

G 59071
4,50 EUR*

RATING **C** **aktuell**

Information für Unternehmen und Finanzdienstleister

06/2005
Dezember/Januar

www.ratingaktuell-news.de
www.ratingaktuell-ticker.de

* zzgl. Versand und 7 % MwSt.

OPERATIONELLES RISIKO

Rating von IT-Risiken

BANKEN

Wie Rating-Systeme
durch Datenpflege
optimiert werden

INTERVIEW

Ralf Garrn von Euler
Hermes Rating im
Gespräch

**Basel II:
Endlich auf der Zielgeraden**

Operationelles Risiko: Rating von IT-Risiken

Manfred Stallinger

Solvency II und Basel II fordern die Eigenmittelunterlegung für operationelle Risiken und unterstreichen damit deren hohe Bedeutung. Gleichzeitig rückt auf Grund der stetig steigenden Kosten und der hohen Abhängigkeit für den Unternehmenserfolg die Informationstechnologie (IT) in den Mittelpunkt der Betrachtungen. Die IT als Komponente der „Soft Facts“ lässt sich nur dann sinnvoll identifizieren, bewerten und steuern, wenn sie in „Hard Facts“ dargestellt werden kann. Die „Corporate Risk and IT-Security Application Method“ (CRISAM) zeigt einen pragmatischen Weg auf, der sich an dem von Standard & Poor's (S&P) entwickelten Rating-Ansatz orientiert und somit einen Benchmark der Informationstechnologie zu den Finanz- und Marktrisiken liefert.



Das Risiko ist per se noch keine Bedrohung, sondern gefährdet den Geschäftsprozess erst durch eine entsprechende Relevanz. Risiko ist nicht nur die Gefahr des Eintretens eines negativen Ereignisses, sondern im kommerziellen Sinne auch die Gefahr einer Überinvestition von Maßnahmen in der IT, die Kapital binden, ohne einen Nutzen abzuwerfen. Das sinnvolle und vertretbare Niveau im Sinne der Nutzenbilanz ist dort zu finden, wo Kosten und resultierender Nutzen in der Balance gehalten werden. Im Sinne einer Rating-Betrachtung bedeutet dies, dass der Nutzen einer ‚AAA‘ gesicherten IT-Infrastruktur, in einem mit ‚BB‘ gerateten Unternehmen kaum dar-

stellbar ist. Im Gegenteil: Die Überinvestition in die „High Secure“-IT verursacht hohe Kapitalkaufwendungen, 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 einer eventuell implementierten 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 (Rating-Kennzahl) zu transformieren (Abb. 1).

Eine Rating-Kennzahl für die IT

Ein operatives Risiko aus dem IT-Betrieb zur Unterstützung der wertschöpfenden Geschäftsprozesse entsteht, 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 kategorisiert werden. Diese groben Kategorien sind wiederum in Gruppen gleichwertiger Risiko-Eigenschaften unterteilt. Die Kriterien des Finanz- und Versicherungsratings können auch dem Rating der IT-Risiken zu Grunde gelegt werden. Mit dieser Rating-Aussage zur IT kann im unternehmensweiten Risiko-Management IT-Risiko zu Finanz-, Markt- und anderen unternehmensrelevanten Risiken positioniert werden. Die Rating-Agentur Standard & Poor's (S&P) legt für die Bewertung von Versicherungsgesellschaften den „Insurer Financial Strength“-Rating-Ansatz zu Grunde. Dabei werden operative Risiken der Versicherungsunternehmen dem risikotragenden Kapital gegenübergestellt und aus dieser Verhältniszahl eine Rating-Kennzahl abgeleitet. Jedes Unternehmen ist als wirtschaftliche Einheit für operative Risiken ihrer IT verantwortlich. Dieses kann nach Maßgabe ihrer finanziellen Leistungsfähigkeit sich wiederum eine Rück-

versicherung bei Konzernmüttern oder Versicherungsunternehmen einholen. Somit übernimmt für das operative Risiko der Unternehmens-IT, das Unternehmen selbst die Versicherungsfunktion erster Instanz. Eine Risiko-Beurteilung dieser ersten Versicherungsinstanz, so auch des Unternehmens, erfolgt nach dem S&P „Insurer Financial Strength-Ratings“-Ansatz.

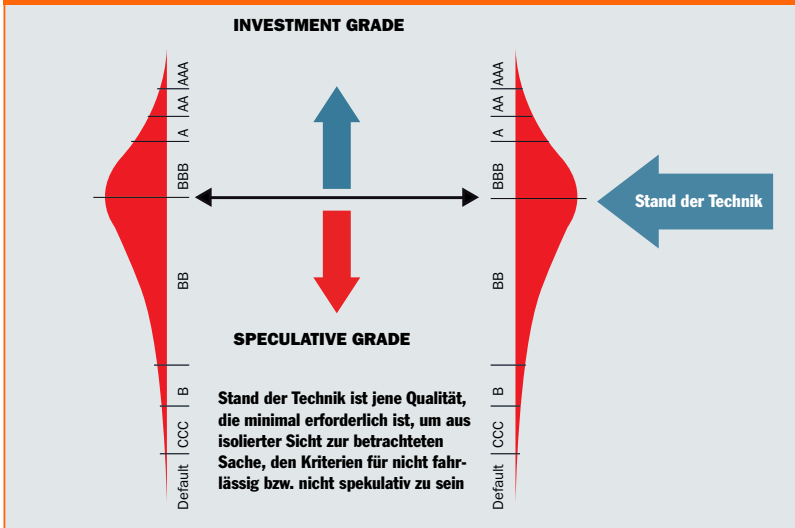
Dieser Ansatz bewertet Risiken von Versicherungsunternehmen als jene Gefahr, dass eine Gesellschaft ihren Verpflichtungen aus einem Versicherungsvertrag nicht mehr nachkommen kann. Die Bezugslinie für die Bewertung und Einstufung der ermittelten Kennzahlen in eine Rating-Kategorie ist ein langfristiger Erfahrungsschatz, der durch Auswertungen und permanente Marktbeobachtung gewonnen wurde und kontinuierlich weitergepflegt wird. Mit dieser Kennzahl ist feststellbar, ob auf Grund einer Rating-Kennzahl 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), also 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 Rating-Kategorie (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 Management-, Gerichts- oder Investitionsentscheidungen zu Grunde gelegt. Es gibt jedoch keine zentrale Instanz, die den Stand



Abb. 1: S&P Ratingmodell für die IT



der Technik aktuell, objektiv und nachvollziehbar darstellt. Jeder, der auf diesen Stand zurückgreifen möchte, muss subjektiv und nach dem „Gefühl im Bauch“ entscheiden. Als Stand der Technik werden technische Möglichkeiten zu einem bestimmten Zeitpunkt bezeichnet, basierend auf gesicherten Erkenntnissen von Wissenschaft und Technik. Der Stand der Technik impliziert auch, dass er wirtschaftlich durchführbar ist. Dies bedeutet nicht, dass jedes Unternehmen sich den Stand der Technik leisten kann, aber die Mehrheit in einem betroffenen industriellen Sektor. Den Stand der Technik bestimmen

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

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. Dementsprechend widersprüchlich kön-

nen die Expertenmeinungen ausfallen. Damit diese Subjektivität reduziert werden kann, ist dieser objektiv und aus gefestigten Meinungen von Herstellern und Nutzern zyklisch festzuschreiben. Jeder Risiko-Management- und IT-Governance-Prozess erfordert einen objektiven und nachvollziehbaren Stand der Technik, um Effizienz und Effektivität von Maßnahmen nachweisen zu können.

Der Wert der IT

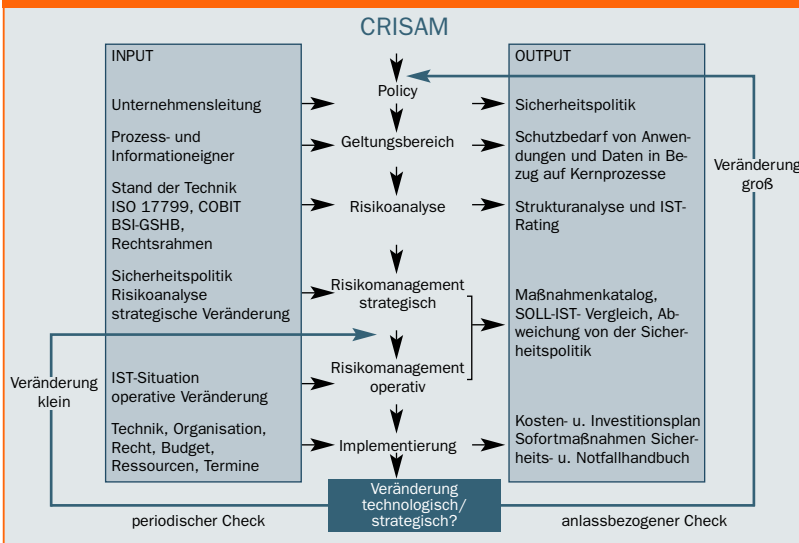
Entsprechend der von S&P angewandten Bewertung der Risiko-Qualität wird die Abweichung von der Bezugslinie (Übergang von Investment- nach Speculative Grade), festgestellt und eine Einstufung durchgeführt. In Analogie zu diesen Bewertungskriterien erfolgt eine Einstufung der operationalen Risiken der IT in die jeweilige IT-Rating-Kategorie. Die konkrete Aufgabe des Risiko-Managements ist dabei alle potenziellen Gefahren für eine negative Einflussnahme auf den Kapitalertrag des Unternehmens zu identifizieren, zu bewerten und angemessene Maßnahmen zu ergreifen, um diese potenziellen Bedrohungen auf ein für das gesamte Unternehmen ange-

passtes Niveau zu reduzieren. Aus der so formulierten betriebswirtschaftlichen Zielsetzung des Risiko-Managements ist die Bewertung des IT-relevanten Risikos als Reihe von positiven und auch negativen Cashflows zu betrachten. Der Nutzen aus dem IT-Einsatz ist als positiver Cashflow, der finanzielle Aufwand aus den Investitionen und dem Betrieb als Kapitalabfluss zu werten. Potenzielle Gefährdungen sind als negativer Cashflow mit dem Wert der verbleibenden Risiken anzusetzen. Mit dieser Transformation des Risiko-Managements der IT in eine betriebswirtschaftliche Wertebetrachtung gewinnt die IT eine zusätzlich wertbare Größe. Die Aufgabenstellung des Risiko-Managements 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.

Risiko-Management ist mehr als eine Momentaufnahme potenzieller IT-bedingter Risiken!

Das Verfahren CRISAM stellt eine sechsstufige Methode dar, die auf dem Versicherungsansatz von S&P basiert und die Relevanz der Bedrohungen zu den Geschäftsprozessen berücksichtigt. Etwaige Schwachstellen können auf Grund der abgebildeten Abhängigkeiten bis auf einzelne Risiko-Objekte zurückverfolgt werden. Das Ergebnis ist eine Bewertung nach dem bekannten S&P-Rating-Modell und ermöglicht damit eine objektive Positionierung zu den Finanz- und Marktrisiken. Als Risiko-Management lässt es sich nahtlos in bestehende Managementprozesse integrieren und ist für bestehende und zukünftige Standards und Normen offen.

Abb. 2: Implementierungsansatz nach CRISAM®



Stufe 1: Policy

CRISAM leitet aus den strategischen Festlegungen des Unternehmens zunächst eine von der Unternehmensleitung freizugebende und bindende Sicherheitspolitik ab (Abb. 2). In klaren, als Leitsätze formulierten Anweisungen ist diese Sicherheitspolitik auch als Abgrenzung zu sehen, in deren Grenzen anstehende Entscheidungen getroffen werden müssen.

Stufe 2: Geltungsbereich

Im Geltungsbereich werden die in der Sicherheitspolitik erfassten Geschäftsprozesse identifiziert. 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 sind.

Stufe 3: Risiko-Analyse

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 Rest-Risiko

auf jeder Hierarchiestufe dieses IT-Ressourcen-Baumes. Für den Reifegrad des IT-Risiko-Managements ergibt sich eine Rating-Kennzahl, 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-Risiko-Management.

Stufe 4/5: Risiko-Management

Die Abweichung des analysierten Rating-Wertes 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.

Stufe 6: Implementierung

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

Um Risiken bzw. IT-bedingte Restrisiken managen zu können, sind grundsätzliche Rahmenbedingungen im Unternehmen zu schaffen. Von letztendlich verantwortlicher

Stelle ist eine Zielvorgabe als Positionierung im Umgang mit IT-relevanten Risiken vorzugeben (Sicherheitspolitik). Potenzielle Bedrohungen aus dem Einsatz des Werkzeuges IT für die wertschöpfenden Geschäftsprozesse sind zu identifizieren und das IT-Werkzeug selbst ist auf Abweichungen zum aktuell gültigen Stand der Technik zu überprüfen. Die Aktualität der eingesetzten Technologien ist zudem 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 stellen eine potenzielle Bedrohung im Sinne eines Unternehmensrisikos dar und sind durch entsprechende 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 potenziellen Rest-Risikos. Diese Transformation des IT-Risiko-Managements 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. ■

Dr. Manfred Stallinger ist geschäftsführender Gesellschafter der Calpana Business Consulting GmbH mit dem Sitz in Linz/Österreich und Lektor an der Donau Privatuniversität Krems sowie Ziviltechniker für Informatik und gerichtlich beideter Sachverständiger.