

Lernzielfragen Kapitel 7:

1. Welche Arten von IT-Risiken werden unterschieden? Geben Sie Beispiele dazu!

[Folie 21]

operative Risiken:

- a. Unzureichende Verfügbarkeit und Sicherheit:
 - i. Mitarbeiter des Unternehmens bekommen mehr/weniger Rechte, als ihnen eigentlich zusteht → Gefährdung von Daten, wenn z.B. ein MA das Recht bekommt diese zu löschen (Risiko hier ist auch, dass es zu geringe Zugriffsrechte gibt und dann die Sicherheitsmaßnahmen unterlaufen werden, um die tägliche Arbeit zu erledigen => „IT austricksen“ und zugleich Sicherheitsmanagement ad absurdum führen)
 - ii. Serverausfall → Services können dem Kunden nicht mehr angeboten werden, was zu einem Imageverlust, Kosten etc. führen kann
 - iii. geheime oder private Daten werden nicht ausreichend geschützt und sind von Dritten einsehbar
- b. Prozessdisfunktionalität (suboptimaler IT-Management Prozess Output):
 - i. Planen und Entwerfen der falschen oder veralteter Services für das Unternehmen bzw. Entwurf fehlerhafter Services
 - ii. seltene und unregelmäßige Überwachung der Datenbankserver
 - iii. instabiler Betrieb von IT Anwendungen aufgrund von zu hohen Performance Anforderungen für die genutzten Rechner/Server

strategische Risiken:

- c. Informationspathologien
 - i. die vom Geschäft gelieferten Produktionsdaten werden falsch interpretiert in CNC Maschinen übertragen, wodurch bei der Herstellung Fehler auftreten
 - ii. Abgabe von Informationen an das Business ohne diese vorher betriebswirtschaftlich „anzupassen“ → Fehlinterpretation kann zu Fehlern in der Planung führen
 - iii. wichtige Informationen, die ein Mitarbeiter mit Hilfe einer SW festhält werden durch Sicherheitsfilter ausgesondert oder zu eingeschränkt zugänglich gemacht
- d. Mangelnde Strategieorientierung:
 - i. IT konzentriert sich zu sehr darauf dem Unternehmen möglichst fortschrittliche Services anbieten zu können, anstatt zunächst das Notwendige zu Bearbeiten
 - ii. die Absprache der Aktionen der IT mit dem Business findet nur eingeschränkt oder gar nicht statt → Abstimmung der Strategien unmöglich
 - iii. daraus folgt der Kauf / die Lizenzierung von SW, die für das Erreichen der Unternehmensziele vollkommen unerheblich ist
- e. Gefährdung der Wettbewerbsfähigkeit:
 - i. IT ist bei den aktuellen Technologien auf dem Markt nicht mehr „up-to-date“ und kann ohne diese keine verhältnismäßig „besseren“ Services anbieten

- ii. durch den verpassten Anschluss an die gewinnbringenden Technologien entstehen Opportunitätskosten, das Einbüßen von Marktanteilen an die Konkurrenz etc.
- iii. Verschaffung eines Vorteils für die Konkurrenz aufgrund mangelhafter Reaktionsfähigkeit und Flexibilität, welche z.B. aus starren IT-Architekturen resultieren

2. Illustrieren Sie den Prozess der Risikowahrnehmung anhand eines Beispiels!

[Folie 10]

- a. Selektion und Interpretation von Umweltmerkmalen:
der steigende Preis von Strom und Benzin in den letzten Monaten aufgrund von (künstlicher?) Verknappung von entsprechenden Rohstoffen
- b. Kognitive Konstruktion von Risiken:
 - i. Risiko (zu) hohe Rechnungen von dem aktuellen Stromlieferanten
 - ii. Risiko erhöhter Benzinkosten des Fuhrparks (LKW...)
 - iii. Risiko des Verbrauchs der Rohstoffe bevor Alternativen gefunden werden können (hier möglicherweise **Risikofehl Wahrnehmung** → **siehe künstliche Verknappung**)
- c. Aggregation von Risiken:
 - i. Risiko erhöhter laufender Kosten (die ersten beiden)
 - ii. Risiko von „Versorgungsengpässen“ (letztes Risiko)
- d. Analyse von Einflussgrößen und Schwachstellen:
 - i. Inflation als eine Einflussgröße der Beitragserhöhungen
 - ii. Ausstieg Deutschlands aus der Produktion von Atomstrom
 - iii. nicht unendliche Vorkommen von Ölreserven auf der Welt
- e. Maßnahmenplanung und –durchsetzung:
 - i. Finden von Alternativen und günstigeren Stromerzeugern (z.B. über www.verivox.de)
 - ii. Nutzung alternativer/erneuerbarer Energielieferanten (Windkraft etc.)
 - iii. Anschaffung sparsamerer Motoren für den Fuhrpark oder gar Ausweiten der Auslieferung auf den Schienenverkehr
- f. Risikokommunikation:
 - i. Weitergabe des erkannten Risikos an die Mitarbeiter (→ kreative Lösungen durch MA möglich...)
 - ii. Weitergabe an Partner-/Geschwisterunternehmen

Beispiel hier aus dem **Unternehmens/IT-Bereich** wäre schön => **Hinweis für die Klausur:** „anhand eines Beispiels“ meint in der Regel „anhand eines Beispiels aus dem Unternehmens- oder IT-Bereich“ ;-)

Vielleicht wäre hier abschließend noch ein Satz zu „**Risikofehl Wahrnehmungen**“ nicht verkehrt (oder ins Beispiel eingebettet). Es gibt einen schönen Ausspruch von einem Umweltrisikoforscher (Peter Sandmann, muss man nicht kennen): „**The risks that kill you are not necessarily the risks that anger and frighten you.**“

//...

Informationspathologie ist ein Sammelbegriff in der Betriebspsychologie für verschiedene Aspekte, die bei Erzeugung, Austausch und Anwendung von Informationen fehlschlagen können, mit der Konsequenz, dass Entscheidungen auf Basis einer unzulänglichen Informationsgrundlage gefällt werden.

Qualität von Information und Kommunikation werden unter diesem Oberbegriff in der Betriebspsychologie untersucht. Man unterscheidet im wesentlichen die individuelle Informationspathologie aufgrund unzureichender Grundkenntnisse oder Betriebsblindheit eines Mitarbeiters, die interaktionsbezogene Informationspathologie aufgrund eingeschränkten Meinungsaustauschs oder Unverständnis zwischen Spezialisten und die wissensbezogene Informationspathologie aufgrund naiven Realismus bzw. der Überbetonung von Fakten und quantitativen Aussagen. Zusammenfassend lassen sich mit diesem Modell Kommunikationsfehler analysieren und in Folge vermeiden. [Muss man also nicht für die Klausur wissen, wenn die Frage kommt...]

3. Veranschaulichen Sie methodische Probleme des IT-Risikomanagements anhand von Beispielen!

[Folie 11 bis 13]

a. Probleme quantitativer Methoden:

- i. (Skalenbrüche, Skalenübergänge) In einer IT Abteilung wurde durch eine Analyse festgestellt, dass:
 - Zur gleichen Zeit mehrere Nutzer eine Anwendung beanspruchen können (nominale Aussage)
 - Der zuständige Server dabei nur sehr selten ausfällt (ordinale Aussage)
 - Umwandlung in kardinale Werte → Subjektivität und Berechnungen mit diesen (Konsistenz? → Skalenbruch)
- ii. (Orientierung an Vergangenheitsdaten)
 - bis die Analyse und möglicherweise Umwandlung der Daten in kardinale Werte (wie geht denn eine solche Umwandlung → z.B. Festlegen von einem Wert von 0,2 für ein „mittelmäßig“) abgeschlossen ist, hat sich Situation grundlegend verändert
 - dem Beispiel oben folgend:
 - o bis zum Abschluss der quantitativen RM Methode und Einstufung des Risikos wird die Anwendung immer öfter gleichzeitig genutzt, was den Server häufiger abstürzen lässt
 - Risikoeinschätzung erfolgt zeitverzögert
- iii. (konkret in Zahlenform) siehe oben:
 - die Umwandlung von qualitativen Aussagen in quantitative Werte nicht immer eindeutig
 - Beispiel: Im Vergleich zur Konkurrenz ist unsere Produktqualität eher passabel (Was bedeutet „eher“, wie ist „passabel“ einzustufen?)

b. Probleme qualitativer Methoden:

- i. (Wechselwirkung von Szenarien → Komplexität)
 - die Zusammenhänge zwischen den einzelnen Risiken, Schwächen etc. der Systeme ziehen sich aufgrund großer monolithischer Systeme durch das gesamte Unternehmen
 - die Darstellung dieser Zusammenhänge in Modellen oder sonstigen qualitativen Methoden zu umfangreich (und durch den Menschen (beschränkte Informationsverarbeitungskapazität, verborgene Wechselwirkungen in „Tiefenstrukturen“) nicht vollständig zu erfassen) → unübersichtlich

- mit solchen (riesigen) Modellen lässt sich kein RM betreiben → ineffizient
- Beispiel: Ein Szenariodiagramm muss immer weiter in Unterszenarien aufgeteilt werden, da sonst nicht genügend Informationen vorhanden sind. In jedem Diagramm bestehen zusätzlich weitere Constraints und Schleifen. Zu guter letzt ergeben sich teilweise aus der Länge der Handlungsketten entsprechend lange (unübersichtliche) Diagramme.
- ii. (ohne Hand und Fuß)
 - aufgrund der Kombination von qualitativen Aussagen miteinander und mit der derzeitigen Situation wird das Risiko festgestellt, einen Verlust der Servicequalität gegenüber dem Kunden in den nächsten Monaten zu erleiden
 - fragt nun jemand nach dem Grund für gerade diese Interpretation der Umstände, so existieren keinerlei Werte, die diese Entscheidung konkret belegen würden (z.B. Serverstabilität um 10% gesunken etc.)
- iii. (Darstellung der Wahrscheinlichkeit) Da in qualitativen RM Methoden kardinale Werte kaum auftauchen, kann die Wahrscheinlichkeit für das Eintreten eines Szenarios nur schwierig dargestellt werden:
 - Beispiel: Bei einer hohen Belastung unseres Webserver (was bedeutet „hohe Belastung“ und wie oft tritt sie ein?) sinkt die Reaktionszeit auf Nutzeraktionen um 10%.

Klausurfragen Kapitel 7:

1. Im Rahmen der Analyse von Bedrohungen der IT Infrastruktur schlägt ein IT-Mitarbeiter die Durchführung einer statistischen Simulation auf Basis der durch die Firewall und Intrusion Detection-Systeme automatisch protokollierten, abgewehrten Angriffe des letzten Jahres vor. Was ist von diesem Vorschlag zu halten? (5 Punkte)
 - a. Die Angriffe können durchaus Hinweis auf die Bedrohung der IT Infrastruktur sein.
 - b. Statistische Simulation = quantitative RM Methode
 - i. Probleme quantitativer RM Methoden [Folie 13]:
 - Realistische Wahrscheinlichkeiten vs. Schätzung?
 - „Worst-Case-Fixierung“
 - Eigene Schwächen in zahlenform?
 - Skalenbrüche, -übergänge
 - Orientierung an Vergangenheitsdaten
 - Aufwand, Nachvollziehbarkeit
 - c. v.a. Orientierung an Vergangenheitsdaten bei diesem Beispiel:
 - i. die protokollierten Werte des letzten Jahres spiegeln nicht unbedingt die aktuelle Bedrohung der IT Infrastruktur wider
 - ii. Simulation auf Basis dieser Daten kann zu unangemessener Risikoeinschätzung führen
 - d. kann nur ein kleiner Ausschnitt einer umfassenden Bedrohungsanalyse sein

Lernzielfragen Kapitel 8:

1. Was sind Gemeinsamkeiten und was sind Unterschiede zwischen der Sichtweise auf IT-Governance nach Weill/Ross und nach dem COBIT-Standard?

[Folie 7+9]

- a. Sichtweise nach Weill/Ross:
 - i. „IT Governance im engeren Sinne“
 - ii. interne Vergabe von Entscheidungsrechten
 - iii. Fokus auf strategische oder Prozesse mit Business Bezug
 - iv. relevant für große Organisationen mit dezentralen IT Einheiten
- b. Sichtweise nach COBIT:
 - i. Control Objectives for Information and related Technology
 - ii. “IT-Governance im weiteren Sinne”
 - iii. erweitert die Sichtweise von Weill/Ross um mehrere Aspekte
 - Führungsaspekte
 - Organisationsstrukturen und Prozesse
 - Erreichung der Unternehmensziele mit Hilfe von IT
 - Ausgleich zwischen Rendite und Risiken

Insofern ist die Sichtweise von IT-Governance des COBIT Frameworks eine Erweiterung der Sichtweise von Weill/Ross, woraus sich die Unterschiede und Gemeinsamkeit implizit ergeben. [Gute Antwort und gute Möglichkeit, eine umfängliche Gegenüberstellung in der Klausur abzukürzen. Allerdings sorgfältig aufpassen, dass man nicht zu stark verkürzt. ;-)]

2. Welche der aktuellen Themen des IT Managements (Kapitel 4) haben einen starken Bezug zu IT-Governance und warum? Diskutieren Sie den IT-Governance Bezug eines Themas im Detail.

- a. „Arbeit in der IT Abteilung“ (z.B. iWorker)
 - i. Die Koordination der Arbeit in der IT Abteilung wird über IT Governance Grundsätze geregelt
 - ii. IT Governance steuert die Art und Weise, wie in der IT Abteilung gearbeitet wird
- b. Bedeutung des CIO & der IT Abteilung
 - i. auch ein Fokus auf das IT-Business-Alignment → Beziehungsmanagement des CIO + festigen seiner Position
 - ii. erhöhte Bedeutung der IT Abteilung durch verbesserte Effizienz und Effektivität
- c. *Manage IT as a Business*
 - i. gerade hier ist der Zusammenhang sehr stark
 - ii. Manage IT as a Business kann als Grundsatz der IT Governance Idee verstanden werden
 - iii. IT Governance zielt darauf ab, die IT Abteilung nach dem Vorbild des Business zu steuern
 - iv. es wird zum Beispiel durch Standards wie COBIT eine „weitere“ Sichtweise auf die IT und ihre Prozesse betont
 - v. IT Governance erreicht eine Verschiebung der bisher recht technischen/IT-lastigen Sichtweise der IT auf eine globalere Sichtweise → Zusammenhänge der IT mit dem Rest des Unternehmens spielen eine größere Rolle

- vi. IT nicht nur auf operativer sondern vor allem auch auf taktischer sowie strategischer Ebene vorhanden → dementsprechend auch strukturierte Steuerung auf diesen Ebenen notwendig
- d. IT-Projektmanagement
 - i. das Management der IT Projekte ist ein fester Bestandteil des IT Governance (so zum Beispiel des COBIT Frameworks)
- e. Der CIO als Mitglied des Vorstands
 - i. damit der CIO sich als Mitglied des Unternehmensvorstandes etablieren kann
 - Verbesserung der Beziehungen
 - Verbesserung Effizienz + Effektivität der IT
 - verständliche Governance Strukturen
- f. Bedeutung von Standards im IT-Management
 - i. auch im Bereich des IT Governance wird Forschung betrieben oder entwickeln sich Standards aus best practise Erfahrungen