

„AAA“ *in der IT!*

... kein Risiko mehr fürs Unternehmen?

Solvency II und Basel II fordern die Eigenmittelhinterlegungspflicht für operationelle Risiken und unterstreichen hiermit deren hohe Bedeutung. Aufgrund der stetig steigenden Kosten und der hohen Abhängigkeit für den Unternehmenserfolg rückt die Informationstechnologie in den Mittelpunkt der Betrachtungen. Die IT als Komponente der sogenannten „Softfacts“ kann nur dann sinnvoll identifiziert, bewertet und gesteuert werden, wenn diese in „Hardfacts“ dargestellt werden kann. Die Methode CRISAM zeigt einen pragmatischen Weg auf, der sich an dem Standard & Poors Ratingansatz orientiert und somit einen Benchmark der Informationstechnologie zu den Finanz- und Marktrisiken liefert.

Die Relevanz macht den Unterschied

Risiko ist per se jedoch noch keine Bedrohung, sondern gefährdet erst durch eine entsprechende Relevanz den jeweiligen Geschäftsprozess. Diese Beziehung und die Rolle der IT in Relation zum unterstützten Prozess sind in der Beantwortung der Frage „Wo ist das, im Sinne der Nutzenbilanz sinnvolle und vertretbare Sicherheitsniveau?“ bedeutungsvoll.

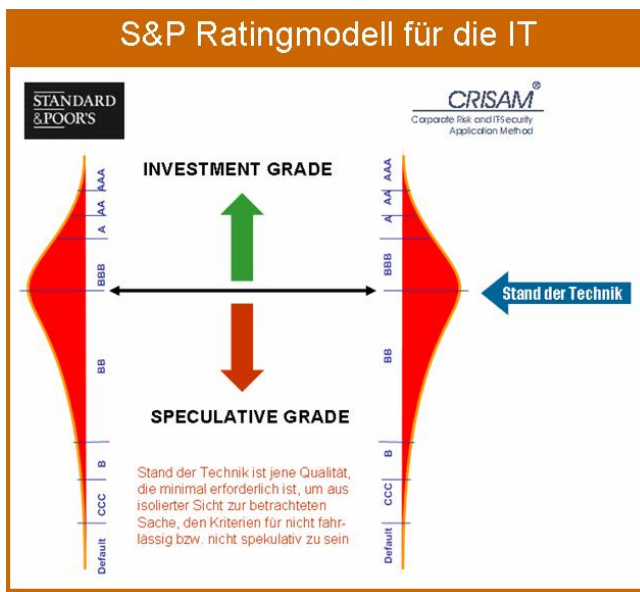
Risiko ist nicht nur die Gefahr des Eintretens eines negativen Ereignisses. Risiko im kommerziellen Sinn ist auch die Gefahr einer Überinvestition von Maßnahmen in der IT, die Kapital binden ohne einen Nutzen zu bringen. Das sinnvolle und vertretbare Niveau, im Sinne der Nutzenbilanz, ist genau dort zu finden, wo Kosten und resultierender Nutzen in Balance gehalten werden. Im Sinne einer Basel II Betrachtung bedeutet dies, dass der Nutzen einer „AAA“ gesicherten IT Infrastruktur, in einem mit „BB“ gerateten Unternehmen kaum darstellbar ist. Ganz im Gegenteil, die Überinvestition in die „High Secure“ IT verursacht hohe Kapitalaufwendungen, die in einer Bilanzanalyse negativ durchschlagen. Auch im Unternehmen gilt der Grundsatz, dass das schwächste Glied die Festigkeit der gesamten Kette bestimmt. Der Einsatz der Informationstechnologie darf keine vom Unternehmen abgekoppelte Entwicklung nehmen, sondern ist aus der Balanced Scorecard, den darin enthaltenen Visionen und Strategien abzuleiten und auf das Geschäftsfeld abzustimmen. Damit diese umfassende Sicht möglich wird, ist es erforderlich, die IT in einem zum Gesamtunternehmen kompatiblen Bewertungsmaßstab (Ratingkennzahl) zu transformieren.

Eine Ratingkennzahl für die IT.

Operatives Risiko aus dem Betrieb der Informationstechnologie zur Unterstützung der wertschöpfenden Geschäftsprozesse ist jene Bedrohung, wenn die IT ihren Verbindlichkeiten aus einem Service Level Agreement (SLA) nicht mehr nachkommen kann und dem unterstützten Geschäftsprozessen daraus ein Schaden (Reduktion der Wertschöpfung) erwächst.

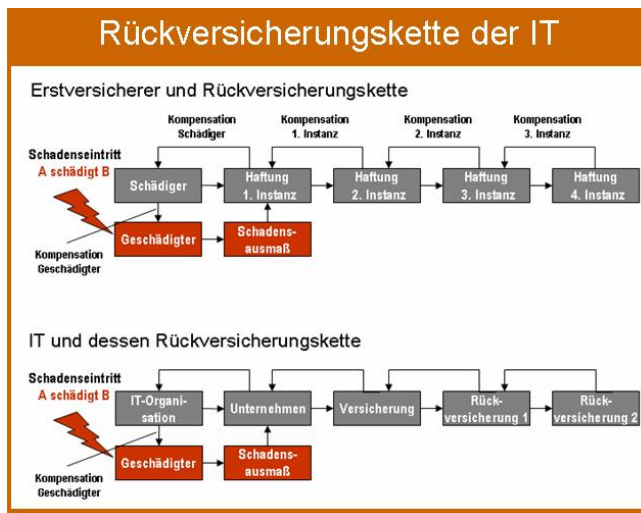
Diese Risiken können identifiziert und durch Kennzahlen beschrieben werden. Sowohl Finanz- bzw. Versicherungsrisiken als auch IT-Risiken können grob als spekulativ oder konservativ (Investment Grade) kategorisiert werden. Diese groben Kategorien sind wiederum in Gruppen gleichwertiger Risikoeigenschaft unterteilt.

Die Kriterien des Finanz- und Versicherungsratings sollten auch dem Rating der IT-Risiken zugrunde gelegt werden. Mit dieser gleichwertigen Ratingaussage zur IT, kann im unternehmensweiten Risikomanagement IT-Risiko zu Finanz-, Markt- und anderen unternehmensrelevanten Risiken positioniert werden.



Standard & Poor's (S&P) legt für die Bewertung der Versicherungsgesellschaften den „Insurer Financial Strength-Ratings“ Ratingansatz zu Grunde. Dabei werden operative Risiken der Versicherungsunternehmen dem risikotragenden Kapital gegenübergestellt und aus dieser Verhältniszahl eine Ratingkennzahl abgeleitet.

Jedes Unternehmen ist als wirtschaftliche Einheit für operative Risiken ihrer IT verantwortlich. Dieses kann nach Maßgabe ihrer finanziellen Leistungsfähigkeit sich wiederum eine Rückversicherung bei Konzernmüttern oder Versicherungsunternehmen einholen. Somit übernimmt für das operative Risiko der Unternehmens-IT, das Unternehmen selbst die Versicherungsfunktion erster Instanz. Eine Risikobeurteilung dieser ersten Versicherungsinstanz, so auch des Unternehmens, erfolgt nach dem S&P „Insurer Financial Strength-Ratings“ Ansatz.



Dieser S&P Ansatz bewertet operative Risiken von Versicherungsunternehmen als jene Gefahr, dass eine Gesellschaft ihren Verpflichtungen aus einem Versicherungsvertrag nicht mehr nachkommen kann. Die Bezugslinie für die Bewertung und Einstufung der ermittelten Kennzahlen in eine Ratingkategorie, ist ein langfristiger Erfahrungsschatz, der durch Auswertungen und permanente Marktbeobachtung gewonnen wurde und kontinuierlich weitergepflegt wird. Mit dieser Kennzahl ist feststellbar, ob aufgrund einer Ratingkennzahl das operative Risiko des Versicherungsunternehmens in Richtung „Investment Grade“ oder „Speculative Grade“ zeigt.

Das operative Risiko eines IT-Dienstleisters (interne IT oder auch Outsourcing Nehmer in einem Outsourcing Verhältnis), nämlich die Gefahr, dass dieser seinen Verpflichtungen aus einer Service Level Vereinbarung nicht mehr nachkommen kann, ist analog dem Versicherungsunternehmen zu werten. Die Bezugslinie für die Bewertung und Einstufung der ermittelten Kennzahlen in eine Ratingkategorie, analog dem langfristigen Erfahrungsschatz in der Versicherungsindustrie, stellt der **Stand der Technik** dar.

Was ist der Stand der Technik ?

Der Stand der Technik wird vielen Entscheidungen, Investitionen in der Wirtschaft oder auch Recht und Ordnung bei Gericht zugrunde gelegt. Es gibt jedoch keine Instanz, die den Stand der Technik aktuell, objektiv und nachvollziehbar darstellen kann.

Jeder, der auf diesen Stand zurückgreifen möchte, muß subjektiv und nach dem „Gefühl im Bauch“ entscheiden.

Nachfolgende Definition (<http://www.uni-protokolle.de/Lexikon/Technologie>) soll den Begriff und dessen Bedeutung näher erklären.

Als Stand der Technik werden technische Möglichkeiten zu einem bestimmten Zeitpunkt bezeichnet, basierend auf gesicherten Erkenntnissen von Wissenschaft und Technik. Der Stand der Technik beinhaltet auch, daß er wirtschaftlich durchführbar ist. Dies heißt nicht, daß jedes Unternehmen sich den Stand der Technik leisten kann, aber die Mehrheit in einem betroffenen industriellen Sektor.

Nach dieser bestimmen:

- Technische Möglichkeiten
- Zeitpunkt
- Umsetzung und Nutzung in der Praxis
- Wirtschaftlichkeit
- Mehrheit

diesen Stand der Technik.

Da für die IT derzeit kein methodisches und allgemein anerkanntes Instrumentarium zu Verfügung steht, geschieht dies anlaßbezogen durch Experten. Dabei spielen subjektive Einschätzungen eine nicht unwesentliche Rolle und dementsprechend widersprüchlich können die Expertenmeinungen ausfallen.

Damit diese Subjektivität reduziert werden kann, ist dieser objektiv und aus gefestigten Meinungen von Herstellern und Nutzern zyklisch festzuschreiben.

Jeder Risikomanagement- und IT Governanceprozess erfordert einen objektiven und nachvollziehbaren STAND DER TECHNIK, um Effizienz und Effektivität von Maßnahmen nachweisen zu können.

Der Wert der IT.

Entsprechend der von Standard & Poor`s verwendeten verbalen Bewertung der Risikoqualität wird die Abweichung von der Bezugslinie (Übergang von Investment- nach Speculative Grade), festgestellt und eine Einstufung durchgeführt. In Analogie zu diesen Bewertungskriterien erfolgt eine Einstufung der operationalen Risiken der IT in die jeweilige IT-Ratingkategorie.

Die konkrete Aufgabe des Risikomanagements ist dabei alle potentiellen Gefahren für eine negative Einflussnahme auf den Kapitalertrag des Unternehmens zu identifizieren, zu bewerten und angemessene Maßnahmen zu ergreifen, um diese potentiellen Bedrohungen auf ein, für das gesamten Unternehmen angepasstes Niveau zu reduzieren.

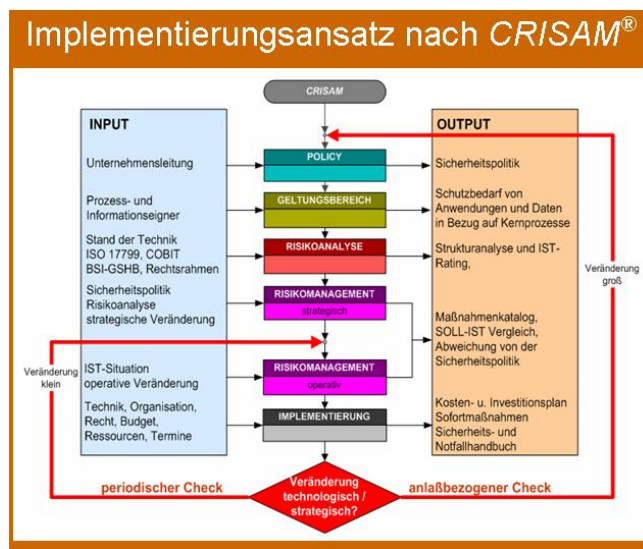
Aus der so formulierten betriebswirtschaftlichen Zielsetzung des Risikomanagements, ist die Bewertung des IT-relevanten Risikos als Reihe von positiven und auch negativen Cash Flows zu betrachten. Der Nutzen aus dem Einsatz des Werkzeuges IT ist als positiver Cash Flow, der finanzielle Aufwand aus den Investitionen und dem Betrieb als Kapitalabfluss zu werten. Potentielle Gefährdungen sind als negativer Cash Flow mit dem Wert der verbleibenden Risiken anzusetzen.

Mit dieser Transformation des Risikomanagements der Informationstechnik in eine betriebswirtschaftliche Wertebetrachtung, gewinnt die IT eine zusätzlich wertbare Größe. Die Aufgabenstellung des Risikomanagements ist es, einen positiven Kapitalwert aus den getätigten IT-Investitionen, dem gestifteten Nutzen und den abgewiesenen Gefahren

darzustellen. Die Bewertung dieses erfolgt nach anerkannten und in der Betriebswirtschaft bewährten Investmentmethoden.

Risikomanagement ist mehr als eine Momentaufnahme potentieller IT-bedingter Risiken!

CRISAM (Corporate Risk and IT-Security Application Method) stellt eine 6-stufige Methode dar, die auf dem Standard & Poors Versicherungsansatz basiert und die Relevanz der Bedrohungen zu den Geschäftsprozessen berücksichtigt. Etwaige Schwachstellen können aufgrund der abgebildeten Abhängigkeiten bis auf einzelne Risikoobjekte zurückverfolgt werden. Das Ergebnis ist eine Bewertung nach dem bekannten S&P Ratingmodell und ermöglicht damit eine objektive Positionierung zu den Finanz- und Marktrisiken. Als Risikomanagement läßt es sich nahtlos in bestehende Managementprozesse integrieren und ist für bestehende und zukünftige Standards und Normen offen.



STUFE 1: POLICY

CRISAM leitet aus den strategischen Festlegungen des Unternehmens zunächst eine von der Unternehmensleitung freizugebende und bindende Sicherheitspolitik ab. Diese Politik ist als der strategische Auftrag im Umgang mit Informationstechnologie an das Unternehmen zu betrachten. In klaren, als Leitsätze formulierten Anweisungen, ist diese Sicherheitspolitik auch als Abgrenzung zu sehen, in deren Grenzen anstehende Entscheidungen getroffen werden müssen. Analog einem Piloten, dem das Flugzeug auf einem Flug zum Zielflughafen anvertraut wird, hat der letztverantwortliche Manager im Unternehmen alle einwirkenden Umweltbedingungen mit seinem Steuerknüppel auszugleichen. Als Beschreibung des vom Management vorgegebenen Kurses dient die Sicherheitspolitik, die der Stellung des Steuerknüppels im Unternehmen entspricht.

STUFE 2: GELTUNGSBEREICH

Im Geltungsbereich identifiziert *CRISAM* die, in der Sicherheitspolitik erfassten Geschäftsprozesse. Diesen werden IT-Anwendungen und Datenbestände in ihrer Relevanz zum jeweils unterstützten Prozess in Bezug gesetzt. Geschäftsprozesse definieren dabei ihre Service Level Anforderungen an IT-Anwendungen, die von der IT-Organisation in der Rolle eines Dienstleisters zu erfüllen ist.

STUFE 3: RISIKOANALYSE

Risikobeeinflussende Ressourcen und Prozesse (z.B. Serversysteme, Stromversorgung oder auch Beschaffungsvorgänge) werden in einer Hierarchie von Ressourcen angeordnet. Experten bewerten mit Hilfe von nachvollziehbaren Metriken das operationelle Restrisiko auf jeder Hierarchiestufe dieses IT-Ressourcen Baumes. Für den Reifegrad des IT-Risikomanagements ergibt sich eine Ratingkennzahl, analog der aus dem Finanzbereich bekannten Bezeichnung und Skalierung. Ein Wert von BBB entspricht dabei dem Stand der Technik. Darüber liegende Werte bis AAA entsprechen einem vorbeugenden, darunter liegende Werte bis CCC einem spekulativen IT-Risikomanagement.

STUFE 4/5: RISIKOMANAGEMENT

Die Abweichung des analysierten Ratingwertes zum Sollwert aus der Sicherheitspolitik bildet die Grundlage für den kontinuierlich durchzuführenden Verbesserungsprozess, ähnlich dem Qualitätsmanagement nach ISO 9001. Maßnahmen zur Erfüllung der Vorgabequalität werden identifiziert.

SCHTITT 6: IMPLEMENTIERUNG

Organisations- und Technologieprojekte werden aus den erkannten Maßnahmen initialisiert und in die Umsetzung geführt.

Zusammenfassung

Unter dem Lichte von Solvency II und Basel II wird die Eigenmittel hinterlegung von operationellen Risiken für Banken und Versicherungen verpflichtend vorgeschrieben. Um Risiken bzw. IT-bedingte Restrisiken managen zu können, sind grundsätzliche Rahmenbedingungen im Unternehmen zu schaffen:

1. Von letztendlich verantwortlicher Stelle ist eine Zielvorgabe als Positionierung im Umgang mit IT-relevanten Risiken vorzugeben (Sicherheitspolitik).
2. Potentielle Bedrohungen aus dem Einsatz des Werkzeuges IT für die wertschöpfenden Geschäftsprozesse sind zu identifizieren.
3. Das Werkzeug IT selbst ist auf Abweichungen zum aktuell gültigen Stand der Technik zu überprüfen.
4. Die Aktualität der eingesetzten Technologien ist nach dem jeweils geltenden Stand der Technik zu beurteilen. Abweichungen zu diesem Stand sind jedoch über den Nutzungsgrad (Relevanz) zum unterstützten Geschäftsprozess anzupassen.

Identifizierte Fehlabweichungen von der Zielvorgabe (Sicherheitspolitik) stellen eine potentielle Bedrohung im Sinne eines Unternehmensrisikos dar und sind durch Maßnahmen zu kompensieren.

Dieser Ablauf ist im Unternehmen als kontinuierlicher Verbesserungsprozess (KVP) zu implementieren

Die Positionierung und Analyse von Abweichungen bedingt ein nachvollziehbares Bewertungs- und Beurteilungskonzept der IT-Infrastruktur und Organisation, sowie einer reproduzierbaren Beurteilung des potentiellen Restrisikos. Diese Transformation des IT-Risikomanagement in die Betriebswirtschaft ermöglicht es, nach bekannten und anerkannten Methoden Probleme beurteilen und Entscheidungen treffen zu können.

Dieser Managementprozess gibt dem Vorstand, Geschäftsführer bzw. Unternehmer einen Steuerknüppel in die Hand, mit dem er sein Unternehmen im Umfeld Haftung, Finanzierung und Markt risikoadäquat pilotieren kann.

Literatur

Ratingdefinitionen für Insurer Financial Strength-Ratings; Standard&Poor's 2000

Rating, ein Aufsatz zum Thema Rating; Prof. Dr. Ottmar Schneck Professor für Banking, Finance & Risk an der European School of Business (ESB) Reutlingen

Der Stand der Technik; Dr. Hans Langer Richter am Landesgericht für Zivilrechtssachen Wien

Investment Opportunities as Real Options: Getting Started on the Nubers; Havard Business Review; July-August 1998; Timothy A. Luehrmann

Capital Projects as Real Options: An Introduction; Havard Business Review; March 1995; Timothy A. Luehrmann

Investigating the Risk-Return Relationship of Information Technology Investment: Firm-Level Empirical Analysis; Graduate School of Management University of California, Irvine; Sanjeev Dewan, Charles Shi, Vijay Gurbaxani; 2003