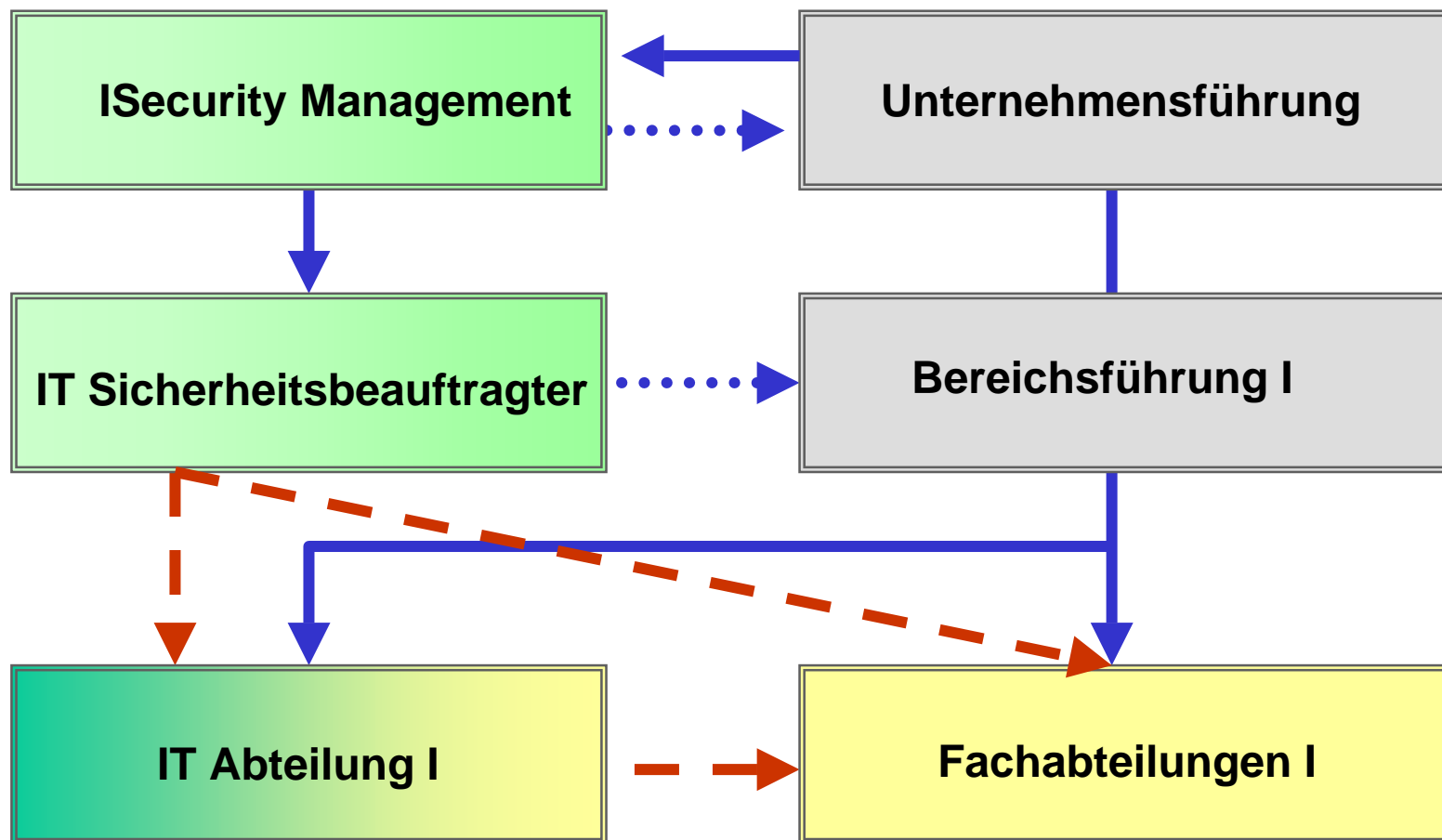
Die Umsetzung im Praxisprojekt

Organisatorische Voraussetzungen

- Politische, organisatorische und wirtschaftliche Trennung der Aufgaben und der Verantwortung 
- Genaue Zuweisung der Aufgaben und Verantwortung an einen bestimmten Besitzer (TEAM: Toll, Ein Anderer Macht es)
- Organisatorische und disziplinarische Vollmachten für die Besitzer einer Aufgabe oder einer Verantwortung 
- Sonderfall: Task Force nach Impact – Notwendigkeit von „Notstandsgesetzen“, mit internen Ressourcen kaum zu lösen 
- Ressourcenmanagement: Der Faktor Humanressource IST der begrenzende Faktor
- Eine besondere Bedeutung kommt daher der Beschaffung der Humanressourcen zu
- Bei externer Beratung bei der Einführung und anschließender Eigenbetreuung im Regelbetrieb, die verwendete Methodik des Wissenstransfers 

Die Umsetzung im Praxisprojekt

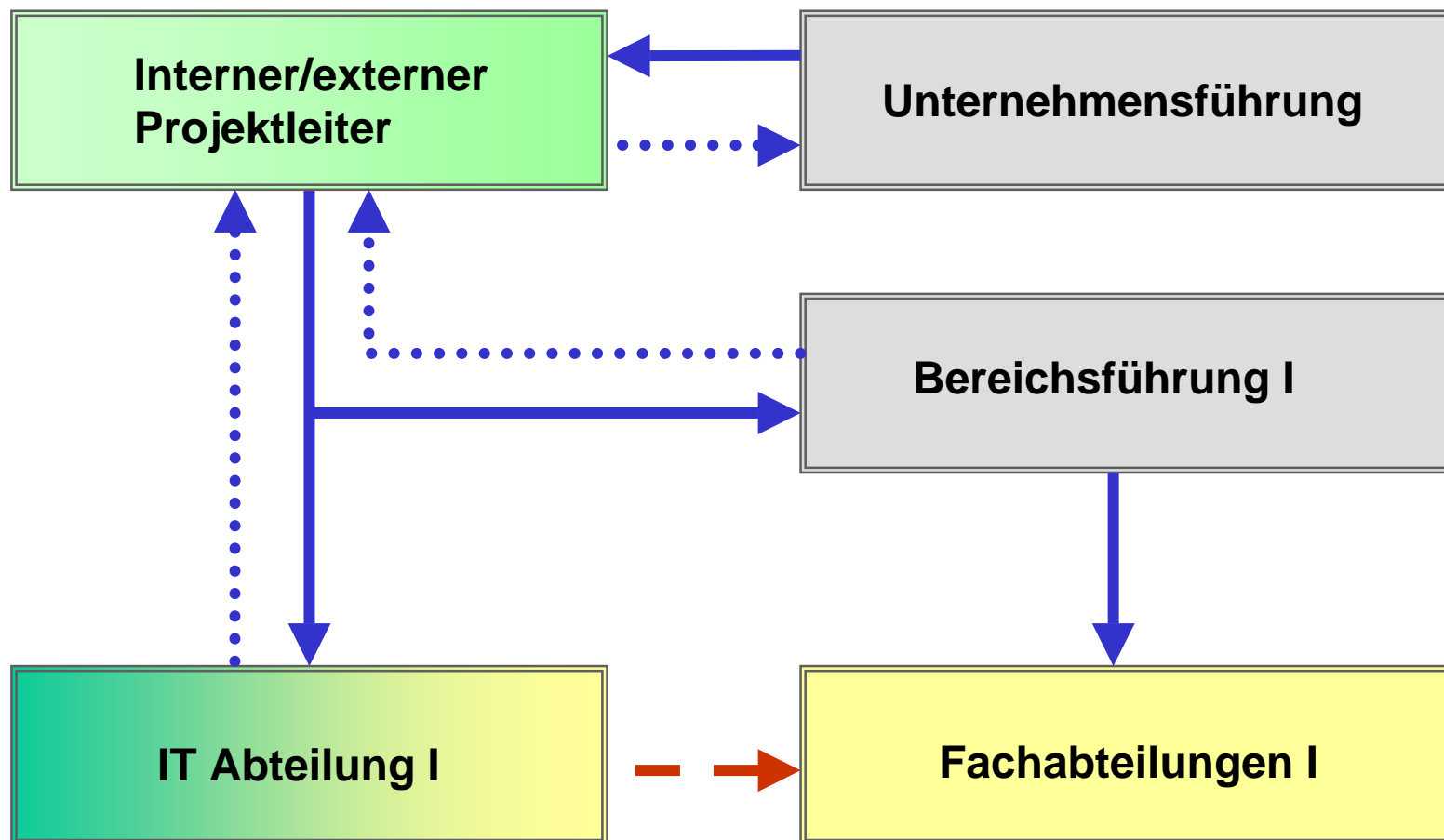
Organisationsvoraussetzungen: Regelbetrieb



- Beratende Funktion
- - - Funktionale Weisungsbefugnisse und fachliche Verantwortung
- Disziplinarische Weisungsbefugnisse und Gesamtverantwortung

Die Umsetzung im Praxisprojekt

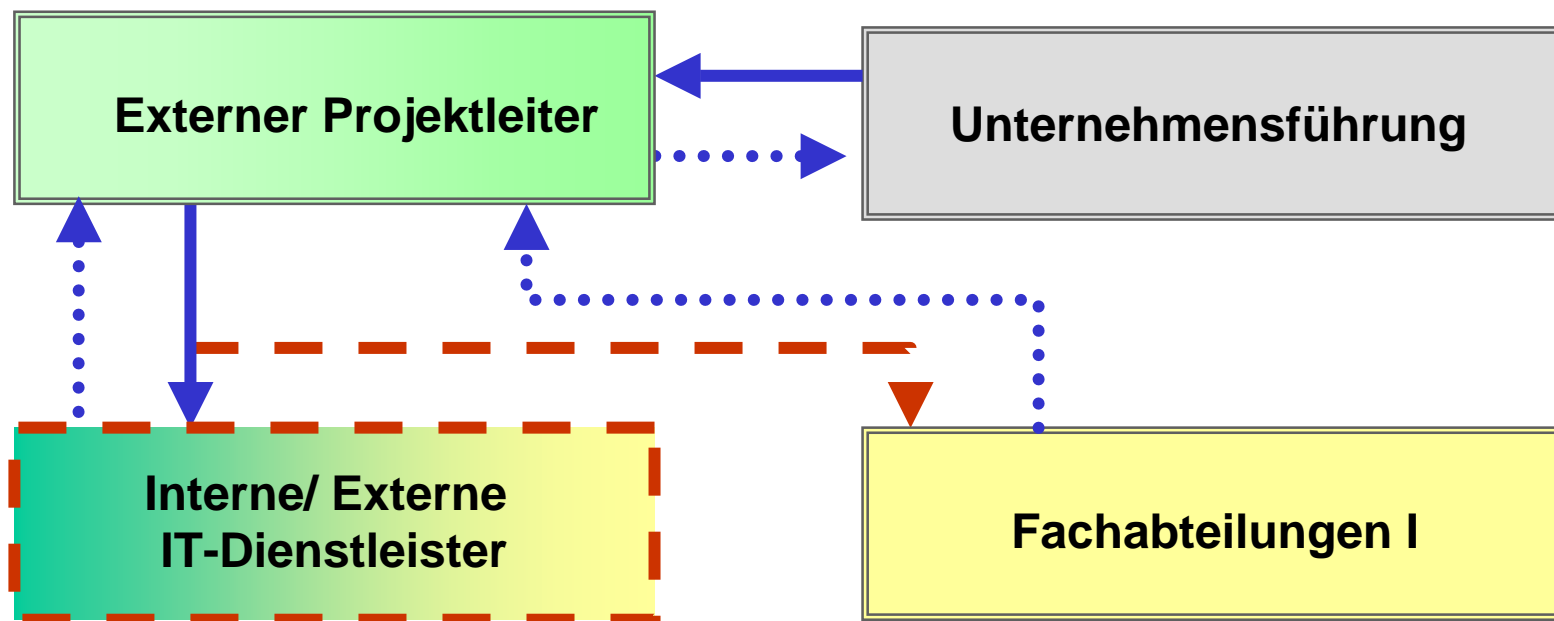
Organisationsvoraussetzungen: Einführung



- Beratende Funktion
- — Funktionale Weisungsbefugnisse und fachliche Verantwortung
- Disziplinarische Weisungsbefugnisse und Gesamtverantwortung

Die Umsetzung im Praxisprojekt

Organisationsvoraussetzungen: Task Force nach Impact



- Beratende Funktion
- - - Fachliche Verantwortung
- — — — — Umfassende Weisungsbefugnisse und Gesamtverantwortung

Die Umsetzung im Praxisprojekt

Top Down-Analyse der Geschäftsprozesse und IT-Services: Methodik

- ITIL orientiert bedeutet „Sicht der IT-Services statt der IT-Server“
- Die erweiterte Delphi-Methode: Gerichtete schriftliche und mündliche Befragung der im Unternehmen beteiligten Akteure (Fragebogen, Interview, Risk-Workshop), insbesondere der verantwortlichen Geschäftsführung
- Analyse der Marktsituation und der Marktpartner (Kunden, Zulieferer, interne und externe Partner)
- Analyse der buchhalterischen Daten (Umsatz, Gewinn, Investitionsquote, Bildungsinvestitionen, Alterungsgrad der technischen Infrastruktur, ...)
- Analyse der Dokumentationen der Geschäftsprozesse (Prozessbeschreibungen, Aufgaben der Mitarbeiter, ...)
- Analyse der IT-Dokumentationen (Technische Dokumentationen, Verträge, SLA, Tätigkeitsnachweise, Lizenzsituation, ...)
- Stichpunktartige Überprüfung (Ansicht vor Ort, verdeckte Ermittlung, ...)

Die Umsetzung im Praxisprojekt




Top Down-Analyse der Geschäftsprozesse und IT-Services

- Definition der Geschäftsprozesse in der Wertschöpfungskette
- Definition der IT-Services, die die Geschäftsprozesse abbilden
- Zuordnung der IT-Services zu den entsprechenden primären IT-Systemen
- Zuordnung der sekundären Sicherheitssysteme zu den primären Systemen der IT-Services
- Zuordnung der primären und sekundären IT-Systeme zu den tertiären Organisations- und Ressourcen-Strukturen des IT-Managements

Eine Analyse, ist sie auch noch so Normenkonform, genügt nicht – Sie müssen die richtigen Entscheidungen treffen und auch bereit sein, diese gegen massive Widerstände durchzusetzen 





Die Umsetzung im Praxisprojekt

Entwicklung von alternativen Umsetzungsszenarien

- Outsourcing vs. Insourcing der Humanressourcen 
- Outsourcing vs. Insourcing der technischen Infrastruktur
- ASP-Varianten 
- Entscheidungsgrundlagen
 - Kann ich die notwendigen Investitionen tätigen
 - Kann ich die Humanressourcen aufbauen
 - Kann ich die Humanressourcen beschaffen
 - Ist mein Standort geeignet 
 - ...

Die Umsetzung im Praxisprojekt

Schlüsselsituationen

- Stabilisierung der vorhandenen Systeme und Organisationsstrukturen 
- Konflikte bei der Analyse des Ist-Standes und der Definition des Soll-Konzeptes 
- Kommunikation während der Umsetzung 
- Vermarktung der Ergebnisse 

Teil IV

Die Bedeutung des Projektmarketing am Beispiel eines Kredit-Ratings nach Basel II

Projektmarketing

„Marketing bedeutet .. Planung, Koordination und Kontrolle aller auf die aktuellen und potentiellen Märkte ausgerichteten Unternehmensaktivitäten. Durch eine dauerhafte Befriedigung der Kundenbedürfnisse sollen die Unternehmungsziele im gesamtwirtschaftlichen Güterversorgungsprozeß verwirklicht werden.“

Meffert, Heribert (1986): Marketing. S. 31 (Schreibweise wie im Original).

Projektmarketing

Basel II beim Kreditkunden

- Ist vor allem ein Mittel der Kreditrationierung
- Soll mittels eines Rating-Verfahrens das Kreditrisiko bestimmen
- Das ermittelte Risiko entscheidet über die Vergabe und über die Höhe der Kreditzinsen
- Unterscheidet zwischen harten und weichen Ratingfaktoren
- Die Informationssicherheit fällt unter die operationellen Risiken bzw. weichen Rating-Faktoren
- Wird beim Endkunden i.a.R. von Kreditsachbearbeitern durchgeführt
- Diese haben kaum bis keine IT-Kompetenz und halten sich im Zweifelsfall an die harten Rating-Faktoren
- Ohne pro-aktive und zielgruppenspezifisches Projektmarketing ist keine Verbesserung des Ratings zu erreichen
- Und selbst dann, deckt der Nutzen nicht die Kosten
- Kredit-Rating nach Basel II ist daher auch kein primäres Entscheidungskriterium für Investitionen in die Informationssicherheit

Projektmarketing

Harte Rating-Faktoren

- Vermögenslage
 - Z.B. Eigenkapitalquote
 - Selbstfinanzierungsgrad
- Finanzlage
 - Z.B. Cash Flow
 - Schuldentilgungsdauer
- Ertragslage
 - Z.B. Jahresüberschuss
 - Umsatzrendite

Projektmarketing

Weiche Rating-Faktoren

- **Marktumfeld**
 - **Z.B. Marktlage**
 - **Produktqualität**
- **Management**
 - **Z.B. Führungsstruktur**
 - **Qualifikation**
 - **Krisenplanung**
- **Informationssicherheit wird als Rating-Faktor nicht einmal explizit genannt. Umso entscheidender ist die pro-aktive Eigendarstellung der Bedeutung**

Ausblicke

Entwicklungen

- Das technische Modell der IT-Sicherheit wird zunehmend von dem betriebswirtschaftlichen Modell der Informationssicherheit abgelöst
- Im Rahmen der Internationalisierung der Produktion an verteilten Standorten und der Professionalisierung des Informationsmanagements gewinnt die Arbeit nach Standards an Bedeutung
- Zertifizierungen nach Normen sind weiterhin vor allem ein Instrument der Markterschließung
- Sie haben daher auch langfristig nur einen Wert, wenn sie eine internationale Gültigkeit besitzen
- Insbesondere unter der Berücksichtigung des Zwangs zur Re-Zertifizierung
- Nationale „Zertifizierungs-Labels“ sind eine Sackgasse und letztlich ohne Existenzberechtigung
- Vereinfachte Anwendung und Integration verschiedener Standards
- Aufeinander aufbauende Zertifizierungsmodelle
- Skalierbare Softwaretools mit gemeinsamer Datengrundlage



Ausblicke

Unternehmensprozesse

Qualitätsmanagement / ISO 9000f

Servicemanagement / ISO 20000, ITIL Framework

Informationssicherheitsmanagement/ ISO 27001f, ISMS

Datenschutz

IT-Sicherheit / BSI Standard 102 Framework

Humanressourcen / ISO 17024, CISSP, IT Security Coordinator

Kontakt

Bernd Donabauer

IT Management and Resources

Rodauer Str. 20

64372 Ober-Ramstadt

Tel.: 06154 575264

Fax.: 06154 575265

Mobil: Auf Anfrage

mailto: info@it-mare.com

www.it-mare.com

Die kommentierte Fassung steht Ihnen auf dem CAST-Mitgliederbereich oder unter www.it-mare.com zur Verfügung.

Zitierweise:

Donabauer, Bernd: Den Erfolgsfaktor Informationssicherheit in der Praxis gestalten. Kommentierte Fassung. Vortrag zum Workshop des CAST e.V. IT-Sicherheitspflicht als Chance. 26.04.2007, CAST e.V., Darmstadt. Veröffentlicht unter www.it-mare.com/sources/070426_vortrag_cast.pdf, Stand 26.04.2007.