



2010 – AUSGABE 5/6 **agens Audit & Risk Newsletter**

Informationen zu Revision,
Risikomanagement und Trainings

agens – gedacht, getan

AKTUELLES

Liebe agens Newsletter Leserinnen und Leser,

unser Team möchte Sie weiter über Neuigkeiten rund um das Thema Revision und Risikomanagement informieren.

Dem aufmerksamen Leser dürfte sicherlich nicht entgangen sein, dass die angekündigte Schutzbedarfsanalyse das letzte Mal gefehlt hat. Aus gegebenem Anlass wurde dieser Artikel durch einen Beitrag zu QIS 5 ersetzt.

In dieser Ausgabe des Newsletter möchten wir Ihnen das versprochene Schwerpunktthema „Schutzbedarfsanalyse in Anlehnung an die Vorgehensweise des BSI“ präsentieren. Im Weiteren möchten wir Sie auf die aktuellen Themen „Risikotransfer mittels Captives“ und „Methoden und Kennzahlen für Stresstest“ aufmerksam machen.

Ich wünsche Ihnen eine angenehme Lektüre.



Christof Merz
(Geschäftsbereichsleiter)



Agenda

Schwerpunktthema	3
Schutzbedarfsanalyse in Anlehnung an die Vorgehensweise des BSI	3
Aktuelles	9
Risikotransfer mittels Captives	9
Methoden und Kennzahlen für Stresstests.....	11
Nachbetrachtungen zum DIIR-Forum für Kreditinstitute sowie zur Jahrestagung des DIIR 2010	15
Literatur	17
Seminartermine	18
Microsoft Excel.....	19
Who is Who	21
Impressum.....	22

SCHWERPUNKTHEMA

Schutzbedarfsanalyse in Anlehnung an die Vorgehensweise des BSI

Weit verbreitete Fehleinschätzung

In den Unternehmen betrifft eine weit verbreitete Fehleinschätzung den eigenen Schutzbedarf. Oft stößt man auf die folgenden Aussagen:

- *„Bei uns ist noch nie etwas passiert“.* Diese Aussage ist mutig. Vielleicht hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt!
- *„Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.“* Diese Einschätzung ist in den meisten Fällen zu oberflächlich. Bei sorgfältiger Betrachtung von möglichen Schadensszenarien zeigt sich schnell: Es können durchaus Daten verarbeitet werden, die vielfältigen Missbrauch ermöglichen, wenn sie in die falschen Hände fallen.
- *„Unser Netz ist sicher.“* Die Fähigkeiten potenzieller Angreifer werden oft unterschätzt. Hinzu kommt, dass selbst ein erfahrener Netz- oder Sicherheitsspezialist nicht alles wissen und gelegentlich Fehler machen kann. Externe Überprüfungen decken nahezu immer ernste Schwachstellen auf und sind ein guter Schutz vor „Betriebsblindheit“.
- *„Unsere Mitarbeiter sind vertrauenswürdig.“* Verschiedene Statistiken zeichnen ein anderes Bild: Die Mehrzahl der Sicherheitsverstöße wird durch Innentäter verursacht. Dabei muss nicht immer Vorsatz im Spiel sein. Auch durch Versehen, Übereifer oder Neugierde - gepaart mit mangelndem Problembewusstsein - entstehen manchmal große Schäden.

Jeder sollte sich bewusst machen: Sicherheit ist kein statischer Zustand, sondern ein ständiger Prozess. Stellen Sie sich daher immer wieder folgende Fragen:

- Welche Formen von Missbrauch wären möglich, wenn vertrauliche Informationen Ihres Unternehmens oder Ihrer Behörde in die Hände Dritter gelangten?
- Welche Konsequenzen hätte es für Sie, wenn wichtige Informationen - z. B. während einer Datenübertragung oder auf Ihrem Server - verändert würden? Als Ursache kann nicht nur böse Absicht unbekannter Dritter, sondern auch technisches Versagen in Frage kommen.
- Was würde geschehen, wenn in Ihrer Organisation wichtige Computer oder andere IT-Komponenten plötzlich ausfielen und einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr nutzbar wären? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden?

Wenn ein Unternehmen ein gut durchdachtes IT-Sicherheitskonzept umsetzt, werden sich nach einiger Zeit - neben dem Sicherheitsgewinn - weitere Vorteile einstellen. IT-Leiter beobachten häufig folgende „Nebeneffekte“:

- *Die Mitarbeiter sind zuverlässiger, die Arbeitsqualität steigt.* - Gelebte IT-Sicherheit fördert eine Unternehmenskultur, in der verantwortungsbewusstes Handeln, Kundenorientierung und die Identifikation mit den Unternehmenszielen fest verankert sind.
- *Wettbewerbsvorteile* - Nachgewiesene IT-Sicherheit schafft Vertrauen bei Kunden und anderen Geschäftspartnern und wird zunehmend von diesen auch eingefordert.
- *Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit. Administratoren arbeiten effektiver.* - Administratoren und Anwender kennen sich besser mit ihren Systemen aus. IT-Systeme sind gut dokumentiert, was Administrationsarbeiten, Planung, Neuinstallation von Software und Fehlerbeseitigung erleichtert. Ein gutes IT-Sicherheitskonzept vermeidet zudem einige Probleme unter denen Administratoren normalerweise besonders leiden: Anwender setzen verschiedene Programme für den gleichen Zweck ein, unterschiedliche Betriebssysteme müssen betreut werden, verschiedene Versionen der gleichen Software sind im Einsatz, jeder Anwender hat indi-

SCHWERPUNKTHEMA

viduelle Rechte, Anwender nutzen private Software und gestalten ihren Arbeitsplatz-PC selbst - ohne entsprechendes Know-how. Eine zentrale Administration des „Rechnerzoos“ ist so kaum möglich. Jeder Rechner muss mit hohem Aufwand individuell analysiert und betreut werden.

BSI-Methodik zur Schutzbedarfsanalyse

Der klassische Ansatz zur Herstellung eines gewissen Sicherheitsniveaus einer Organisation ist die Risikoanalyse. Da mit der Risikoanalyse ein ggf. sehr hoher Aufwand verbunden ist, schlägt das BSI eine vereinfachte Methode vor, die man als eine Untermenge der Risikoanalyse betrachten kann und die vom BSI mit der Bezeichnung Schutzbedarfsanalyse (bzw. Schutzbedarfsfeststellung) versehen wurde. Um diesen Begriff besser bestimmen zu können, soll er im Folgenden zunächst von der Risikoanalyse abgegrenzt werden.

Risikoanalyse

Die Risikoanalyse setzt sich zusammen aus Risikoidentifikation und Risikobewertung. Die *Risikoidentifikation* (die auch in der Schutzbedarfsanalyse der BSI-Methodik auftaucht, und zwar als Aufzählung von *Gefährdungen*) ist auf die spezifische Risikosituation des Unternehmens abgestimmt und erfasst möglichst alle Risiken, die das Unternehmen treffen können. Die Identifikation technischer Risiken – nur um solche geht es hier – basiert z. B. auf Systemanalysen, Fehlerbaumanalysen oder Störfallanalysen. Für die Identifikation von Risiken im IT-Bereich schlägt das BSI eine „Baustein“-orientierte Systematik vor, die grob gesehen folgende Bereiche umfasst:

- Organisation
- Personal
- Notfallvorsorge-Konzept
- Datensicherungskonzept
- Infrastruktur
- Nicht-vernetzte IT-Systeme
- Vernetzte Systeme
- Datenübertragungseinrichtungen
- Telekommunikation
- Sonstige IT-Komponenten

Bei der *Risikobewertung* geht es darum, einerseits die bei Eintritt des Risikos verursachten finanziellen Auswirkungen (Schadenausmaß) zu quantifizieren und andererseits eine Schadenseintrittswahrscheinlichkeit abzuschätzen. Bei der Abschätzung des Schadenausmaßes bedient man sich verschiedener Instrumente und Methoden. Bei der PML- bzw. MPL-Analyse wird z. B. für die Beurteilung eines Großschadenrisikos der *Maximum Possible Loss* (MPL) oder der *Probable Maximum Loss* (PML) ermittelt. Stoßen die quantitativen Verfahren an ihre Grenzen, so bedient man sich qualitativer Aussagen. Das Schadenausmaß kann bei fehlender Quantifizierbarkeit nach den Kategorien „gering“, „mittel“, „groß“ und „katastrophal“ eingeteilt werden. Die Schadeneintrittswahrscheinlichkeit wird in der Praxis fast immer qualitativ nach den Kategorien „sehr gering“, „gering“, „mittel“, „hoch“ und „sehr hoch“ gewichtet. Vor allem betriebswirtschaftliche Schäden (Marktverlust, Imageverlust etc.) können so besser abgebildet werden.

Die erkannten Risiken werden – gegliedert nach ihren finanziellen Auswirkungen und der Eintrittswahrscheinlichkeit – in einer *Risikomatrix* zusammengestellt. Die Risikomatrix liefert in komprimierter und übersichtlicher Form Informationen über die Risikolage eines Unternehmens, um so die Priorität, mit welcher die Maßnahmen zur Risikobewältigung realisiert werden sollen, festzulegen. In der Risikomatrix kann eine individuelle Akzeptanzlinie abgebildet werden, die festlegt, ab welchem Schwellenwert ein Handlungsbedarf ausgelöst wird. Bei der Ermittlung der Gesamtrisikolage müssen auch die Risikointerdependenzen berücksichtigt und aggregiert werden. Insbesondere bei den modernen Produktionsmethoden (Just-in-time, Sing-

SCHWERPUNKTHEMA

le-Sourcing etc.) gewinnt die Aggregation der Einzelrisiken an Bedeutung.

Die Durchführung einer organisationsweiten Risikoanalyse ist sehr aufwändig und verlangt von den durchführenden Personen große Erfahrung. Insbesondere erfordert die Risikoanalyse einen Überblick sowohl über die Bedeutung einzelner Objekte für die zu untersuchende Organisation als auch über die möglichen Gefahren und entsprechende Maßnahmen zu ihrer Beseitigung. Häufig ist dieser Ansatz daher mit den dafür zur Verfügung stehenden Ressourcen nicht durchführbar.

Abgrenzung der Schutzbedarfs- von der Risikoanalyse

Die Schutzbedarfsanalyse lässt sich von der Risikoanalyse in drei Punkten abgrenzen:

- Im Gegensatz zur Schutzbedarfsanalyse betrachtet die Risikoanalyse nicht nur Schadensauswirkungen, sondern auch Schadenseintrittswahrscheinlichkeit.
- Im Gegensatz zur Schutzbedarfsanalyse ist die Risikoanalyse nicht nur auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ausgerichtet, sondern kann ggf. weitere Schutzziele betrachten.
- Die Risikoanalyse versucht, wann immer möglich, mit quantitativen Maßen vorzugehen; darauf wird in der Schutzbedarfsanalyse von vornherein verzichtet.

Durchführung einer Schutzbedarfsanalyse

Die Durchführung einer Schutzbedarfsanalyse bildet grundsätzlich die Basis zur Bestimmung schutzbedürftiger Datenbestände sowie der Dateneigentümerschaft. Aus diesen Ergebnissen ergeben sich für die Datenschutz- und IT-Sicherheitsbeauftragten wesentliche Prüfungs- und Handlungsfelder.

Aus einer nicht durchgeführten Schutzbedarfsanalyse resultieren die Risiken,

- dass die für das Unternehmen wesentlichen Risiken nicht vollständig identifiziert werden
- dass potenzielle Prüfungs- und Handlungsfelder nicht vollständig identifiziert werden und
- dass die Planung und Aufgabenpriorisierung der Datenschutz- und IT-Sicherheitsbeauftragten nicht angemessen ausgerichtet werden.

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können.

Definition der Schutzbedarfskategorien

Vorab sind Schutzbedarfskategorien zu definieren. Dabei ist es wichtig, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien "normal", "hoch" und "sehr hoch".

- "normal" = Die Schadensauswirkungen sind begrenzt und überschaubar.
- "hoch" = Die Schadensauswirkungen können beträchtlich sein.
- "sehr hoch" = Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

SCHWERPUNKTHEMA

Diese Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess bzw. eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

- Verstoß gegen Gesetze/Vorschriften/Verträge
- Beeinträchtigung des informationellen Selbstbestimmungsrechts (Datenschutz-Grundrecht)
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung
- Finanzielle Auswirkungen

Erfassung der Abhängigkeiten

Aufgrund der steigenden Komplexität von IT-Anwendungen sind sich die Fachverantwortlichen oftmals nicht darüber im Klaren, welche Abhängigkeiten zwischen einem Geschäftsprozess bzw. einer Fachaufgabe und einer konkreten Anwendung bestehen. Es sollte also für jeden Geschäftsprozess bzw. jede Fachaufgabe festgestellt werden, welche Anwendungen für die Abwicklung notwendig sind und auf welche Daten dabei zugegriffen wird. In einer gemeinsamen Sitzung der Fachabteilung, der Verantwortlichen der einzelnen Anwendungen und der unterstützenden IT-Abteilung können diese Abhängigkeiten erfasst werden.

Im Weiteren erstreckt sich die Schutzbedarfsanalyse auf folgende Objekte:

- Geschäftsprozesse
- IT-Anwendungen
- Dienstleistungsverträge
- IT-Systeme: Server, Speicher, Netzwerk, Drucker, Clients
- Kommunikationswege
- Räume.

Analyse der Geschäftsprozesse

Bei der Analyse der Geschäftsprozesse sind alle Geschäftsprozesse mit ihren Kritikalitäten, Bezug zu unterstützenden IT-Anwendungen und Verträgen aufzulisten.

Dabei sind folgende Aspekte zu berücksichtigen: Geschäftsprozess, Prozessbeschreibung, verantwortlicher/fachzuständiger Bereich, Outsourcing-Partner, prozessspezifische IT-Anwendungen, Kritikalität, Anlaufzeit im Notbetrieb und Anlaufzeit im Normalbetrieb.

Bei der Kritikalität ist zu unterscheiden in kritisch, essenziell, notwendig und wünschenswert:

Kritikalität	
kritisch	Ohne diesen Prozess kann der Geschäftsbetrieb nicht durchgeführt werden.
essenziell	Ohne diesen Prozess kann der Geschäftsbetrieb nur mit hohen Verlusten durchgeführt werden.
notwendig	Ohne diesen Prozess kann der Geschäftsbetrieb nur mit Einschränkungen durchgeführt werden.
wünschenswert	Dieser Prozess ist für den Geschäftsbetrieb erlässlich.

SCHWERPUNKTHEMA

Analyse der IT-Anwendungen

Bei der Analyse der IT-Anwendungen werden - ausgehend von der Möglichkeit, dass Vertraulichkeit, Integrität oder Verfügbarkeit einer Anwendung oder der zugehörigen Informationen verloren gehen - die maximalen Schäden und Folgeschäden betrachtet, die aus einer solchen Situation entstehen können. Unter der Fragestellung "Was wäre, wenn ...?" werden aus Sicht der Anwender realistische Schadensszenarien entwickelt und die zu erwartenden materiellen oder ideellen Schäden beschrieben. Die Höhe dieser möglichen Schäden bestimmt letztendlich dann den Schutzbedarf der Anwendung.

Bei der Auflistung aller IT-Anwendungen mit ihrem Schutzbedarf, Bezug zu unterstützenden IT- und Netzwerksystemen sind folgende Aspekte zu berücksichtigen: Gesellschaft, IT-Anwendung, Beschreibung (Verwendungszweck), Ort der Datenhaltung, genutzte IT-Systeme, genutzte Netzwerke, Abhängigkeit von IT-Anwendung, fachlich verantwortlich in der Gesellschaft, personenbezogene Daten (Datenschutz), juristische Daten, rechnungslegungsrelevante Daten sowie Integrität, Vertraulichkeit und Verfügbarkeit, kategorisiert nach sehr hoch, hoch und normal.

Analyse der Verträge

Bei der Analyse der Verträge sind alle relevanten Verträge, der Bezug zu IT-Anwendungen, IT-Systemen und Kommunikationsverbindungen aufzulisten. Dabei sind folgende Aspekte zu berücksichtigen: Mandant, Beschreibung, Vertragspartner, Vertragsnummer, Vertragsbeginn, Vertragsende, Bezug zu IT-System, IT-Anwendung oder anderen, fachliche Zuständigkeit, Bezug zu anderen Verträgen, Systemverfügbarkeit, Reaktionszeit und Wiederherstellungszeit.

Analyse der IT-Systeme

Zur Ermittlung des Schutzbedarfs des IT-Systems müssen die möglichen Schäden der relevanten Anwendungen in ihrer Gesamtheit betrachtet werden. Im Wesentlichen bestimmt der Schaden bzw. die Summe der Schäden mit den schwerwiegendsten Auswirkungen den Schutzbedarf eines IT-Systems.

Bei der Betrachtung der möglichen Schäden und ihrer Folgen muss auch beachtet werden, dass IT-Anwendungen eventuell Arbeitsergebnisse anderer Anwendungen als Input nutzen. Eine, für sich betrachtet, weniger bedeutende Anwendung A kann wesentlich an Wert gewinnen, wenn eine andere, wichtige Anwendung B auf ihre Ergebnisse angewiesen ist. In diesem Fall muss der ermittelte Schutzbedarf der Anwendung B auch auf die Anwendung A übertragen werden. Handelt es sich dabei um Anwendungen verschiedener IT-Systeme, dann müssen Schutzbedarfsanforderungen des einen IT-Systems auch auf das andere übertragen werden.

Werden mehrere Anwendungen bzw. Informationen auf einem IT-System verarbeitet, so ist zu überlegen, ob durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Dann erhöht sich der Schutzbedarf des IT-Systems entsprechend.

Zu analysieren sind die Server, der Speicher, das Netzwerk, die Drucker und die Clients. Im Folgenden werden die Aspekte aufgezählt, die hierbei zu analysieren sind:

- **Server:** Kürzel, Seriennummer, Mandant, Physischer Name, Logischer Name, Verbale Beschreibung, Anzahl, Plattform, HA-Cluster, Loadbalancing, Hot-Stand-by, Cold-Stand-by, Netzsegment, Raum, Rackname, Verantwortlich sowie Integrität, Vertraulichkeit und Verfügbarkeit
- **Speicher:** Kürzel, Seriennummer, Mandant, Physischer Name, Logischer Name, Verbale Beschreibung, Anzahl, Type, Raid-Level, Spiegelung, Server, Netzsegment, Raum, Verantwortlich, Assetnummer, Zugriffsschutz, Zugriffsberechtigte, Outsourcing-Partner, Außenverbindung, Wartungsvertrag, Status, Umgebung (Produktion, Test, Integration, Entwicklung, Schulung) sowie Integrität, Vertraulichkeit und Verfügbarkeit

SCHWERPUNKTHEMA

- **Netzwerk:** Kürzel, Mandant, Gesellschaft, Physischer Name, Logischer Name, Verbale Beschreibung, Anzahl, Plattform, Media, Loadbalancing, Backup, Netzsegment, Raum, Verantwortlich, Assetnummer sowie Integrität, Vertraulichkeit und Verfügbarkeit
- **Drucker:** Kürzel, Seriennummer, Mandant, Physischer Name, Logischer Name, Verbale Beschreibung, Anzahl, Plattform, Netzsegment, Raum, Verantwortlich, Assetnummer, Zugriffsschutz, Zugriffsberechtigte, Outsourcing-Partner, Wartungsvertrag, Status, Umgebung (Produktion, Test, Integration, Entwicklung, Schulung) sowie Integrität, Vertraulichkeit und Verfügbarkeit
- **Client:** Kürzel, Seriennummer, Mandant, Physischer Name, Logischer Name, Verbale Beschreibung, Anzahl, Plattform, Netzsegment, Raum, Verantwortlich, Assetnummer, Zugriffsschutz, Zugriffsberechtigte, Outsourcing-Partner, Außenverbindung, Wartungsvertrag, Status, Umgebung (Produktion, Test, Integration, Entwicklung, Schulung) sowie Integrität, Vertraulichkeit und Verfügbarkeit

Analyse der Räume

Aus den Ergebnissen der Schutzbedarfsfeststellung der Anwendungen und der IT-Systeme sollte abgeleitet werden, welcher Schutzbedarf für die jeweiligen Gebäude bzw. Räume besteht. Dieser Schutzbedarf leitet sich aus dem Schutzbedarf der im jeweiligen Raum installierten IT-Systeme, verarbeiteten Informationen oder der Datenträger, die in diesem Raum gelagert und benutzt werden, ab. Dabei sollten eventuelle Abhängigkeiten und ein möglicher Kumulationseffekt berücksichtigt werden, wenn sich in einem Raum eine größere Anzahl von IT-Systemen, Datenträgern usw. befindet, wie typischerweise bei Serverräumen, Rechenzentren oder Datenträgerarchiven. Für jede Schutzbedarfseinschätzung sollte eine Begründung dokumentiert werden.

Analyse der Kommunikationsverbindungen

Nachdem die Schutzbedarfsfeststellung für die betrachteten Anwendungen, IT-Systeme und Räume abgeschlossen wurde, wird nun der Schutzbedarf bezüglich der Vernetzungsstruktur erarbeitet.

Um die Entscheidungen vorzubereiten, auf welchen Kommunikationsstrecken kryptographische Sicherheitsmaßnahmen eingesetzt werden sollten, welche Strecken redundant ausgelegt sein sollten und über welche Verbindungen Angriffe durch Innen- und Außentäter zu erwarten sind, müssen die Kommunikationsverbindungen analysiert werden.

Aufwand für die Durchführung einer Schutzbedarfsanalyse

Der Aufwand für die Durchführung einer Schutzbedarfsanalyse variiert in Abhängigkeit von der Unternehmensgröße und den bereits vorliegenden Daten. Das Ergebnis liefert jedoch wertvolle Informationen über die Abhängigkeiten der Geschäftsprozesse von den IT-Komponenten. Erst damit wird die Transparenz geschaffen, um bedarfsgerechte Maßnahmen in Abhängigkeit vom Risiko, Schutzbedarf und Kritikalität umsetzen zu können.

Ansprechpartner: Jörg Wöhler (Leitender Berater)

Risikotransfer mittels Captives

- Anforderungen, Probleme und Lösungsansätze -

Ein **Eigenversicherer** oder **Eigenversicherungsunternehmen** (englisch **Captive Insurance Company** oder auch kurz **Captive**) ist ein firmeneigenes Versicherungsunternehmen, das dem Mutterunternehmen zur Absicherung firmeneigener Versicherungsrisiken dient.

Typischerweise gehören Captives zu großen, meist multinationalen Konzernen, da hier am ehesten die erforderliche Betriebsgröße für das firmeneigene Versicherungsportfolio erreicht wird.

Man kann Eigenversicherer nach der Art der Einbindung in den Konzern und der Variation der Einsatzgebiete unterteilen. Ein reiner Captive ist der Eigenversicherer eines einzigen Konzerns, der auch nur Risiken dieses Konzerns trägt. Bei einem gemeinsamen Captive schließen sich verschiedene Konzerne zusammen, um über ein gemeinsam betriebenes Eigenversicherungsunternehmen ihre Risiken decken zu lassen.

Bei den Einsatzgebieten kann die Captive danach unterschieden werden, ob sie die kompletten Risiken des Konzerns direkt übernimmt und dann üblicherweise einen Teil des Risikos an die Rückversicherer weitergibt. Bei der zweiten Variante fungiert der Captive quasi als Eigenrückversicherer bei dem die Risiken des Konzerns durch einen normalen Erstversicherer getragen werden und ein Teil bei dem Captive rückgedeckt wird.

Die Gründe für einen Konzern eine Captive zu gründen sind vielfältig und variieren von Unternehmen zu Unternehmen. Im Wesentlichen treffen aber immer einer oder mehrere der folgenden Motive zu:

- Reduzierung/Stabilisierung von Versicherungsprämien auf Konzernebene. Durch die Bündelung der Nachfrage und dem Aushandeln von globalen Kontrakten und Bedingungen werden die Prämien in aller Regel günstiger sein als bei lokalen Policen.
- Hebung von Synergien und komparativen Vorteilen durch gutes Risikomanagement. Basierend auf den eigenen Schadenerfahrungen können Prämien marktgerechter bepreist und risikoreduzierende Maßnahmen sofort ertragssteigernd bzw. verlustmindernd berücksichtigt werden.
- Legung von Reserven bzw. „Bilanzschutz“. Risiken, die nicht am Markt versicherbar sind, können über eine Captive getragen und somit im Bedarfsfall zum Schadenausgleich herangezogen werden.
- Spitzenausgleich bei fehlender Möglichkeit Risiken insgesamt oder in ausreichender Höhe am Markt zu versichern.
- Direkter Zugang zum weltweiten Rückversicherungsmarkt
- Verbesserung des Risikomanagements auf Konzernebene durch Aggregation, Überwachung und Limitierung der Risiken. Gleichzeitig wird hierdurch das Risikobewusstsein gestärkt und die Transparenz erhöht

Welchen Herausforderungen muss sich nun ein Captive in der Regel stellen?

Die Antwort auf diese Frage lässt sich in aller Regel auf folgende Problemkreise reduzieren:

- Rechtlicher und aufsichtsrechtlicher Rahmen
- Überwachungsfunktion und Internal Audit
- Wissen und Kopfmonopole
- Risikomanagement und Risiken

Unabhängig von der Größe des Captive handelt es sich bei den Unternehmen um Versiche-

AKTUELLES

rungsunternehmen, d. h. sie unterliegen auch den rechtlichen und aufsichtsrechtlichen Regelungen des Heimatlandes. Die Regelungsdichte kann dabei in Abhängigkeit vom Sitz des Captives stark schwanken. So hat eine Captive mit einem Dienstsitz auf den Bahamas sicherlich gegenüber einem europäischen oder gar deutschen Sitz den Vorteil der geringen Anzahl von einzuhaltenden Regularien und Gesetzen. Nachteilig wirkt sich umgekehrt aber auch der unbekannte Rechtsraum, die ggf. schwierigere Einbindung des Captives in die bestehende Erstversicherer-Struktur und der Nachweis der Anforderungen aus Rundschreiben 1/97 aus.

Für Captives ergibt sich ebenfalls die Notwendigkeit, eine Revisionsfunktion vorzuweisen. Oftmals wird diese Funktion durch die Konzernrevision wahrgenommen. Dies hat den Vorteil von bereits eingespielten Prüfungsabläufen sowie Kenntnisse über konzerninternen Prozessen. Eine nicht zu unterschätzende Schwierigkeit in diesem Zusammenhang ist, dass bei Prüfung einer Captive auch ein umfangreiches Wissen über die aufsichtsrechtlichen Anforderungen sowie versicherungsspezifisches Wissen notwendig ist. Dieses Wissen kann aufgrund von Umfang und Komplexität bei ansonsten unregulierten Non-Finanzdienstleistungsunternehmen verständlicherweise nicht ohne weiteres immer auf dem neuesten Stand gehalten werden. Hier bietet sich nach unserer Erfahrung punktuelle Unterstützung durch Experten an.

Viele Captives haben ihr operatives Geschäft bzw. die Geschäftsbesorgung in großen Teilen an Konzernunternehmen oder Dritte ausgelagert. Hierdurch können die operativen Kosten relativ gering gehalten und Spezialwissen eingekauft werden. Gleichzeitig entstehen hiermit aber auch Abhängigkeiten und Kopfmonopole. Begegnen kann man diesem Risiko nur mit gut dokumentierten Prozessen und Abläufen sowie über Stellvertreterregelungen.

Ein immanentes Problem bei den meisten dieser Lösungen ist die fehlende Diversifikation über viele Versicherungsnehmer und –sparten. Oftmals sind nur wenige oder gar nur eine Sparte über die Captive versichert. Das hierdurch verursachte Kumulrisiko erhöht grundsätzlich das Verlustpotenzial bei Extremereignissen.

Begegnen kann man diesen Risiken nach unserer Erfahrung nur mit einem guten Risikomanagement und angepassten Risikokapitalmodellen, die mögliche Extremereignisse dem vorhandenen Deckungskapital bzw. Reserven gegenüberstellen. Gerade hier kann das vorhandene Wissen über Schadenverteilungen aus der Vergangenheit zu unternehmensindividuellen Prognosemodellen herangezogen werden.

Die Schwankungen der Passivseite haben auch direkt Auswirkungen auf die Kapitalanlagepolitik. Ohne eine abgestimmte Aktiv-/Passivbetrachtung (ALM) läuft die Kapitalanlage Gefahr, die Anforderungen der Passivseite komplett zu vernachlässigen. Sofern die Kapitalanlage durch eine konzerninterne Treasury Abteilung erfolgt, die nicht über das Wissen hinsichtlich der damit zu versicherungstechnischen Verbindlichkeiten hat, läuft die Captive Gefahr für eine kurzfristige Renditeoptimierung erhebliche Marktpreis- und Marktliquiditätsrisiken einzugehen.

Eine Herausforderung für alle Captives wird zudem die Anwendung von Solvency II sein. Es gibt Bestrebungen, hier den Belangen und Besonderheiten der Captives gerecht zu werden. Wie diese Anforderungen für Captives aussehen werden, müssen die anstehenden Diskussionen erst noch zeigen.

Ansprechpartner: Christof Merz (Geschäftsbereichsleiter)

AKTUELLES

Methoden und Kennzahlen für Stresstests

Die richtigen Messgeräte für den Sturm

Der „Value at Risk“ (VaR) hat sich weitgehend als Risikomesszahl in Finanz- und Realwirtschaft durchgesetzt. Er beschreibt eine monetäre Größe, die Verluste mit einer bestimmten Sicherheit beschränkt. So kann der VaR angeben, dass ein Verlust größer als 10 Mio. € nur in 1 % aller Fälle zu erwarten ist. Er eignet sich damit sehr gut, um sogenannte „worst-case“ Szenarien zu beschreiben: Man kann ermitteln, mit welcher Wahrscheinlichkeit etwas eintritt (z. B. Zahlungsunfähigkeit), dass auf jeden Fall zu vermeiden ist. Eine große Schwäche des VaR ist, dass er ignoriert wie schlimm der Verlust dann tatsächlich ist. Ob ich nun in diesen 1 % der Fälle 11 Mio. € oder 100 Mio. € verliere kann ich dem VaR nicht entnehmen – er ist also als alleinige Risikokennzahl nur geeignet, wenn das keine Rolle (mehr) spielt¹.

Mit dieser Eigenschaft geht auch eine weitere einher, die „fehlende Subadditivität“ genannt wird: Betrachtet man zwei Risiken zusammen, so kann der VaR beider zusammen größer sein als die Summe der VaR der Einzelrisiken für sich. So ist es möglich, dass zwei Banken, die jeweils einen 1 %-VaR von 10 Mio. € ausweisen, in ihrer Gesamtheit betrachtet (z. B. nach einer Fusion) einen 1 % VaR von 25 Mio. € oder mehr ermitteln. Diese Eigenschaft macht besonders die Ermittlung eines Gesamtrisikos für ein Unternehmen aus den Risiken einzelner Geschäftsbereiche sehr kompliziert.

Stresstest für den VaR

Besondere Aufmerksamkeit verdient der VaR allerdings bei Stresstests: Hier geht die Interpretationsmöglichkeit des VaR oft gänzlich verloren. Dies hängt mit dem übersehenen Unterschied zwischen Schaden und Risiko zusammen. Während ein Schaden einen tatsächlich eingetretenen Verlust beschreibt, ist ein Risiko nur die Möglichkeit eines Verlustes in der Zukunft. Erwartet man bei steigendem Risiko richtigerweise einen höheren VaR so kann dieser in gravierenden Stressszenarien sogar sinken.

Obwohl man in den Szenarien auch die Anleihenmärkte und Spreads, den Interbanken-Markt und natürlich auch das erwartete Verhalten der Kunden im Retail und Corporate Bereich/Markt betrachten muss, um so einen Gesamtbank-Stresstest zu entwickeln, sei hier der Fokus für bessere Verständlichkeit nur auf ein Aktienportfolio in den Eigenanlagen gelegt.

Drei Finanzmarkt Stresstests

Szenario 1: Aktiencrash	Szenario 2: Verunsicherung	Szenario 3: Kombination
Die Finanzmärkte geben massiv nach	Starke widersprüchliche Signale existieren	Kurseinbrüche und Verunsicherung
Die wichtigsten Leitindizes verlieren innerhalb kurzer Zeit 50 %	Die Volatilität in allen Märkten verdoppelt sich	Indizes geben 50 % nach und die Volatilität verdoppelt sich
Abschreibungen auf Depot A Anlagen und Effekte auf Kundendepots	Direkte Wertveränderung nur bei Optionen	

Tabelle 1: Drei plausible Stressszenarien

¹ Sollte der Verlust beim Überschreiten der Schwelle von Interesse sein, bietet sich zusätzlich die Kennzahl „Conditional Value at Risk“ an.

AKTUELLES

Zur Illustration betrachtet man drei plausible Stressszenarien, deren Anwendung auf Banken sinnvoll ist: Ein Crash am Aktienmarkt als Szenario 1 und eine massive Verunsicherung an den Finanzmärkten mit steigender Volatilität als Szenario 2². Tabelle 1 zeigt die Szenarioannahmen übersichtlich auf. Ein Kursverlust von etwa 50 % wie im Szenario 1 bedarf wenig Vorstellungskraft – man hat Vergleichbares in den letzten 10 Jahren bereits zweimal erlebt. Betrachtet man den VDAX (siehe Grafik 1), der die implizite Volatilität³ der DAX Titel wiedergibt, erscheint auch das zweite Szenario realistisch (und beinahe etwas zu optimistisch). Da die implizite Volatilität die Erwartung der Marktteilnehmer angibt steigt sie oft in Zeiten, in denen sich auch der DAX stark bewegt – dies ist jedoch kein zwingender Zusammenhang. Im Stressszenario drei treten beide Effekte ein: Die Aktienmärkte brechen ein und die Volatilität **nach** Einbruch bleibt hoch.



Grafik 1: Der VDAX gibt die implizite Volatilität der DAX-Titel an.

Der Ausgangspunkt (Normalfall) ist ein Depot A mit Gesamtwert von 100 Mio. € und eine Marktvolatilität von 20 %⁴. Für diese Situation berechnet sich der VaR mit Konfidenzwahrscheinlichkeit 1 % zu 46,5 Mio. € – die Wahrscheinlichkeit, dass ein Verlust von 46,5 Mio. € überschritten wird, beträgt also 1 %. Betrachtet man die Auswirkungen auf das Eigenkapital und den VaR im Stressfall wird schnell klar, dass die Interpretation des VaR in Stresstests nicht immer ohne weiteres einfach möglich ist. Man sieht, dass der VaR als Risiko- bzw. Schwankungsmaß im Szenario 1 deutlich zurückgeht. Da das Depot A im Stressfall 1 nur noch einen Gesamtwert von 50 Mio. € aufweist, ist ein Verlust von 46,5 Mio. zwar immer noch möglich aber – bei gleicher Volatilität wie im Normalfall – deutlich unwahrscheinlicher. Der VaR für dieses Szenario beträgt nur noch 23,3 Mio. € – er ist halb so groß wie in Normalfall⁵. In diesem

² Steigende Volatilitäten ohne heftige Kursbewegungen werden oft vor wichtigen Nachrichten beobachtet oder wenn sich der Markt bzgl. der Interpretation von Fakten nicht einig ist.

³ Die implizite Volatilität ist die in Optionen eingepreiste erwartete zukünftige Schwankung des Marktes.

⁴ Zur Vereinfachung wird hier mit einer Normalverteilung der Aktienkurse gerechnet ohne dass dies die Qualität der Aussagen beeinflusst.

⁵ Diese spezielle Proportionalität gilt nur für die Normalverteilung.

AKTUELLES

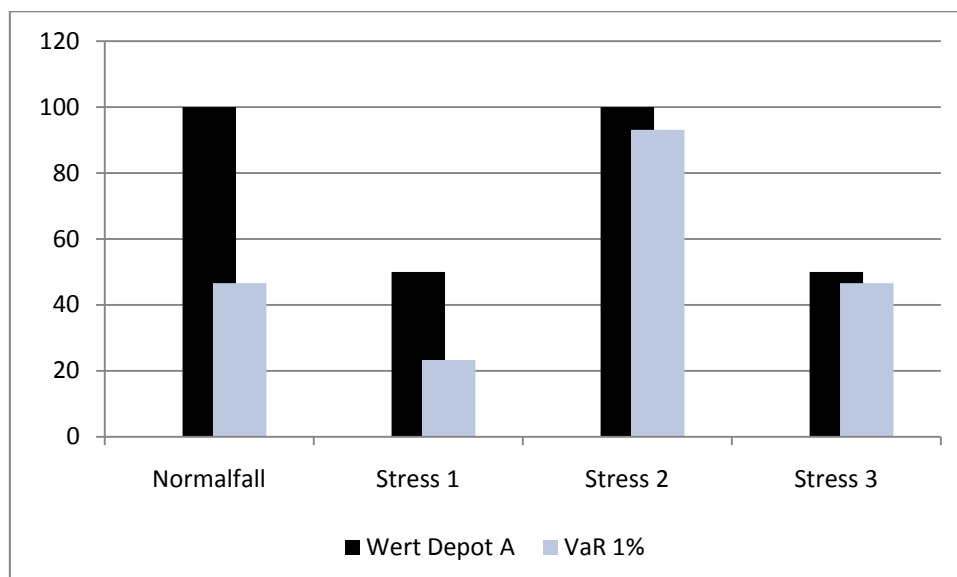
Beispiel, es wird anschaulich klar was in komplexen Szenarien schwer zu erkennen und zu deuten ist: Der Schaden ist im Szenario 1 groß, das Risiko dagegen kleiner.

	Normalfall	Stress 1	Stress 2	Stress 3
Konf	1%	1%	1%	1%
Wert Depot	100	50	100	50
Vola rel.	20%	20%	40%	40%
Vola abs.	20	10	40	20
VaR 1%	46,53	23,26	93,05	46,53

Tabelle 2 – Szenarioparameter und Ergebnisse

Noch deutlicher wird dieser Zusammenhang im Stressfall 2: Hier sind noch keine Verluste eingetreten⁶ – die Bank könnte ohne Abschreibungen aus allen Positionen aussteigen. Dennoch führt eine Erhöhung der Volatilität zum Explodieren des VaR. Das Risiko von Aktien hat deutlich zugenommen. Vergleicht man jedoch nur die VaR der Stressszenarien 1 und 2 könnte man den Eindruck gewinnen, Szenario 1 sei deutlich „milder“ obwohl dort der Schaden unwiederbringlich eingetreten ist. Grafik 2 stellt den Wert(Verlust) und VaR in den Stressszenarien nebeneinander. Im Stressfall 2 ist auch im Stress noch die Sicherung des Gewinns durch eine geeignete Wertsicherungsstrategie möglich. Diese Wertsicherungsstrategien sind idealerweise bereits im Normalfall fertig ausgearbeitet, damit sie ohne Verzögerung im Notfall umgesetzt werden können.

Stressfall 3 kombiniert die vorher gezeigten Effekte. Obwohl die Bank hier nach schweren Verlusten in eine hochriskante Anlage investiert, ist der VaR nicht von seinem Stand im Normalfall abgewichen.



Grafik 2 – Depotwert und VaR in den Stressszenarien

⁶ Von evtl. Optionspositionen, deren Wert sich allein durch die Volatilität ändern kann wird hier abstrahiert.

AKTUELLES

Fazit

Ist ein Stresstest so definiert (wie es z. B. bei den aktuellen EU-Bankenstresstests der Fall ist), dass er einen eintretenden Schaden definiert, so kann dies das Potenzial für zukünftige Schäden – also das Risiko – durchaus reduzieren. Die liebgewonnene Kennzahl VaR muss insbesondere für diese Stresstests genau betrachtet werden und eignet sich keinesfalls als alleinige Maßzahl, denn mit all ihren Vorteilen kann sie manche wichtigen Zusammenhänge nicht erfassen. Anhand dieser Beispiele sei auch darauf hingewiesen, dass ein Stresstest, in dem sich das Risiko erhöht (unabhängig vom eingetretenen Schaden) eine wertvolle Ergänzung der klassischen Schaden-Stresstests sein kann.

Ansprechpartner: Jonas Andrulis (Senior Berater)

Nachbetrachtungen zum DIIR-Forum für Kreditinstitute sowie zur Jahrestagung des DIIR 2010

DIIR-Forum für Kreditinstitute

Das Forum für Kreditinstitute beschäftigte sich in diesem Jahr besonders mit den Auswirkungen der Finanzkrise auf die Finanzwirtschaft und welche Schlussfolgerungen die Interne Revision zu ziehen hat. Hinführend zum Thema hat dazu Frau Gertrude Tumpel-Gugerell von der Europäischen Zentralbank den Einführungsvortrag gehalten. In der anschließenden Podiumsdiskussion unter dem Titel „Lessons learned“ diskutierten Vertreter namhafter Banken und Institute die Fragen:

- Wo liegen die Ursachen?
- Ist die Krise schon überwunden?
- Was ist seither geschehen, um Wiederholungen zu vermeiden?
- Was haben wir gelernt? Oder muss die Frage lauten: Haben wir etwas gelernt?

Diese Fragen sind heute aktueller denn je, denn nach der Krise ist vor der Krise. So wurden diese Fragen auch konsequent in den Fachsitzungen und Erfahrungsaustauschgruppen vertiefend betrachtet. So spielten sie insbesondere auch eine wichtige Rolle zu dem Thema „Vorbeugung gegen Wirtschaftskriminalität – intern und extern“. Dieses Thema wurde in mehreren speziell dieser Frage gewidmeten Runden, aber auch in allen anderen Themenveranstaltungen mittelbar aufgegriffen. Mehr und mehr wird deutlich, dass alle Maßnahmen und Verantwortlichkeiten im Unternehmen noch mehr gebündelt werden sollten. Dazu wären einheitliche, konzertierte Gefährdungsanalysen zu den operativen Risiken, zu Compliance und Fraud sowie systematische Maßnahmen mit wohl dosiertem Tooleinsatz dringend angeraten. Weitere Themen, die keine geringere Tragweite besitzen, waren in den Diskussionen über die MaRisk (BA) sowie der Zusammenhang zu den anderen Mindestanforderungen, die die BaFin stellt, Stresstest, Ratingverfahren, IT-Sicherheit und viele Themen mehr. Übergreifend wurden auch immer wieder die Fragen von Qualität in der Revisionsarbeit, der Personalentwicklung sowie einer wirksamen projektbegleitenden Prüfung erörtert.

Zusätzliche interessante Impulse gaben uns die weiteren Referate und Reden, die über die Rolle der KfW einen Einblick verliehen, über Moral und Ethik philosophierten oder zum Abschluss auch die Frage nach Investitionen in Umwelttechnologien emotional bedeutsam aufwarfen.

DIIR-Jahrestagung

Wer bereits am Forum Kreditinstitute teilgenommen hatte, spürte den nahtlosen Übergang von einer zur anderen Veranstaltung, da die Hauptprobleme und –themen auch in der Jahrestagung eine wesentliche Rolle spielten, wie sie es schon im Forum getan hatten. Jedoch sind natürlich das Branchenspektrum und damit auch die Themenvielfalt noch größer.

Der Auftakt der Jahrestagung 2010 erfolgte durch den Vortrag „Mehrwertschaffende Zusammenarbeit des Bereichs Compliance und der Internen Revision am Beispiel der DB AG“, welchen uns Herr Gerd Brecht, Vorstand Compliance, Datenschutz und Recht der Deutsche Bahn AG präsentierte. Neben Themen Projektrevision, Quality Assessment, Risikomanagement, Fraud-Prevention, Compliance, die unter breiterem Aspekt ähnliche Erfahrungen vermittelten, wie es in den Veranstaltungen des Bankenforums geschah, spielten Fachreferate und Diskussionsforen zur Haftung der IR, zur Toolunterstützung in der Prüfungsarbeit, zur Umsetzung von 8. EU-Richtlinie und BilMoG oder MaRisk (VA), zur Dokumentation der Prüfungshandlungen – Arbeitspapiere und Berichte, das stets aktuelle Diskussionsthema -, zur risiko- und prozessorientierten Prüfungsplanung, über moderne Werkzeuge im Einsatz zur Datenanalyse sowie zum Revisions-Controlling und –Marketing eine wichtige Rolle in der diesjährigen Jahrestagung des DIIR.

AKTUELLES

Frau Sylvia Schenk, Transparency International, Deutschland e.V., Berlin, warf im zweiten Hauptreferat die Frage „Um welchen Preis? – Korruption in Sport und Wirtschaft“ beeindruckend auf. Abschließend bildete der Vortrag von Prof. Dr. Gerd Gigerenzer, Max-Planck-Institut für Bildungsforschung, Berlin, zum Thema „Bauchentscheidung: Die Intelligenz des Unbewussten“ eine gute Grundlage zum weiteren Nachdenken.

Zusammenfassend ist festzustellen, dass in beiden Veranstaltungen wieder interessante Impulse für die weitere Arbeit gesetzt wurden.

Ansprechpartner: Dr. Peter Wesel (Senior Berater)

LITERATUR



Wertbeitrag der Internen Revision

Messung, Steuerung und Kommunikation

H. Buderath, A. Herzig, A. Köhler, B. Pedell

ISBN-10: 3791029436

[\(Mehr ...\)](#)



Risikomanagement in Banken und Finanzinstituten

John C. Hull

ISBN-10: 386894043X

[\(Mehr ...\)](#)



Mindestanforderungen an das Risikomanagement (MaRisk)

Kommentar

Ralf Hannemann, Andreas Schneider

ISBN-10: 3791029525

[\(Mehr ...\)](#)



Mit Compliance Wirtschaftskriminalität vermeiden

M. Harz, D. Noa, J. Schäfer

ISBN-10: 3791029541

[\(Mehr ...\)](#)



Immobilien Asset Management

Rainer Quante

ISBN-10: 3899842421

[\(Mehr ...\)](#)



Risikomanagement in Banken und Finanzinstituten

John C. Hull

ISBN-10: 386894043X

[\(Mehr ...\)](#)



Handbuch Treasury

Ganzheitliche Risiko- steuerung in Finanz- instituten

H. Braun, H. Heuter

ISBN-10: 3791028472

[\(Mehr ...\)](#)



Grundlagen des Risikomanagements im Unternehmen

Werner Gleißner

ISBN-10: 3800637677

[\(Mehr ...\)](#)

SEMINARTERMINE

Im Folgenden möchten wir Ihnen wieder ausgewählte Seminare des agens Revisionsteams vorstellen.

November und Dezember 2010 sowie Januar 2011

Einführung in die Interne Revision - DIIR (Mehr...)	01. – 04.11.2010
Einführung in die IT-Revision - DIIR (Mehr...)	01. – 04.11.2010
Aufbau der Internen Revision im Unternehmen - DIIR (Mehr...)	03. – 04.11.2010
Berichterstattung der Internen Revision - DIIR (Mehr...)	03. – 05.11.2010
Einführung in die Interne Revision – SVIR (Mehr...)	08. – 11.11.2010
Der Revisionsbericht - Teil 2 – Haub + Partner (Mehr...)	11. – 12.11.2010
Prüfen der Wirtschaftlichkeit von Geschäftsprozessen - DIIR (Mehr...)	15. – 17.11.2010
Datenanalyse mit modernen Prüfwerkzeugen (ACL, Idea, RayQ, MS Excel für EU-Finanzkontrolle) – agens (Mehr...)	16. – 18.11.2010
Interne Kontrollsysteme prüfen und gestalten (IKS/VKS für EU-Finanzkontrolle) – agens (Mehr...)	16. – 18.11.2010
Immobilien Audits – Haub + Partner (Mehr...)	16.11.2010
Projekte prüfen aus Sicht der Internen Revision - DIIR (Mehr...)	17. – 18.11.2010
CobIT - DIIR (Mehr...)	18. – 19.11.2010
Prävention von wirtschaftskriminellen Handlungen (Fraud) - Tagesveranstaltung - agens (Mehr...)	16.11.2010
Gesprächs- und Verhandlungstechniken für Prüfende der EU-Finanzkontrolle) – agens (Mehr...)	30.11. – 02.12.2010
Interne Kontrollsysteme prüfen und gestalten (IKS I) - DIIR (Mehr...)	06. – 08.12.2010
Einführung in die Interne Revision - DIIR (Mehr...)	06. – 09.12.2010
Wirtschaftlichen Einsatz der IT prüfen und bewerten - DIIR (Mehr...)	09. – 10.12.2010
Revision von Veränderungsprozessen – Haub + Partner (Mehr...)	20.01.2011

Ansprechpartner: Dr. Peter Wesel (Senior Berater)

MICROSOFT EXCEL

Microsoft Excel

Auch wenn Microsoft Excel ein weit verbreitetes Standardprodukt in vielen Unternehmen ist, bleiben jede Menge Funktionen im Alltag verborgen. Wir möchten an dieser Stelle Hilfeleistung bieten und Ihnen regelmäßig über ausgewählte Funktionen/Formeln berichten.

Verwendung der Pivot-Tabelle für die Analyse von Daten (Fortsetzung)

In der letzten Ausgabe des Newsletters haben wir Ihnen die Excel-Funktion PivotTable präsentiert. Dabei wurden die ersten Schritte - wie Erstellung der PivotTable sowie die Durchführung der ersten Datenanalyse - dargestellt.

Im Weiteren möchten wir Ihnen andere Möglichkeiten der PivotTable - wie etwa die Ermittlung eines Zusammenhanges zwischen einzelnen Untersuchungsobjekten z. B. Käufer, Verkäufer und Anzahl der Rabatte - präsentieren. Mit Excel lassen sich solche Zusammenhänge am einfachsten mit PivotTable durch die Erstellung von Kreuztabellen untersuchen und grafisch darstellen.

Für die Analyse der Daten mit PivotTable nehmen wir Vertriebsdaten, wie etwa Informationen über Produkt, Bestellung, Verkäufer, Käufer, die wir im letzten Beispiel verwendet haben. (Siehe: Newsletter 2010 - Ausgabe 4_6)

Beispiel für die Erstellung von Kreuztabellen in PivotTable:

In diesem Beispiel erstellen wir den Zusammenhang zwischen dem Verkäufer und den Käufen anhand der vergebenen Rabatten und dem Umsatz. Am Ende der Analyse wollen wir sehen, bei welchen Verkäufern der Käufer eingekauft hat und welche Rabatte ihm gegeben wurden.

Dafür wird das Feld „Verkaufsberater“ in den Bereich „Zeilenbeschriftungen“, das Feld „Empfänger“ in den Bereich „Spaltenbeschriftungen“ und die Felder „Rabatt“ und „Endpreis“ in den Bereich „Werte“ verschoben (siehe Abbildung unten). Die ausgewählten Daten werden in die Tabelle automatisch übernommen (siehe Abbildung unten).

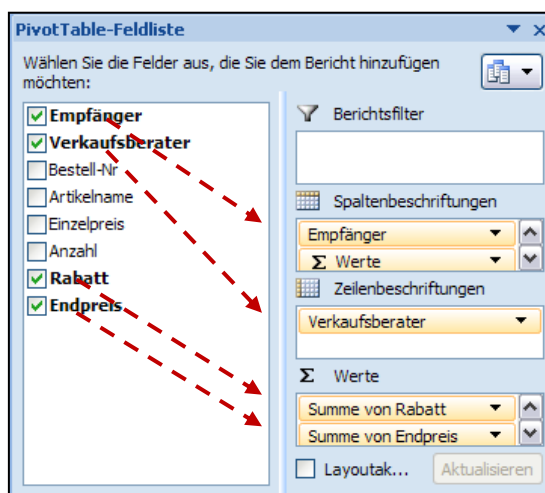


Abbildung 1: Auswahl der Felder in der PivotTable-Feldliste.

MICROSOFT EXCEL

		Victuailles en stock		Wellington Importadora		Gesamt: Anzahl von Rabatten	Gesamt: Umsatz
Verkaufsberater	Anzahl von Rabatten	Umsatz	Anzahl von Rabatten	Umsatz			
Anne Dodsworth					1	85,5	
Janet Leverling					6	548,24	
Laura Callahan					5	1131,7	
Margaret Peacock	1	159	2	241,5	9	768,36	
Michael Suyama					3	240,75	
Nancy Davolio			1	33,75	2	92,55	
Steven Buchanan					1	20,25	
Gesamtergebnis	1	159	3	275,25	27	2887,35	

Abbildung 2: Darstellung der Ergebnisse (Datenausschnitt).

In der Abbildung 2 kann man erkennen, bei welchen Verkäufern die Kunden kaufen und welcher Verkäufer am häufigsten die Rabatte (Spalte: Gesamt Anzahl von Rabatten) vergibt. Außerdem sieht man den gesamten Umsatz, den die Verkäufer erzielt haben. Anhand dieser Information kann die Analyse erweitert werden. Es kann z. B. geprüft werden, warum ein Verkäufer am häufigsten die Rabatte vergibt.

In der PivotTable können weitere Einstellungen vorgenommen werden. Man kann z. B. den Umsatz in der Tabelle prozentual darstellen. Dafür muss man mit der rechten Maustaste in die Spalte „Gesamt: Umsatz“ drücken und das Feld „Wertfeldeinstellungen“ auswählen. Im erschienenen Assistent unter Register „Werte anzeigen als“ wählt man dann „% des Ergebnisses“ und bestätigt den Auswahl mit der Taste „OK“. (Siehe Abbildung 3)

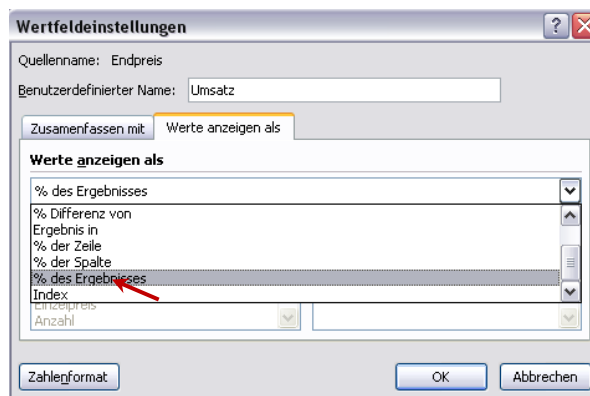


Abbildung 3: Assistent „Wertfeldeinstellung“.

		Victuailles en stock		Wellington Importadora		Gesamt: Anzahl von Rabatten	Gesamt: Umsatz
Verkaufsberater	Anzahl von Rabatten	Umsatz	Anzahl von Rabatten	Umsatz			
Anne Dodsworth					1	2,96%	
Janet Leverling					6	18,99%	
Laura Callahan					5	39,20%	
Margaret Peacock	1	5,51%	2	8,36%	9	26,61%	
Michael Suyama					3	8,34%	
Nancy Davolio			1	1,17%	2	3,21%	
Steven Buchanan					1	0,70%	
Gesamtergebnis	1	5,51%	3	9,53%	27	100,00%	

Abbildung 4: Darstellung der Ergebnisse in prozentualer Form.

In der Abbildung 4 sieht man die prozentuale Darstellung der einzelnen Umsätze zu dem Gesamtergebnis. Das gleiche Vorgehen kann man für andere Felder wie „Anzahl der Rabatte“ durchführen.

WHO IS WHO

In jeder Ausgabe werden wir Ihnen Mitglieder unseres Teams bzw. Kollegen die Revision oder Risikomanagement nahe stehen, vorstellen. Diesmal Michael Stoffels, Senior Berater im Geschäftsbereich Aktuariat



Michael Stoffels

Senior Berater

Welches war Ihr schönstes Musikerlebnis?

Ganz schwere Frage: The Clash in London, die Ärzte in WHV oder Gasoy-Romdal in Dinslaken? Hm, ich warte noch auf die 1. CD von meinem Sohn.

Welche Freizeitaktivitäten üben Sie aus?

Im nächsten Jahr möchte ich einmal einen Kurztriathlon ausprobieren. Daher versuche ich jetzt regelmäßig zu laufen, zu schwimmen und radzufahren. Theater, Städtereisen.

Was hat Sie am meisten beeindruckt?

Technisch die Entwicklung des Internets. Menschlich der Kniefall Willy Brandts in Warschau.

Was können Sie besonders gut kochen?

Als geborener Bielefelder kann das nur Pudding sein.

Was beherrschen Sie im Haushalt besonders gut?

Der Arbeit aus dem Weg zu gehen.

Was haben Sie als schönstes Käuferlebnis empfunden?

Mein erstes Auto, ein R4.

Was gefällt Ihnen an der agens am besten?

Das Geburtstagsgeschenk. Für mich ein Zeichen, dass es bei aller Leistung, die sein muss, sehr menschlich zugeht. Die tolle Unterstützung aus dem Back-Office.

Was treibt Sie an?

Die Neugier.

Welche Themen würden Sie gern beschleunigen?

Eine Fusion, aber vier Kundenanschriften. Das ist für mich eine Katastrophe, denn das unterschwellige Signal an den Kunden ist mehr Bürokratie. Es gibt ganz viele einfache Maßnahmen, um die Kundenbeziehungen zu verbessern. Man muss sie nur anpacken.

Was sind Ihre persönlichen Motivationen?

Ich löse gern Probleme.

Nennen Sie ein unentdecktes Traumreiseziel:

Es reizt mich, einmal mit dem Motorrad soweit nach Norden zu fahren wie irgend möglich.

Wen bewundern Sie am meisten?

Jeden, der schon vor dem Frühstück gute Laune hat.

Was tun Sie, um sich zu entspannen?

Ich ziehe Sportsachen an und laufe ein Stündchen.

Wo hätten Sie gern Ihren Zweitwohnsitz?

Brauche ich nicht. Auf unserem Hof ist noch Platz für ein zweites oder drittes Häuschen.

IMPRESSUM



agens Consulting GmbH
Buchenweg 11 - 13, 25479 Ellerau
Ein Unternehmen der [agens Gruppe](#)
HRB 3660 NO AG Kiel

Fon: +49(0)4106-7777-0
Fax: +49(0)4106-7777-333
Internet: <http://www.agens.com>
E-Mail: <mailto:info@agens.com>
Geschäftsführer (vertretungsberechtigt im Sinne § 6 EGG/§ 6 TDG):
Dr. Stefan Giesecke, Florian Lang, Klaus Leitner
USt.-IDNr. : DE 176972447

Aktuelle Anzahl der Ausgaben (im Zwei-Monatsrhythmus): ca. 7.800

Zum Bestellen bzw. Abbestellen des „agens Audit & Risk Newsletters“ schicken Sie bitte eine E-Mail mit dem jeweiligen Betreff und Ihrem Namen an die folgende E-Mail Adresse:

rev-ace-newsletter-akte-pf@agens.com

Disclaimer

Alle Links zu externen Anbietern wurden zum Zeitpunkt ihrer Aufnahme auf ihre Richtigkeit überprüft. Da sich das Internet jederzeit wandelt, kann die agens Consulting GmbH nicht garantieren, dass diese Links zum Zeitpunkt des Besuchs a) noch zum Ziel führen oder b) noch dieselben Inhalte besitzen, wie zum Zeitpunkt der Aufnahme.

Insbesondere macht sich die agens Consulting GmbH nicht die Inhalte der Links zu Eigen und übernimmt dafür auch keine Verantwortung. Links zu externen Anbietern stellen keine Wertung oder eine Empfehlung der agens Consulting GmbH dar.

Der Inhalt dieses Newsletters ist urheberrechtlich geschützt. Ohne Genehmigung der agens Consulting GmbH darf der Inhalt dieser Seite in keiner Form reproduziert und/oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© agens Consulting GmbH, Ellerau, Deutschland, 2010. All rights reserved.

Stand: 24.Oktober 2010