

Imagine making better decisions

CRISAM®

A Decision Engineering Framework

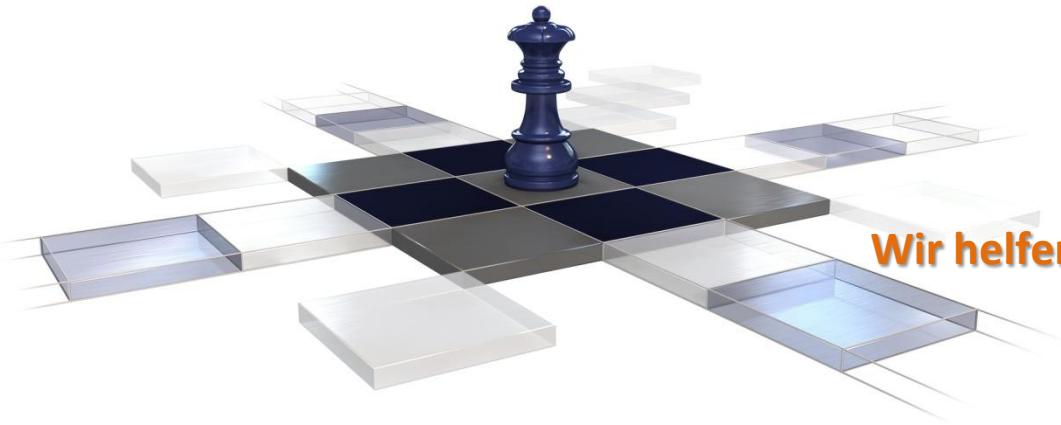
IT Riskmanagement als Basis für Entscheidungen im IT Umfeld - auch in Krisenzeiten

kapsch >>>
always one step ahead

Kapsch Solution Day Salzburg

Dipl. Ing. Dr.Dr. Manfred Stallinger, MBA
manfred.stallinger@calpana.com

Bereits die Asiaten verstanden unter „calpana“ das schwer Vorstellbare vorstellbar zu machen!



calpana
business consulting

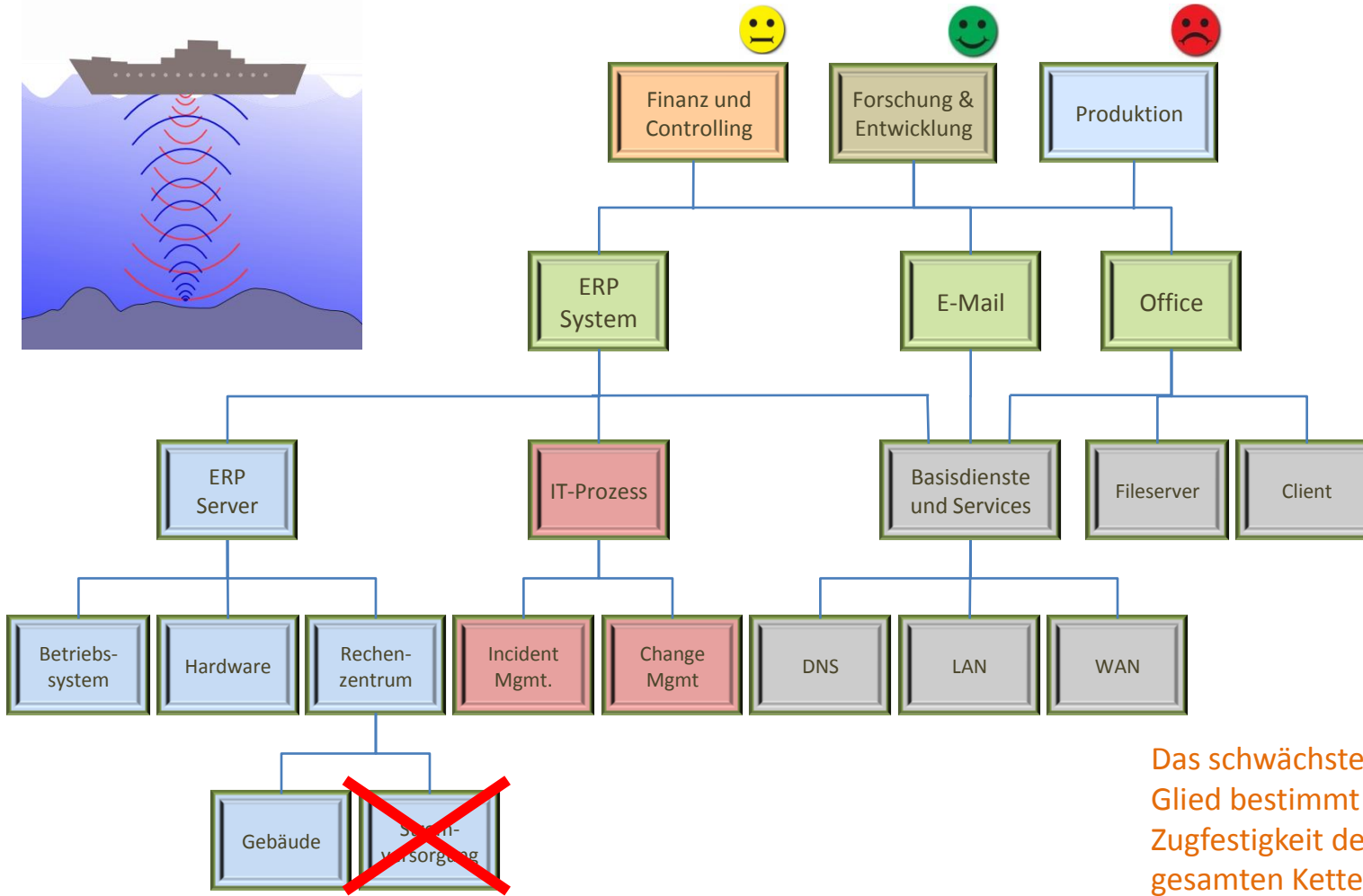
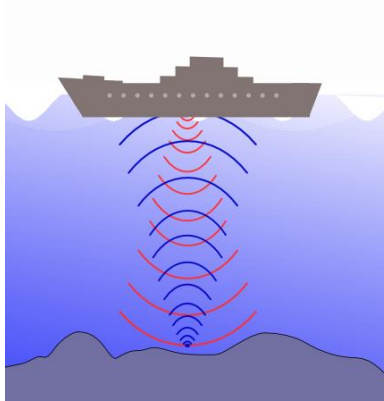


Wir helfen Ihnen den richtigen nächsten Schritt zu finden und auch zu setzen!

- ⊗ **Calpana Business Consulting** ist Entwickler und Hersteller der Risikomanagement- bzw. **Decision Engineering Methodologie CRISAM®**.
- ⊗ Wir konzentrieren uns als Software- und Beratungsunternehmen ausschließlich auf **Risiko- und Sicherheitsmanagement** aus einer Unternehmensgesamtansicht.
- ⊗ Wir verstehen uns als international tätiges Unternehmen, indem wir **Partner** bei der Umsetzung von Projekten unterstützen und unsere Kunden in deren strategischen Zielmärkten rund um den Globus begleiten.
- ⊗ DI Dr.Dr. Manfred Stallinger, MBA gründete 2005 das Unternehmen, das seither als eigentümergeführtes Unternehmen seine Kompetenz am Unternehmensstandort in Linz (Österreich) bündelt.



Die IT ist im Unternehmen ein wesentliches, jedoch **komplexes, hoch vernetztes** und ein sich **sehr rasch änderndes** Gebilde!!



Das schwächste Glied bestimmt die Zugfestigkeit der gesamten Kette!

Schematische Darstellung



Die **TOP 10 Herausforderungen**, denen sich das **IT-Management** heute stellen muss?

1. Trotz **Kostendruck** die **richtigen** und **notwendigen Investitionen** und **Maßnahmen** herausfinden.
2. Den **Nutzwert** von **IT-Maßnahmen** dem Management transparent darstellen (ROI-Analyse).
3. Die geforderte **Betriebssicherheit** und **Zuverlässigkeit** sicherstellen.
4. Die **Komplexität** und **Vernetztheit** der **IT** bewältigen.
5. Erforderliche **Notfallvorsorgen**, **Notfallhandbücher** und **Notfallplanung** bereitstellen.
6. Die nötige **Transparenz** und **Nachvollziehbarkeit** für Informationssicherheit in unternehmensübergreifenden **Geschäftsprozessen** herstellen - ein **internes Kontrollsystems** für die IT bereitstellen.
7. National und international **geltende Normen, Gesetze** und **Vorschriften** einhalten (aus Vorgaben von **Kunden** und Prüf- bzw. **Aufsichtsorganen**).
8. An das **unternehmensweite Risikomanagement** (ERM) eine **monetär formulierte Risikoabschätzung** liefern.
9. Die vom Service Provider gelieferte **Service-Qualität** (SLA-Management) überprüfen.
10. Die **kontinuierliche Verbesserung** der **Prozessqualität** sicherstellen.

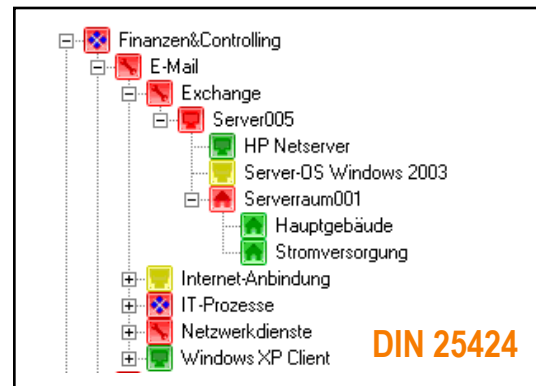


CRISAM® RV identifiziert operationale Risiken anhand anerkannter Modelle, Normen und Standards.

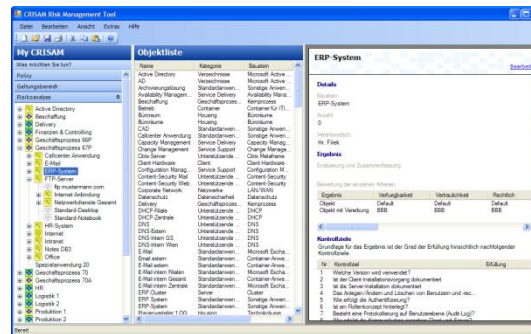
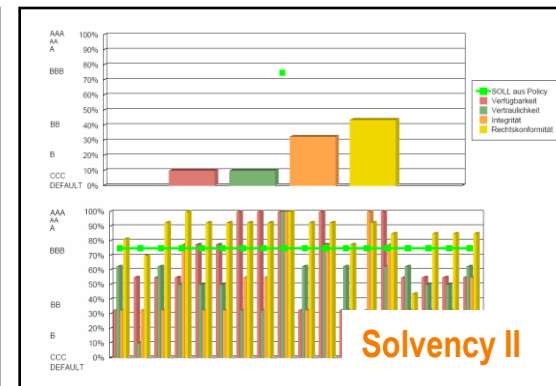
Vorgehensmodell



Risikobaum-Modell



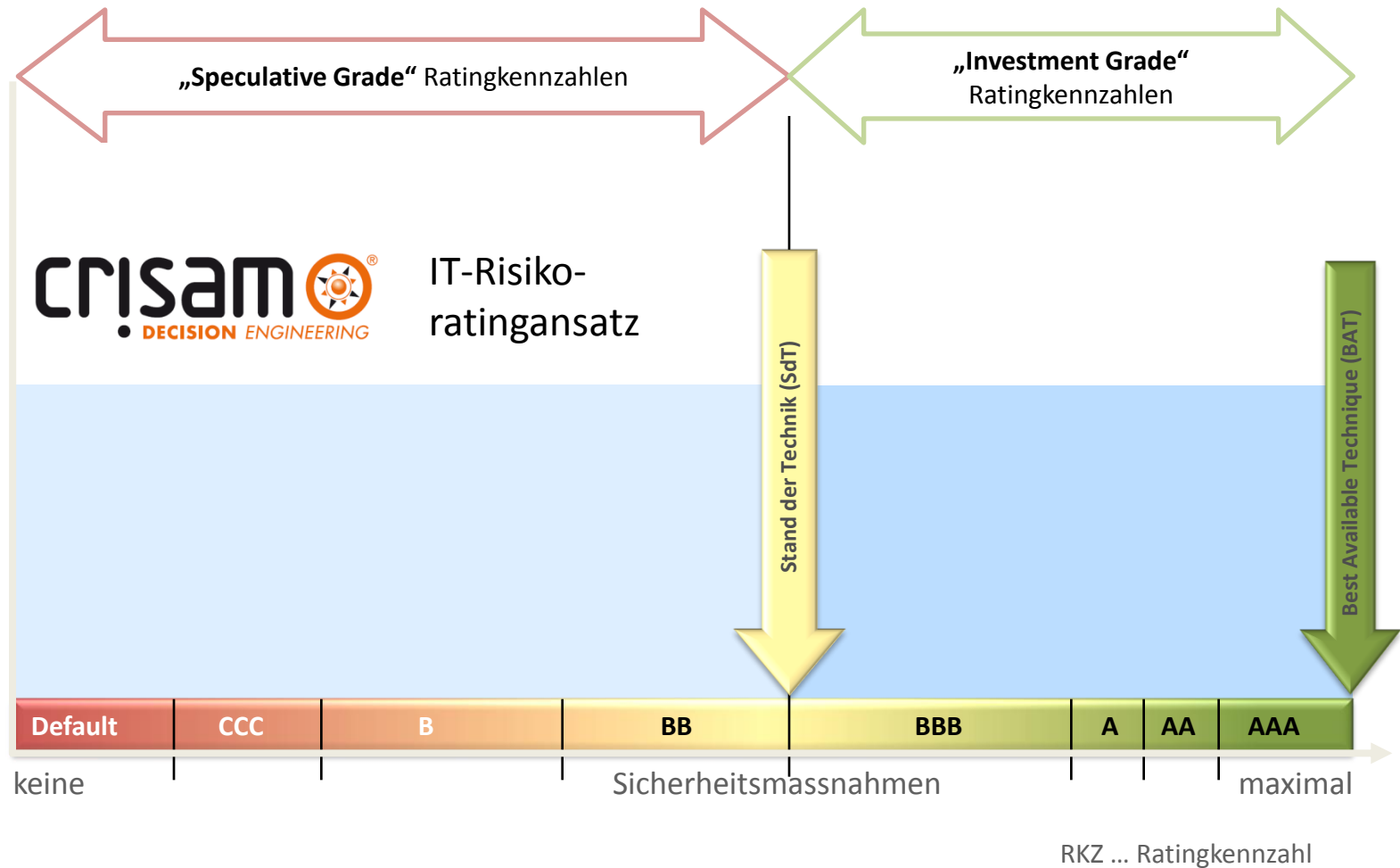
Ratingmodell



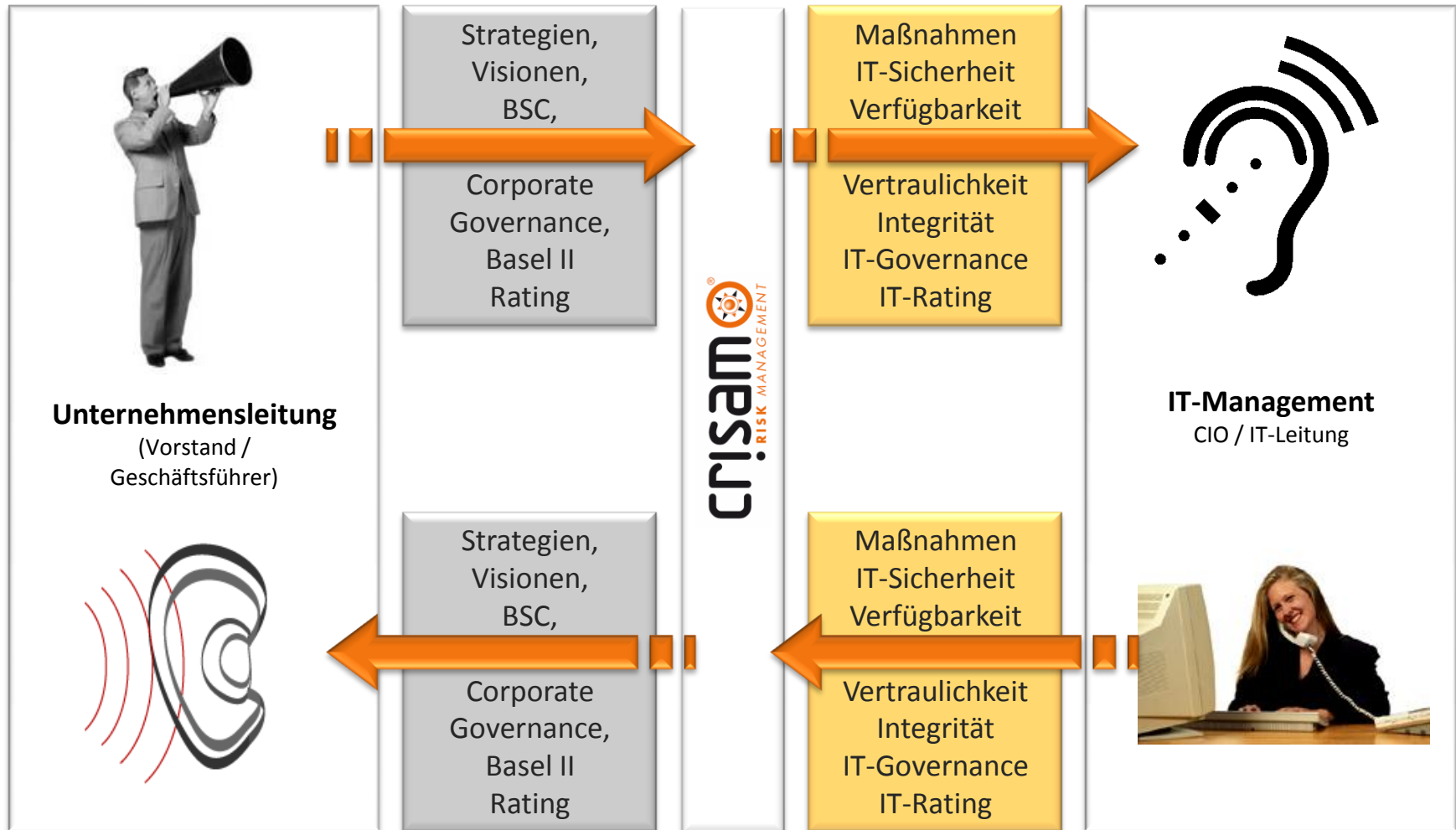
CRISAM® Explorer



Identifizierte Risiken aus dem Einsatz der IT im Unternehmen werden durch Kennzahlen der Versicherungswirtschaft dargestellt!



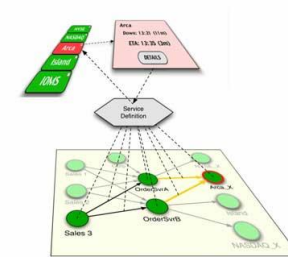
CRISAM® RV liefert der Unternehmensleitung ein, in ihrer „Sprache“ formuliertes, transparentes, nachvollziehbares und effizientes Management **operationaler IT-Risiken**.



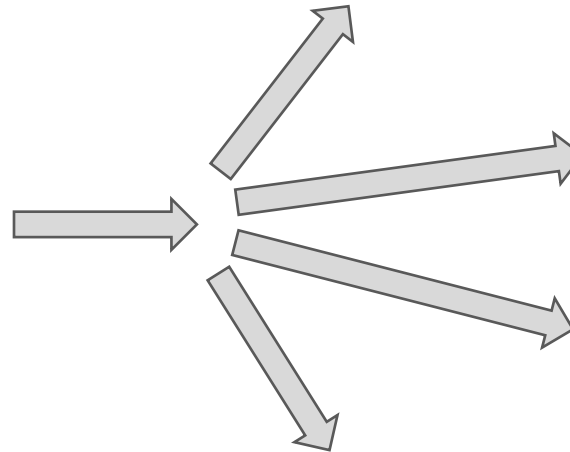
CRISAM® RV liefert auch erforderliche Fakten für den **Informationssicherheits-, Service Level Management- und Business Continuity Management Prozess**, sowie eine **Nutzwertanalyse** und Grundlagen der **Notfallplanung**.



ISMS nach ISO 27001



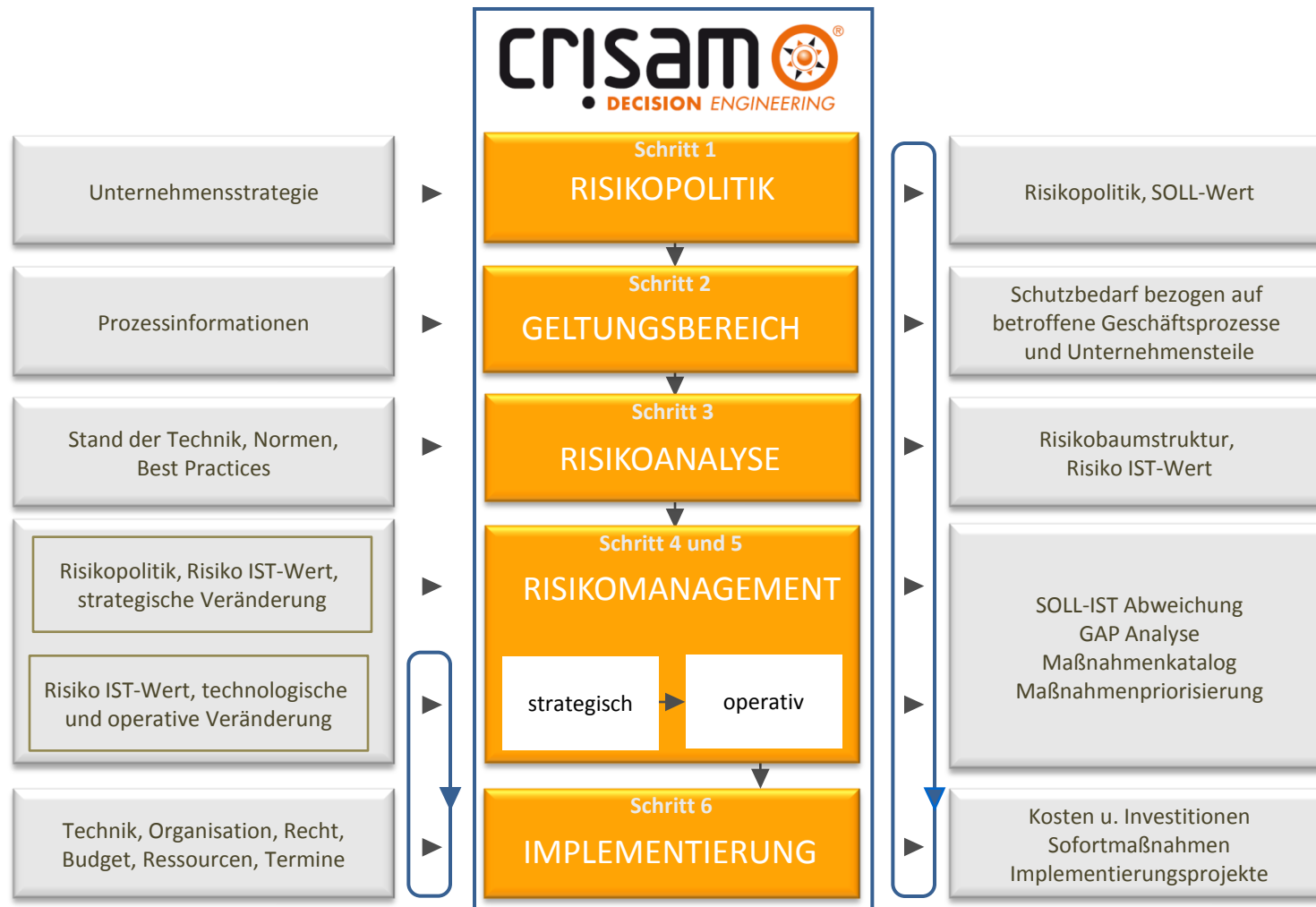
Service Level Management



BCM nach BS 25999-1:2006



CRISAM® RV folgt dem ISO 27001-Prozessmodell und liefert Daten und Fakten für weiterführende IT- (Management-) Projekte.

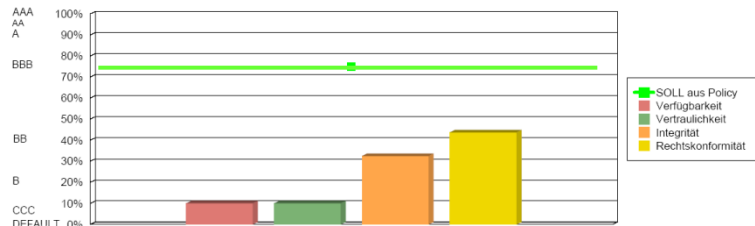


(CRISAM ... Corporate Risk Application Method)

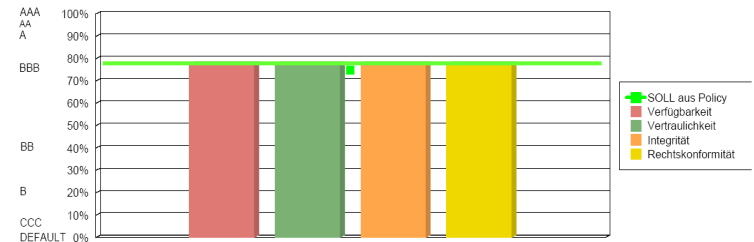


Durch Simulationen wird die **Effizienz** der erforderlichen **Maßnahmen** und **Investitionen** am IT-Modell bewertet und eine **Implementierungspriorität** festgelegt.

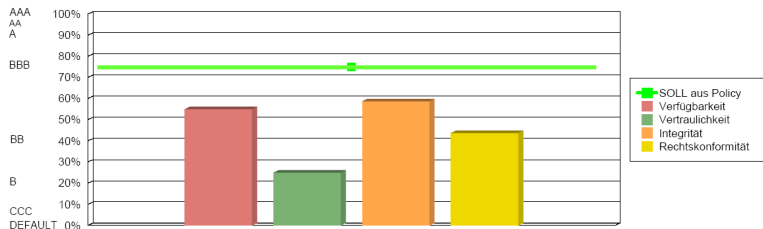
Ausgangssituation



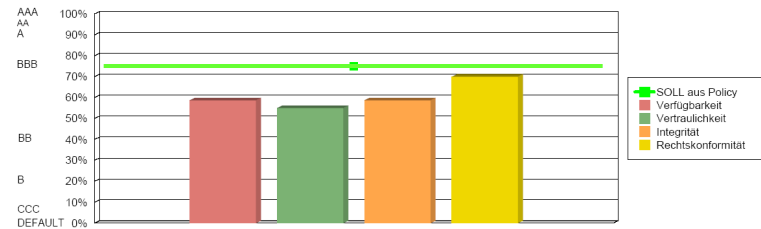
Optimierter IST-Zustand



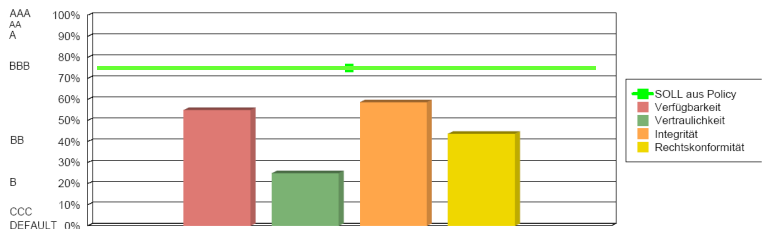
Umsetzung der Maßnahme 1



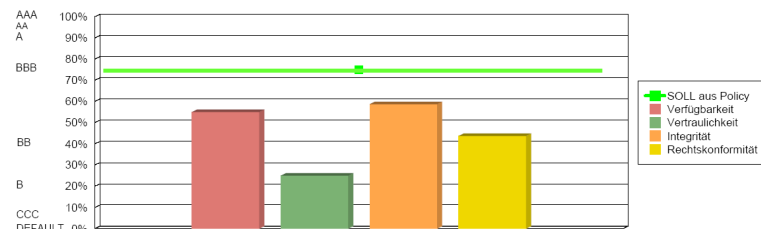
Umsetzung der Maßnahme 5



Umsetzung der Maßnahme 2



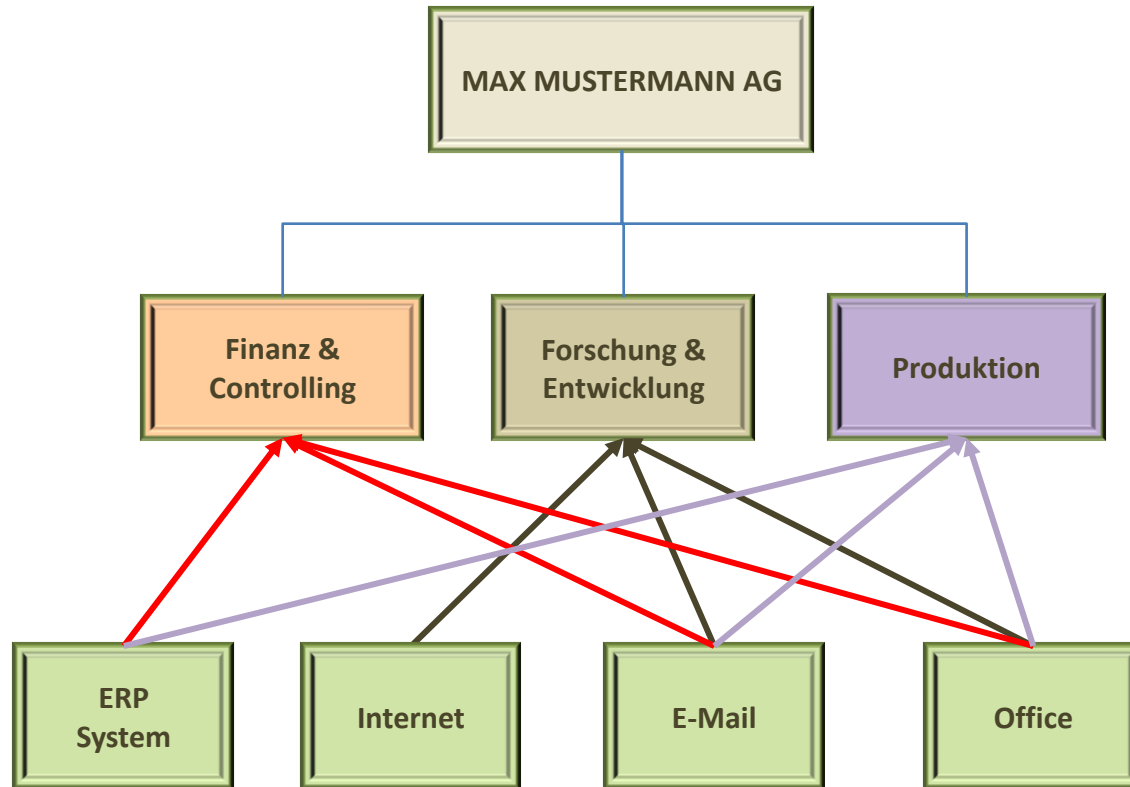
Umsetzung der Maßnahme 4



Umsetzung der Maßnahme 3



Casestudy: Max Mustermann AG am Beispiel IT-Risiko.



Prozess- und Bereichsleiter legen den Business Impact und den maximalen IT-relevanten Schaden an ihren Prozessen bzw. Bereichen fest.

Verfügbarkeit

	keine Verwendung
u	unbedeutend
g	gering
m	mittel
h	hoch
s	sehrhoch

	Finanzen&Controlling	Forschung&Entwicklung	Produktion	Risk AG
E-Mail	u	g	g	s
Finanzen&Controlling				
Forschung&Entwicklung				s
Internet		g		
Office	g	g	u	
Produktion				s
SAP	u	h		

Vertraulichkeit

	keine Verwendung
u	unbedeutend
g	gering
m	mittel
h	hoch
s	sehrhoch

	Finanzen&Controlling	Forschung&Entwicklung	Produktion	Risk AG
E-Mail	u	s	u	s
Finanzen&Controlling				
Forschung&Entwicklung				s
Internet		u		
Office	g	m	u	
Produktion				s
SAP	m		u	

Integrität

	keine Verwendung
u	unbedeutend
g	gering
m	mittel
h	hoch
s	sehrhoch

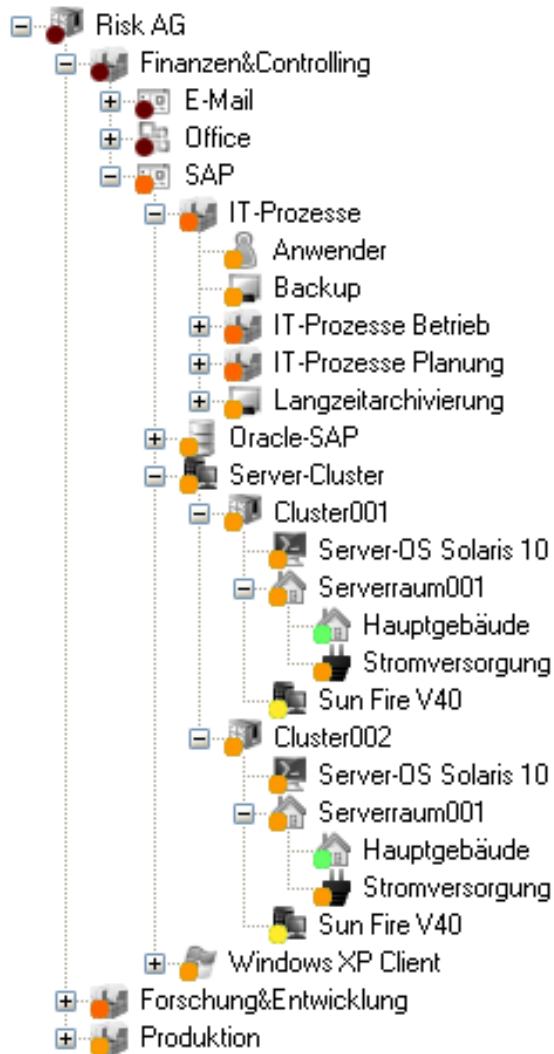
	Finanzen&Controlling	Forschung&Entwicklung	Produktion	Risk AG
E-Mail	u	g	g	s
Finanzen&Controlling				
Forschung&Entwicklung				s
Internet		u		
Office	g	g	u	
Produktion				s
SAP	m		u	

IT-SERVICE	Rating	F&C MFL [€]	F&E MFL [€]	Produktion MFL [€]
ERP	BB	400.000,-	-	1.000.000,-
E-Mail	B	20.000,-	8.000.000,-	20.000,-
Office	BBB	150.000,-	300.000,-	10.000,-
Internet	BBB	-	100.000,-	-

Verfügbarkeit,
Vertraulichkeit
und Integrität aggregiert



Risikoobjekte werden in einer Ursache-Wirkungsbeziehung entsprechend der DIN 25424 – Fehlerbaumanalyse modelliert.



- ⊗ An der Wurzel des Risikobaumes, den Geschäftsprozessen, wirkt das Risiko aller Risikoobjekte.
- ⊗ Das resultierende Risiko ergibt sich aus den Einzelrisiken in den jeweiligen Organisationseinheiten bzw. Geschäftsprozesse.
- ⊗ Die Aggregation der einzelnen Risikoquellen folgt den Bildungsregeln der Fehlerbaumanalyse (DIN 25424).



Aus Abweichungen vom SOLL werden konkrete Maßnahmen abgeleitet, ...

Objekt	Ist-Erfüllung	Soll-Erfüllung	Abweichung
HP Netserver	F	C+	
Service Continuity Management	D	A-	
Configuration Management	C-	A-	
Serverraum001	C	A-	
Standard Arbeitsplatz	C	A-	
Server-OS Solaris 10	C	A-	
Server-Cluster	C	A-	
Release Management	C	A-	
Langzeitarchivierung	C	A-	
Incident Management	C+	A-	
Stromversorgung	C+	A-	
Anwender	C+	A-	
SAP	B-	A-	
Oracle-SAP	B-	A-	
Problem Management	B-	A-	
Security Management	B-	A-	
Windows XP Client	B-	A-	
Service Desk	B-	A-	
Backup	B-	A-	
Datenträgerarchiv	B-	A-	
Sun Fire V20	B	A-	
Service Level Management	B	A-	
Change Management	B+	A-	
Availability Management	B+	A-	
Exchange	C	C+	
Active Directory	C	C+	
Server-OS Windows 2003	C	C+	
Hauptgebäude	A-	A-	
Firewall1	C+	C+	
Firewall2	C+	C+	
Internet-Anbindung	C+	C+	
Capacity Management	A-	A-	
Office	C+	C+	
DHCP	B-	C+	
Serverraum015	B-	C+	
Sun Fire V40	B	B-	
Gebäude Linz	B-	C+	
Serverraum002	B	C+	
SAN	B	C+	

Kosten „BBB“:

Jahr	Inhalt	Kosten [€]
1	Invest	300.000,00
1	Betrieb	10.000,00
2	Betrieb	10.000,00
3	Betrieb	10.000,00
4	Betrieb	10.000,00
5	Betrieb	10.000,00
Ges:	10% Finanz.	550.309,10

Kosten „A“:

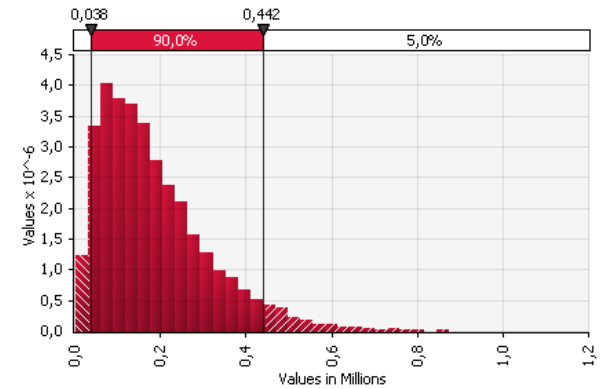
Jahr	Inhalt	Kosten [€]
1	Invest	450.000,00
1	Betrieb	15.000,00
2	Betrieb	15.000,00
3	Betrieb	15.000,00
4	Betrieb	15.000,00
5	Betrieb	15.000,00
Ges:	10% Finanz.	825.463,65



Deren quantitatives, monetäres Risiko wird bezogen auf die unterstützten Geschäftsprozesse ermittelt.

IT-Service Prozess	Rating	MFL	BestCase	MostLikely	WorstCase
ERP F&C	BB	€ 400.000,00	€ 1.960,00	€ 11.534,00	€ 27.480,00
E-Mail F&C	B	€ 20.000,00	€ 21,04	€ 1.236,00	€ 2.932,00
OFFICE F&C	BBB	€ 150.000,00	€ 315,60	€ 1.858,50	€ 4.419,30
Internet F&E	BB	€ 100.000,00	€ 490,00	€ 2.883,50	€ 6.870,00
E-Mail F&E	B	€ 8.000.000,00	€ 3.155,40	€ 185.400,00	€ 439.800,00
OFFICE F&E	BBB	€ 300.000,00	€ 631,20	€ 3.717,00	€ 8.838,60
ERP Produktion	BB	€ 1.00.000,00	€ 2.450,00	€ 14.417,50	€ 34.350,00
E-Mail Produktion	B	€ 20.000,00	€ 21,04	€ 1.236,00	€ 2.932,00
OFFICE Produktion	BBB	€ 10.000,00	€ 21,04	€ 123,90	€ 294,62

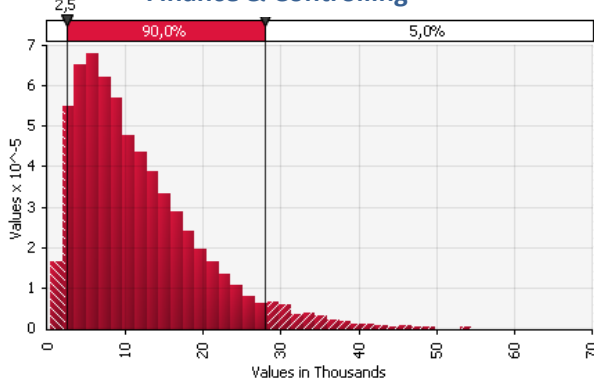
ERGEBNIS IST-Bewertung



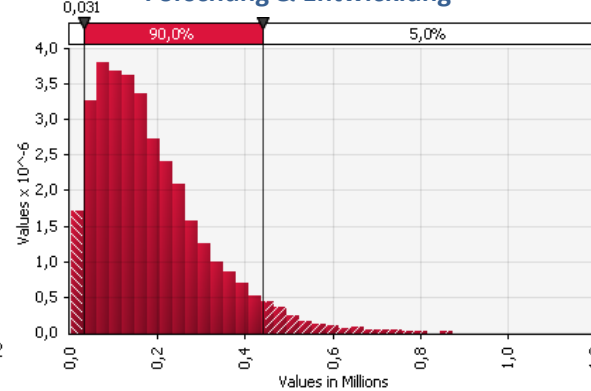
Erwartetes Risiko IT: € **187.939,00**

Risikokosten in 5 Jahren: € **1.262.125,00**

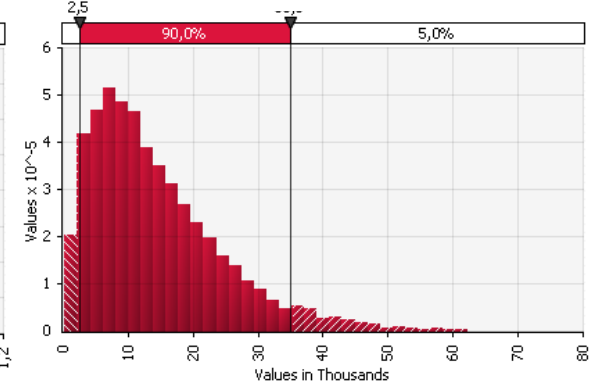
Finance & Controlling



Forschung & Entwicklung



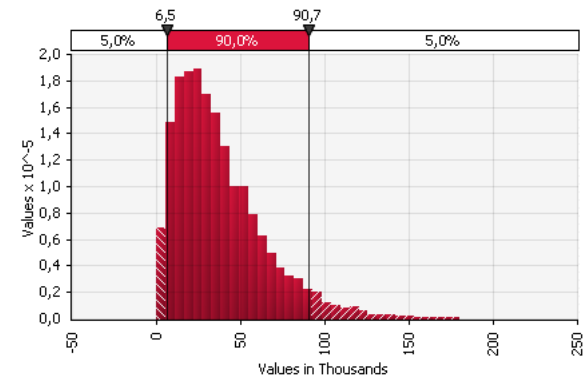
Produktion



Eine „Was wäre wenn?“-Simulation für eine „BBB“ IT-Qualität, zeigt den potentiellen Nutzen, **eine Risikoreduktion von etwa € 150.000,-, der Verbesserung! Einen 5-Jahres Nettonutzen von etwa € 456.000,00.**

IT-Service Prozess	Rating	MFL	BestCase	MostLikely	WorstCase
ERP F&C	BBB	€ 400.000,00	€ 841,60	€ 4.956,00	€ 23.468,00
E-Mail F&C	BBB	€ 20.000,00	€ 42,08	€ 247,80	€ 1.173,40
OFFICE F&C	BBB	€ 150.000,00	€ 315,60	€ 1.858,50	€ 8.800,50
Internet F&E	BBB	€ 100.000,00	€ 210,40	€ 1.239,00	€ 5.867,00
E-Mail F&E	BBB	€ 8.000.000,00	€ 6.312,00	€ 37.170,00	€ 176.010,00
OFFICE F&E	BBB	€ 300.000,00	€ 631,20	€ 3.717,00	€ 17.601,00
ERP Produktion	BBB	€ 1.00.000,00	€ 1.052,00	€ 6.195,00	€ 29.335,00
E-Mail Produktion	BBB	€ 20.000,00	€ 42,08	€ 247,80	€ 1.173,40
OFFICE Produktion	BBB	€ 10.000,00	€ 21,04	€ 123,90	€ 586,70

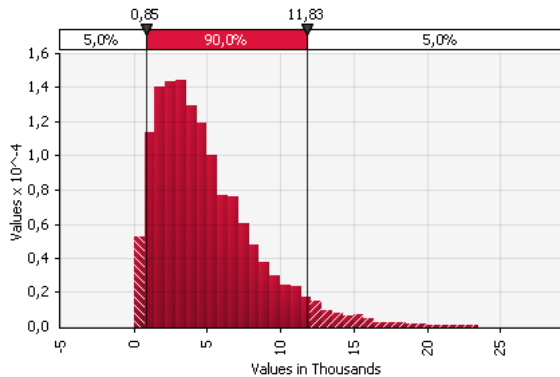
ERGEBNIS IST-Bewertung



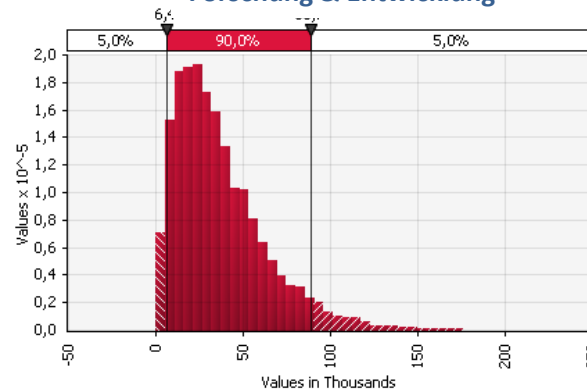
Erwartetes Risiko IT: € 37.998,00

Risikokosten in 5 Jahren: € 255.179,00

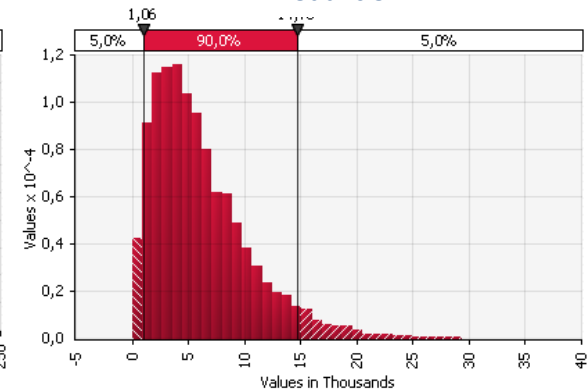
Finance & Controlling



Forschung & Entwicklung



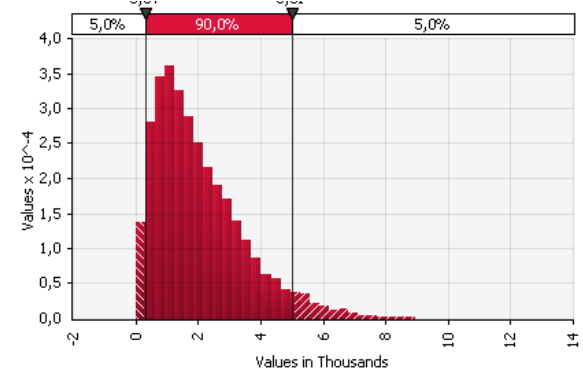
Produktion



Eine Simulation für die geplante Zielsituation, einer „A“ IT-Qualität, zeigt den potentiellen Nutzen, **eine Risikoreduktion von etwa € 150.000,-, der Verbesserung! Einen 5-Jahres Nettonutzen von etwa € 350.000,00.**

IT-Service Prozess	Rating	MFL	BestCase	MostLikely	WorstCase
ERP F&C	A	€ 400.000,00	€ 278,04	€ 1.651,20	€ 3.912,80
E-Mail F&C	A	€ 20.000,00	€ 13,90	€ 82,56	€ 195,64
OFFICE F&C	A	€ 150.000,00	€ 104,27	€ 619,20	€ 1.467,30
Internet F&E	A	€ 100.000,00	€ 69,51	€ 412,80	€ 978,20
E-Mail F&E	A	€ 8.000.000,00	€ 2.085,30	€ 12.384,00	€ 29.346,00
OFFICE F&E	A	€ 300.000,00	€ 208,53	€ 1.238,40	€ 2.934,60
ERP Produktion	A	€ 1.00.000,00	€ 347,55	€ 2.064,00	€ 4.891,00
E-Mail Produktion	A	€ 20.000,00	€ 13,90	€ 82,56	€ 195,64
OFFICE Produktion	A	€ 10.000,00	€ 6,95	€ 41,28	€ 97,82

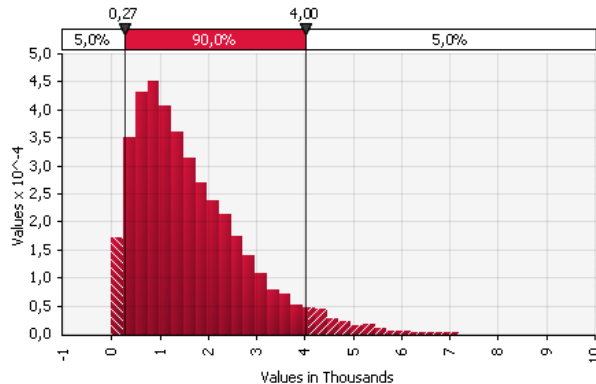
ERGEBNIS IST-Bewertung



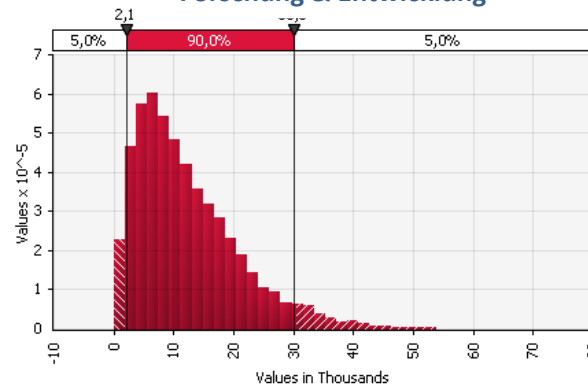
Erwartetes Risiko IT: € 12.682,00

Risikokosten in 5 Jahren: € 85.167,00

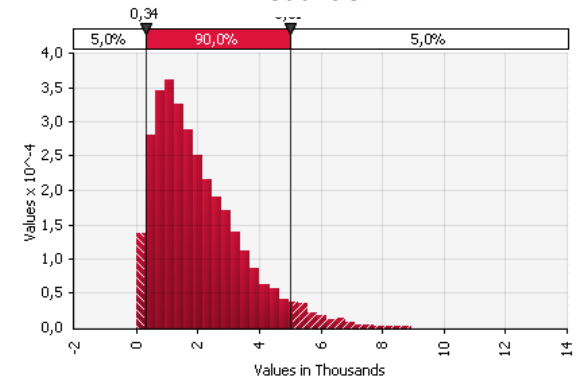
Finance & Controlling



Forschung & Entwicklung



Produktion



Nutzwerte, die Kunden durch den Einsatz von CRISAM® im IT-Management erkannt haben.

Eigentümer	Geschäftsführer	IT-Management
<p>Transparenz</p> <ul style="list-style-type: none"> • Transparenz für die Mittelverwendung wird erreicht <p>Corporate Governance</p> <ul style="list-style-type: none"> • Anforderungen an die Corporate Governance finden auch Niederschlag in rechtlichen Rahmenbedingungen wie SOX, 8.EU-RL, KontraG etc. • Der Nachweis eines effizienten Risikomanagements reduziert die Gefahr unerwarteter Kapitalbedarfe und schützt die Liquidität des Unternehmens. <p>Abhängigkeit</p> <ul style="list-style-type: none"> • Ausmaß und Kritikalität der Abhängigkeit aller Unternehmensprozesse von der IT werden dargestellt 	<p>Haftung</p> <ul style="list-style-type: none"> • Risiken aus der Fahrlässigkeit werden drastisch reduziert • Sorgfaltspflicht wird dokumentiert und überprüft <p>Markt</p> <ul style="list-style-type: none"> • Dem Kunden wird eine nachvollziehbare und dokumentierte Prozessqualität aus dem IT-Einsatz gewährleistet • Wettbewerbsvorteile durch Zuverlässigkeit <p>Risikoidentifikation</p> <ul style="list-style-type: none"> • Risiken werden kalkulierbar • Steuerung des IT-Einsatzes wird möglich <p>Finanzierung</p> <ul style="list-style-type: none"> • Möglichkeit der Risikodarstellung zu Finanz- und Kreditgebern • Transparenz der zu versichernden Risiken für bringt Transparenz in der Prämienberechnung 	<p>Qualität</p> <ul style="list-style-type: none"> • Qualität wird nachweisbar • Laufende Qualitätsverbesserung durch den kontinuierlichen Risikomanagement-Prozess • Service Levels mit Dienstleister werden transparent <p>Verantwortung</p> <ul style="list-style-type: none"> • Vorstand und Nutzer werden in die Verantwortung miteinbezogen <p>Planung/Budgetierung</p> <ul style="list-style-type: none"> • Vereinfachte Budgetplanung • Nachweis der Budgetwahrheit • Nutzwert der Investition kann dargestellt werden <p>Technologieeinsatz</p> <ul style="list-style-type: none"> • Investitionen können bestmöglich priorisiert werden • Eine Notfallplanung wird aus Business-Sicht getrieben



Imagine making better decisions



Dr. Manfred Stallinger
Geschäftsführer
calpana business consulting GmbH

**Vielen Dank für
Ihre Aufmerksamkeit!**

calpana business consulting
calpana business consulting gmbh
A-4020 Linz, Blumauerstraße 43
Tel: +43 (732) 601216-0
www.calpana.com, www.crisam.net

Copyright © 2009