Ergebnisprotokoll

LSZ CIO-Kongress 2014

23.-25. November 2014, Spa & Conference Hotel Loipersdorf

Arbeitskreis Nummer: 3

Workshopthema: Ist der CIO der eigentliche Risikomanager im Unternehmen?

Name des Workshopleiters: Bernhard Göbl, Werner Weinguny

Name des Arbeitskreisleiters: Christian Kudler

Teilnehmerzahl: 18

Ergebnisse / behandelte Themen:

- Bernhard Göbl (Initialstatement): in der Praxis ist entweder gar kein Risikomanagement/Risikomanager und wenn doch, dann häufig im IT-Bereich angesiedelt
- Werner Weinguny (Initialstatement): IT im Spannungsfeld zwischen Chancen nutzen und Risiko minimieren; häufig werden auch dem IT-Bereich Dinge zugeschoben, die sie aufgrund zu geringer Ressourcenausstattung gar nicht leisten kann
- Christian Kudler (Initialstatement): Risiko kommt im Dreieck des IT-Wertbeitrags (Nutzen, Kosten, Risiko) zwei Mal vor: Positiv im Nutzenbereich (IT als Mittel zur Risikosenkung im Unternehmen); Negativ als Risiko des IT-Einsatzes selbst

- Manchmal ist eine klare Risikoanalyse im Unternehmen ganzheitlich gar nicht möglich, da jeder Bereich Risiko anders einschätzt
- Chancenmanagement ist zielführender als Risikomanagement
- Die hochdiskutierten IT-Risken sind meist nicht wirklich die existenzbedrohenden Risken in einem Unternehmen (Kollege von der Wirtschaftskammer OÖ)
- **Risiko muss vom Kunden her gedacht werden**
- Risikomanagement ist als **Business Continuity Management** zu sehen, das eine **Aufgabe des Business** ist → und welcher Risikoanteil darin ist IT-related?
- Häufig wird aber das gesamte **Business Risk Management „schleichend" an die IT übertragen**
- Es gibt aber auch einen Grund dafür: **Über die IT laufen alle Systeme/Geschäftsprozesse des Unternehmens** (ganzheitliche Sicht), deshalb auch prädestiniert → noch besser wäre das Thema allerdings beim Quality Manager angesiedelt
- **Corporate Trust Studie (AT und DE):** jedes 2. Unternehmen hat einen eCrime Verdachtsfall, 75% Schaden von 200 bis 500K (Kollege aus der Versicherungswirtschaft bietet an, Details zur Verfügung zu stellen)
- **IT-**Risiko ist abhängig vom **Durchdringungsgrad der Geschäftsprozesse** mit IT
- Daher ist **strategisches IT-Risikomanagement** ein wichtiges Element

Schwerpunkte:

- IT Risiko-Management ist ein **Teil des Business-Risk-Management**, welches NICHT Aufgabe der IT ist → Risiko muss „vom Kunden her gedacht werden"
- **Risiko muss kalkuliert/gemessen werden**, da es sonst nicht managebar ist
- Dazu muss es eine **End-to-End-Betrachtung** des Risikos (Business → IT und retour) geben, welches systematisch gesteuert werden muss (gibt es dafür Tools?)
- Organisatorisch muss es ein **Risk-Management-TEAM** geben, aus Business und IT; der Lead muss aber vom Business ausgehen