

# KRISENMANAGEMENT IN IT PROJEKTEN

Was tun, wenn die IT zu einer Gefahr für das Unternehmen wird

Bernd Donabauer



GPM Workshop, Saarbrücken, 19.08.2008

## **Lieber Leser,**

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 überbortet werden.

Als Ergebnis meiner Überlegung finden Sie nun hier eine 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**

Sie können die Kommentare einblenden, indem Sie mit dem Mauszeiger darauf deuten.

Mit einem einfachen Linksklick werden diese geöffnet, so dass Sie den Kommentartext auch über die Zwischenablage kopieren können.

# **Krisenmanagement in IT-Projekten**

## **Was tun, wenn die IT zu einer Gefahr für die Existenz des Unternehmens wird**

### **GPM Workshop**

**Bernd Donabauer**

**Saarbrücken, 19.08.2008**



# Agenda

**Vorstellung**

**Begriffe**

**Beispiel**

**Top Down Vorgehensweise**

**Vergleich TD und BU**

**Definition Risiko**

**PDCA Zyklus**

**Vorgehensweise in der Praxis**

**Unterstützende Standards**

**Praxisprobleme Critical Incident**

**Excurs Humanressourcen**

**Praxisprobleme Critical Incident**

**Critical Incident als Chance**

**Kontakt**

# Vorstellung

## Der Referent

- / Bernd Donabauer**
- / Seit 1994 Tätigkeit als freier Consulter in verschiedenen IT-Projekten**
- / 14 Jahre Berufserfahrung als Mitarbeiter und Projektleiter in verschiedenen IT Projekten im In- und Ausland**
- / Davon 4 Jahre als Projektleiter IT Security, Leiter Marketing und Human Resources in einem IT-Unternehmen**
- / ITIL zertifiziert**
- / Master Examiner under ISO 17024:2003**
- / Mitglied in verschiedenen Normierungsgremien des BITKOM e.V. und des GI e.V. zu dem Thema Informationssicherheit und Qualifizierung**

# Vorstellung

## Beratungskompetenz

- / Überprüfung vorhandener Projekte auf ihre Konformität hinsichtlich anerkannter Best Practice Methoden und Normen
- / Entwicklung und Überwachung von Projekten in Übereinstimmung von Best Practice Methoden und Normen
- / Transfer und Aufbau von Wissen und Handlungskompetenz nach dem Advanced IT Training System (AITTS) in das Unternehmen des Klienten in einem integrierten Projekt- und Qualifizierungsmanagement





# Vorstellung

## Handlungskompetenz im Bereich Incident und Disaster

- / Externe Projektleitung nach einem vollständigen Ausfall der IT-Infrastruktur für fünf Arbeitstage  
Projektleitung in der anschließenden Reorganisation der IT-Infrastruktur und IT-Organisationsstruktur**
- / Externe Projektleitung nach Ausfall der kritischen Geschäftsprozesse  
Projektleitung in der anschließenden Reorganisation der IT-Infrastruktur und IT-Organisationsstruktur**
- / Externe Projektleitung nach Störung der kritischen Geschäftsprozesse durch den Ausfall von Humanressourcen**
- / Beratung der Geschäftsleitung bei der Identifikation kritischer Geschäftsprozesse und Ressourcen**

# Begriffe

## Unterscheidung Critical Incident, Desaster und Catastrophe

- / Ein kritischer Vorfall entsteht aufgrund interner Faktoren 
- / Ein kritischer Vorfall beeinträchtigt einen oder mehrere kritische Geschäftsprozesse 
- / Ein Geschäftsprozess ist immer dann kritisch, wenn damit eine erhebliche Gefährdung der materiellen Unternehmenswerte (Assets) verbunden ist 
- / Ein Desaster ist eine Störung einer oder mehrerer kritischer Geschäftsprozesse aufgrund externer Faktoren
- / In aller Regel wirkt ein Desaster großflächig und betrifft interne und externe Strukturen 
- / Eine Katastrophe ist ein Critical Incident oder ein Desaster mit existenzbedrohenden Schäden aufgrund nicht angemessener Reaktionen oder Vorbereitung


# Beispiel

## Beispiel Critical Incident

- / Zeitkritische Projektbuchungen konnten nicht durchgeführt werden, weil die Mitarbeiter keinen Zugriff auf die Buchungssoftware hatten**
- / Der kritische Geschäftsprozess ist das Projekt-Rechnungswesen**
- / Es besteht die Gefahr hoher Konventionalstrafen, Auftragsverlust und des Reputationsschaden (Assets)**
- / Die technische Ursache war ein korrupter Active Directory Service (ADS)**

# Beispiel

## Beispiel Disaster

- / Die Betreuung und Beratung von IT Geschäftskunden konnte teilweise nicht durchgeführt werden, weil die notwendigen Mitarbeiter nicht zur Verfügung standen
- / Der kritische Geschäftsprozess war die Leistungserstellung des Unternehmens
- / Es besteht die Gefahr hoher Konventionalstrafen, Auftragsverlust und des Reputationsschaden (Assets)
- / Die Ursache war der Tropensturm Katrina in New Orleans und ein mangelndes Social Engineering
- / Die Mitarbeiter wurden zwar in ein sicheres Ausweichrechenzentrum evakuiert, nicht jedoch deren Familienangehörige 

# Beispiel


## Beispiel Catastrophe

- / Zeitkritische Projektbuchungen konnten nicht durchgeführt werden, weil die Mitarbeiter keinen Zugriff auf die Buchungssoftware hatten. Der teilweise Ausfall der IT-Kernprozesse hielt 12 Werktage an**
- / Das Unternehmen wurde mit Konventionalstrafen belegt und es drohte der Verlust des Hauptkunden**
- / ...**
- / Die technische Ursache war ein korrupter Active Directory Service (ADS)**
- / Die Backup-Datenbestände waren unbrauchbar**
- / Es war kein Workaround definiert**
- / Es standen kein Ersatzsystem zur Verfügung**
- / Die Implementierung einer neuen ADS im laufenden Betrieb schlug fehl**



# Top Down Vorgehensweise

## Top Down vs. Bottom Up

- / Bottom Up pflegt die Betrachtung technischer Systeme
- / Ein effizienter Einsatz der Ressourcen findet i.a.R. nicht statt (Gießkannenprinzip)
- / Ein effektiver Einsatz der Ressourcen findet i.a.R. nicht statt, weil die Zieldefinitionen unklar sind (IT als Selbstzweck) 
- / Top Down definiert die Unternehmenswerte
- / Die kritischen Geschäftsprozesse
- / Die Services, die für die Durchführung der kritischen Geschäftsprozesse notwendig sind
- / Die Soft- und Hardware, auf denen die Services abgebildet werden

# Vergleich

## Vergleich einer Bottom Up und Top Down Methode in der Informationssicherheit

- / Der Grundschutzkatalog des Bundesamt für Sicherheit in der Informationstechnik ist eine Bottom Up Methode**
- / Es besteht im wesentlichen aus einem technischen Maßnahmenkatalog technischer und organisatorischer Einzelmaßnahmen**
- / Er geht von einem Schutzbedarf für technische Systeme aus**
- / Das Information Security Management System nach ISO 2700ff ist eine Top Down Methode**
- / Es geht von einem Risiko für die Unternehmenswerte aus**
- / Der Plan Do Check Act Zyklus (PDCA) ist vorgeschrieben**



# Definition Risiko

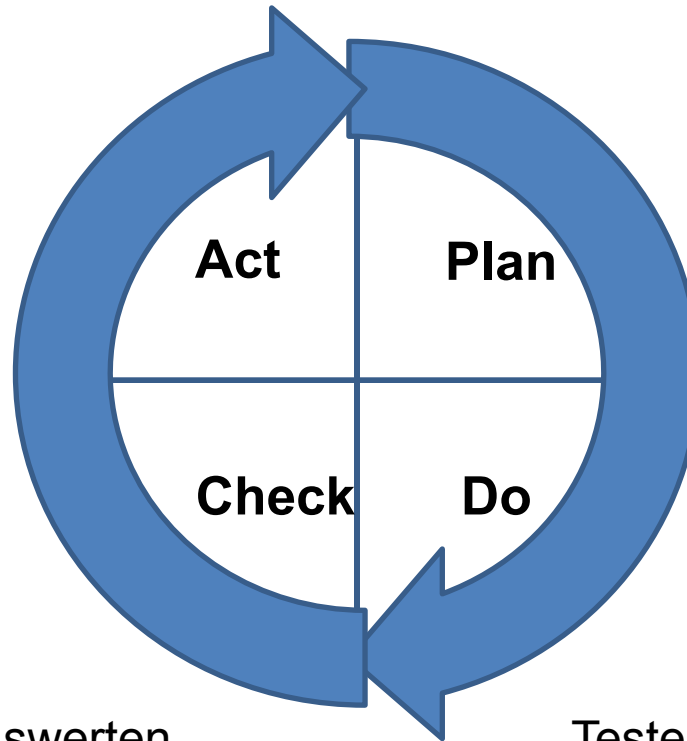
**„Risiko ist definiert als möglichen Eintritt eines potentiellen Schadensereignisses sowie dessen Höhe und entspricht der Wahrscheinlichkeit des Zusammenwirkens von Bedrohung und Schwachstelle bezogen auf ein System“**

- / Ohne Schaden (negative Asset) kein Risiko**
- / Ohne Bedrohung kein Risiko**
- / Ohne Schwachstelle kein Risiko**
- / Ohne die Definition des Systems kein Risiko**

# PDCA Zyklus

Anpassen und Einführen



Bedarfsfeststellung und  
Planung



Prüfen und Auswerten

Testen und Einführen

# Vorgehensweise in der Praxis

- / Identifizierung der Unternehmenswerte in Zusammenarbeit mit der Unternehmensführung 
- / Definition, Anpassung und Dokumentation der kritischen Geschäftsprozesse in Zusammenarbeit mit den Abteilungsleitern und Mitarbeitern
- / Identifizierung der Risiken für Geschäftsprozesse und Unternehmenswerte
- / Definition der Kritikalität (tolerierete Ausfallszeiten), des Workaround und des Besitzers des Prozesses
- / Planung (Budgetplanung, organisatorische Planung, Ressourcen- und Qualifizierungsplanung, Projektmarketing, technische Planung, Prozessplanung, etc.) und Einführung der Maßnahmen zur Verringerung der Risiken
- / Regelmäßige und unabhängige Überprüfung nach einem festen Audit-Plan 
- / Anpassung der Maßnahmen



# Unterstützende Standards



- / ISO 9000ff**  
Dokumentation und Überwachung der Geschäftsprozesse, der Organisation und der Mitarbeiter (Qualitätsmanagement)
- / ISO 20000/ ITIL**  
Dokumentation und Überwachung der IT Serviceprozesse, der Organisation und der Mitarbeiter. Best Practice zum Aufbau einer IT Service Infrastruktur
- / ISO 27000ff/ ISMS**  
Dokumentation und Überwachung der Informationssicherheit, der Organisation und der Mitarbeiter. Best Practice zum Aufbau eines Informationssicherheitsinfrastruktur
- / BS 25999/ Business Business Continuity Management System (BCMS)**  
Dokumentation und Überwachung des BCM, der Organisation und der Mitarbeiter. Best Practice zum Aufbau eines BCM Infrastruktur

# Praxisprobleme Critical Incident

## Das Problem der Innenansicht vor dem Critical Incident

- / Fehlende externe Kontrolle führt zur „Betriebsblindheit“
- / Mangelnde Kommunikation zwischen technischer und kaufmännischer Leitung 
- / Mangelhafte Organisationsstrukturen werden nicht erkannt
- / Mangelhafte Methodik wird akzeptiert
- / Mitarbeiter verfügen nicht über die Mittel um ihre Funktion auszuüben 

# Praxisprobleme Critical Incident

## Das Problem der Trauerphasen nach dem Critical Incident

- / **Vorhandene Strukturen haben zum Critical Incident geführt**
- / **Verantwortliche sind direkt betroffen**
- / **Wertvolle Zeit geht verloren**
- / **1. Phase:  
Schock, Verleugnung, Nicht-wahrhaben-Wollen**
- / **2. Phase:  
Aufbrechende Gefühle, gegenseitige  
Schuldzuweisungen**
- / **3. Phase:  
Anpassung und Akzeptanz der Situation**
- / **4. Phase:  
Beginnende Suche nach Lösungen und  
grundsätzlichen Veränderungen**

# Praxisprobleme Critical Incident

## Das Problem des Machtvakuumms bei der Aufarbeitung des Critical Incident

- / Vorhandene Strukturen haben zum Critical Incident geführt**
- / Schnelle Reaktionen und Entscheidungs- und Handlungsfreiheit notwendig**
- / Umgehung üblicher Hierarchien notwendig**
- / Klare Benennung der Ursachen und der Verantwortlichkeiten notwendig**
- / Charakterstarke Führung notwendig**

# Excurs Humanressourcen

## Humanressourcen

- / Begriff aus dem Organisationsmanagement impliziert eine begrenzte Ressource**
- / Der Menschen und seine Befähigung mit den gegebenen Produktionsmitteln umzugehen**

## Humankapital



- / Produktionsfaktor neben Kapital, Arbeit und Boden**
- / Fähigkeiten und Fertigkeiten (Handlungskompetenz) sowie das Wissen von Menschen**

## Human Assets

- / An die Mitarbeiter gebundenes Vermögen einer Organisation in Form von Handlungskompetenz und Wissen**
- / Durch die Mitarbeiter repräsentierte Kernkompetenz der Organisation**

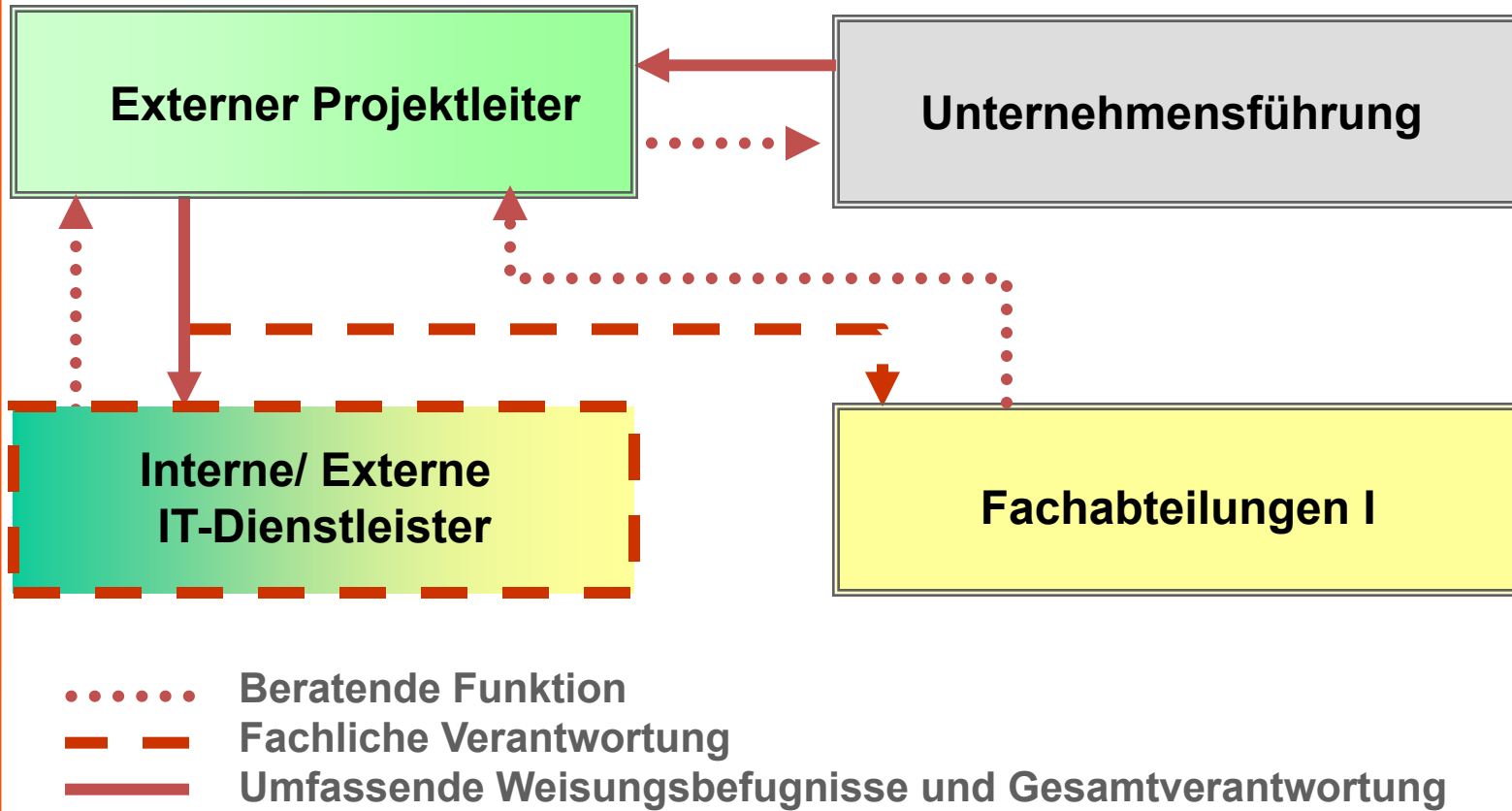
# Praxisprobleme Critical Incident

## Das Problem der Humanressourcen bei der Aufarbeitung des Critical Incident

- / **Besondere Handlungskompetenzen erforderlich**
- / **Besondere Wissensbestände erforderlich**
- / **Spezialisierung Im „Tagesgeschäft“ oft nicht Nutzbar  und sogar abträglich**
- / **Hohe Kosten für die Aneignung, den Erhalt, die Entwicklung und die Überwachung der geforderten Kompetenzen und Wissensbestände**
- / **Nach Aufarbeitung des Critical Incident Einbindung in  die Unternehmensorganisation nicht möglich**

# Praxisprobleme Critical Incident

Vorschlag zur Problemlösung: Definition des Critical Incident als Projekt auf Zeit



Quelle: Eigene Darstellung.

# Critical Incident als Chance

- / Überprüfung von Organisation und Prozessen**
- / Ausschaltung aller nicht für die Leistungserstellung notwendigen Prozesse und Teilprozesse**
- / Überprüfung und Änderung der Vertragsverhältnisse mit internen und externen Dienstleistern**
- / Zieldefinitionen**
- / Servicedefinitionen**
- / Ausreichende Mittelbereitstellung für die Abbildung der verbliebenen Prozesse**
- / Mittelfristige strategische IT- und Budget-Planung**

# Kontakt

## **Bernd Donabauer**

IT Management & Resources

Rodauer Str. 20

64372 Ober-Ramstadt

Tel.: 06154 575264

Fax.: 06154 575265

Mobil: Auf Anfrage

mailto: [info@it-mare.com](mailto:info@it-mare.com)

[www.it-mare.com](http://www.it-mare.com)

Die kommentierte Fassung steht Ihnen ab dem 24.08.2008 unter [www.it-mare.com](http://www.it-mare.com) zur Verfügung.

Donabauer, Bernd: Krisenmanagement in IT-Projekten. Was tun, wenn die IT zu einer Gefahr für die Existenz des Unternehmens wird. GPM Workshop. Saarbrücken, 19.08.2008. Veröffentlicht unter [www.it-mare.com/sources/190808\\_vortrag\\_gpm.pdf](http://www.it-mare.com/sources/190808_vortrag_gpm.pdf).