➲ Liebe Leserinnen und Leser,

die Risiken unserer vernetzten IT-Welten sind evident und permanentes Thema auch in ReVision; trotzdem konstatiert der IT-Revisor bei vielen Prüfungen immer wieder mit Erstaunen, mit welcher Leichtfertigkeit diesen Risiken begegnet wird oder mit welcher Oberflächlichkeit die IT "outgesourced" wird. IT-Sicherheit kostet Geld, und der Wirtschaftlichkeitsnachweis fällt zugegebenermaßen schwer. Unter dem Stichwort RoSI - Return on Security Investment - versucht man methodisch, diese Argumentationslücke zu schließen. Lesen Sie den diesbezüglichen Leitbeitrag von Wilhelm Kruth.

Sie führen in der aktuellen IT-Security-Diskussion bzgl. Internet, Intranet, eCommerce, WLANs als sog. “Dinosaurier” ein scheinbares Schattendasein, sind aber in den IT-Landschaften immer noch gegenwärtig und revisionsrelevant: die Großrechner und ihre Sicherheits-Tools wie RACF, ACF2 oder TOP SECRET. Halten Sie auch diesbezüglich Ihren Prüfungsplan und Ihr Prüfungswissen auf dem Laufenden.

Aktuell und dargestellt in sehr grossen Projekten findet in zahlreichen Kommunen die Umstellung von der Kameralistik zur kaufmännischen Buchhaltung statt, oft verbunden mit der Einführung von SAP R/3. Die Umsetzung und toolgestützte Begleitung dieser SAP-Projekte, wie im Beitrag von Herrn Dr. Daum von der Stadt Mannheim geschildert, ist sicher nicht nur für Revisoren des "Public"-Bereiches ein brisantes Thema.

Viel Inspiration aus unseren Beiträgen für Ihre praktische Prüfung wünscht Ihnen wie immer

herzlichst Ihr

Ottokar R. Schreiber

IT Revision

SAP R/3®

Revision

Impressum

Erscheinungsweise: ¼-jährlich jeweils Februar/Mai/August/November

Herausgeber: Ottokar R. Schreiber

Verlag: OSV Ottokar Schreiber Verlag GmbH
Friedrich-Ebert-Damm 145 • 22047 Hamburg
Fon: +49(0)40 /69 69 85 -14 • Fax +49(0)40 /69 69 85 -31
eMail: sales@osv-hamburg.de • www.revision-hamburg.de

Beiträge

Für unaufgefordert eingesandte Manuskripte wird keine Haftung übernommen. Der Verlag behält sich insbesondere bei Leserbriefen das Recht der Veröffentlichung, der Modifikation und der Kürzung vor. Leserbriefe können in beliebiger Form (handschriftlich, per eMail, Fax usw.) zugesandt werden. Manuskripte sollten uns in Dateiform zugesandt werden, vorzugsweise im RTF- oder Winword-Format, Bildmaterial bitte im TIFF-Format/Auflösung 200 dpi od. JPEG 300dpi. Zur Veröffentlichung angebotene Beiträge müssen von allen Rechten Dritter frei sein. Wird ein Artikel zur Veröffentlichung akzeptiert, überträgt der Autor dem OSV das ausschließliche Verlagsrecht, das Recht zur Herstellung weiterer Auflagen und alle Rechte zur weiteren Vervielfältigung bis zum Ablauf des Urheberrechts. Wird der Artikel Dritten ebenfalls zur Veröffentlichung angeboten, muss dies dem OSV bekanntgegeben werden.

eMail: redaktion@osv-hamburg.de

Anzeigen

Zu den Konditionen rufen Sie bitte unsere aktuellen Mediadaten ab. Zur problemlosen Abwicklung und korrekten Darstellung stellen Sie uns die Anzeigen vorzugsweise als tiff- oder eps-Datei zur Verfügung. Sollte dies nicht möglich sein, bitten wir um Rücksprache hinsichtlich der gelieferten Dateiformate. Telefon 040 / 69 69 85 -14. Design-Erstellung auf Wunsch auch durch unsere Medienabteilung möglich.

Anzeigenleitung: Alexandra Palandrani,
Telefon 040 / 69 69 85 -14
eMail: anzeigen@osv-hamburg.de

Bestellung/Abonnement:
Alexandra Palandrani
OSV Ottokar Schreiber Verlag GmbH
eMail: sales@osv-hamburg.de

DTP-Produktion

Grafik/Illustration: Dirk Kirchner, ibs schreiber gmbh
Layout/Satz: Alexandra Palandrani, OSV Hamburg

Druck: Druckerei Zollenspieker Kollektiv GmbH
Zollenspieker Hauptdeich 54
21037 Hamburg

Printed in Germany. • Gedruckt auf chlorfrei gebleichtem Papier

Allgemein

Verlagshinweis

Nächste Ausgabe der **ReVision**

November 2004

Redaktions-/ Einsendeschluss für diese Ausgabe: 20.10.2004

➲ Mission RoSI

Wirtschaftlichkeit der IT-Sicherheit

Trojaner-, Hacker- und Virenattacken gehören inzwischen zum Alltag jedes Unternehmens. Und immer noch wird das Thema Sicherheit beim Einsatz von Informationstechnik (IT), verkürzt als IT-Sicherheit bezeichnet, nicht ernst genug genommen. Die ernüchternde Botschaft fast aller Befragungen, die im vergangenen Jahr zum Thema Sicherheit in der technikunterstützten Informationsverarbeitung durchgeführt wurden, lautet: Die überwiegende Anzahl der befragten Chief Information Officer (CIO) und Chief Securiy Officer (CSO) gab zu, dass externe und interne Angriffe ihre Systeme gefährdet hätten.

Wilhelm Kruth
Euskirchen

Mit anderen Worten: es gab keine oder leicht überwindbare Sicherheitsbarrieren. In zahlreichen Fällen wurden Schäden durch gelungene Angriffe verursacht. Einer internationalen Studie zufolge haben mehr als die Hälfte der befragten Unternehmen ihr finanzielles Engagement in Sachen IT-Sicherheit im Jahr 2003 nicht aufgestockt, obwohl das Bedrohungspotenzial durch Hacker, frustrierte Mitarbeiter und andere Risikoquellen nicht kleiner wird. Nur jedes vierte Unternehmen war bereit, in 2004 mehr als im Vorjahr in IT-Sicherheit zu investieren.

Warten auf RoSI

Viele Unternehmen haben berechtigte Sorge um einen Teil- oder Gesamtausfall der installierten IT. Obwohl dieser Angstfaktor genug Antriebskraft entwickeln müsste, um mehr in Sicherheitsmaßnahmen zu investieren, ist der Sparzwang, den Chief Financial Officers (FCO) ausüben, stärker. Die Diskrepanz zwischen dem Zwang zum notwendigen Handeln einerseits und dem Zurückfahren der IT-Budgets andererseits wird oft dadurch verstärkt, dass technische und betriebswirtschaftliche Begründungen nicht auf einen gemeinsamen und für beide Seiten verständlichen Nenner harmonisiert werden können.

Aushilfe in solchen Situationen bieten Sicherheits-Metriken, die CIOs und CSOs Argumentationshilfen liefern, um Investitionen in Sicherheitsmaßnahmen überzeugender zu rechtfertigen. Voraussetzung hierfür ist, dass Risiken, denkbare Schäden und Sicherheitsmaßnahmen bereits zum Beschaffungszeitpunkt der zu schützenden Systemkomponenten ermittelt werden. Wenn dann die IT-Abteilung zum Beispiel ein Netzwerk mit einer höheren Übertragungsleistung fordert, das den Zuwachs an Anwendern und ihren Transaktionsbedarf kompensieren soll, dann muss daraus für das Sicherheitsziel der Verfügbarkeit die Metrik entwickelt werden, dass ein Netzwerk mit einer bestimmten Kapazität Risiken durch technische Ausfälle ausgesetzt ist, von denen erheblich mehr Applikationen - und damit Anwender - betroffen sind als bei einem Netzwerk mit geringerer Transferleistung. Metriken können zwar helfen, Verständigungsprobleme zu reduzieren, indem sie die Brücke zwischen technischen und wirtschaftlichen Argumenten

schlagen. Ein Ersatz für mathematische Verfahren zur Bewertung der Wirtschaftlichkeit der IT sind sie nicht.

IT-Sicherheit wird meist nur auf der Ausgabenseite verbucht. Unter dem Schlagwort "RoSI (Return on Security Investment) hilft sparen" wird die Diskussion um eine wirtschaftliche Betrachtung der IT-Sicherheit wiederbelebt.. Die Befürworter von RoSI begründen die RoSI-Mission damit, dass Investitionen in IT-Sicherheit notwendig sind, um die Kosten, die durch Angriffe real entstehen oder mit einer hohen Eintrittswahrscheinlichkeit als Schadenshöhe kalkuliert werden, erheblich zu reduzieren und damit einen Zusammenhang zwischen Gewinn und IT-Sicherheit herzustellen.

RoSI ist nicht einfach

RoSI wird allgemein definiert als eine Ertragsberechnung auf das in die IT-Sicherheit investierte Kapital. Sicherheitsinvestitionen stellen keinen unmittelbaren errechneten Nutzen dar, sondern vermeiden lediglich den Abzug von Werten. Die Bewertung des Risikos und die Bemessung der Sicherheitsmaßnahmen sind wesentliche Berechnungsgrundlagen für RoSI. Die Bemessung der Risiken umfasst die wahrscheinliche Schadenshöhe, den Aufwand, den ein Angriff und dessen Abwehr mit sich bringen, sowie die Wahrscheinlichkeit, mit der ein bestimmtes Ziel als Angriffsziel ausgesucht werden könnte.

Daraus lassen sich mehrere Erkenntnisse ableiten:

- Eine aufwändige Wirtschaftlichkeitsberechnung mit konsequenter Anwendung der RoSI-Regeln lohnt sich nicht in jedem Fall. Großunternehmen haben es hier natürlich leichter als mittelständische Unternehmen. Allerdings können auch mit einfacheren Verfahren für Sicherheitsinvestitionen in überschaubare IT-Infrastrukturen aussagefähige Erkenntnisse zur Gesamtwirtschaftlichkeit gewonnen werden.
- Sicherheitsinvestionen vermeiden oder reduzieren lediglich Wertabflüsse. Sie erzeugen allerdings auch Positiveffekte, zum Beispiel Umsatzsteigerungen infolge von Zusatzgeschäften durch sichere, neue Geschäftsmöglichkeiten oder Reduzierung des Administrationsaufwandes in der Benutzerverwaltung durch Einführung moderner Single-Sign-On-Lösungen.
- RoSI und jedes andere Verfahren zur Ermittlung der Wirtschaftlichkeit von Sicherheitsinvestitionen stehen am Ende eines einem methodischen Analyse- und Bewertungsprozesses.

Auch Anbieter von Sicherheitsprodukten vermarkten ihre Produkte oft mit RoSI-Hilfe. Dabei werden die Entwicklungs-, System- und Organisationskosten gezielt den Erträgen - oder der Vermeidung von Verlusten - gegenübergestellt, die durch eine verbesserte Sicherheit möglich werden. Standen bisher die Kosten der Implementierung einer Sicherheitslösung im Vordergrund, richtet sich der Fokus heute vermehrt auf das mögliche Einsparpotenzial einer Sicherheitslösung.

In drei Schritten zum Erfolg

Die Bewertung der Wirtschaftlichkeit von Sicherheitsinvestitionen ist der letzte Schritt in einer logischen Entwicklungsstruktur für ein Sicherheitskonzept, das diesen Namen auch verdient. Jedes Unternehmen muss sich zunächst darüber klar werden, welche Auswirkungen neue Technologien auf den IT-Einsatz in Zukunft haben werden und welchen Risiken heute und in Zukunft seine schützenswerten Objekte - Daten, Software, Hardware - ausgesetzt sind, und welche Folgen im Schadensfall sich für die Kontinuität der Leistungserbringung insbesondere in den Wertschöpfungsprozessen des Unternehmen, ergeben. Größe, Ertragskraft und Marktposition des Unternehmens bestimmen den Grad der Organisationskomplexität und der informationstechnischen Infrastruktur und damit auch den zu leistenden Aufwand für die Gewinnung von verwertbaren Erkenntnissen. Aber diese Arbeit muss in jedem

Fall geleistet werden. Erst am Ende kann man sich darüber Gedanken machen, welches Verfahren zur Bewertung von Kosten und Nutzen für eine Wirtschaftlichkeitsbetrachtung herangezogen wird.

1. Schritt: Technologie-Trends erkennen und bewerten

In der IT-Technologie spielen so genannte Mega-Trends wie eBusiness und Mobilität eine entscheidende Rolle bei der Planung künftiger Systemarchitekturen. Bekannte und beherrschbare Risikopotenziale verändern ihre Struktur oder mutieren zu neuen Bedrohungen. Das Bild der modernen IT wird geprägt durch

- die Steigerung der Komplexität infolge Abhängigkeiten und Wechselwirkungen zwischen den unterschiedlichen Technologien und dem Problem der Beherrschbarkeit von Risiken. Beispiele sind die Zuwachsraten im eBusiness-Geschäft mit der Folgewirkung dynamisch wachsender Speicheranforderungen und der Öffnung von elektronisch verwalteten Geschäftsprozessen zum Geschäftspartner oder zum Endkunden. Auf diesem operativen Geschäft setzen entscheidungsunterstützende Systeme in Data Warehouse-Technologie auf. Diese komplexe Anwendungsarchitektur stellt nicht nur neue Anforderungen an die Integration von Applikationen auf den unterschiedlichen Ebenen des Architekturmodells, neben bekannten und mehr oder minder beherrschbaren Risiken sind neue Bedrohungen zu berücksichtigen.
- die Dynamik einer Entwicklung, die durch rasante Technologiewechsel mit immer kürzeren Produktlebenszyklen von IT-Komponenten und das Verändern von charakteristischen Eigenschaften von bis dato beherrschbaren Risiken gekennzeichnet ist.
- die Kritikalität des IT-Einsatzes, die in der engen Verbindung von IT und Business und den Wirkungen von Schadenseintritten sichtbar wird.

Der Bedarf an IT und damit auch an IT-Sicherheit wächst kontinuierlich. Die hohe Bedeutung der IT für die Kerngeschäfte des Unternehmens ist unumkehrbar. Eine ordnungsgemäße, seriöse und haltbare Planung des IT-Einsatzes in einem kurz- und mittelfristigen Planungshorizont ist ohne die Entwicklung eines Sicherheitsprofils für die zu schützenden Objekte nicht denkbar.

2. Schritt: Ermittlung des Risikowertes

Eine Risikoanalyse liefert Erkenntnisse über bekannte oder vermutete Bedrohungen, deren Eintrittswahrscheinlichkeit und die Folgen gelungener Angriffe, die in der monetär bewerteten Schadenshöhe sichtbar werden.. Der Analyse- und Bewertungsprozess muss gründlich vorbereitet werden. Dazu gehört ein gemeinsames Verständnis der Beteiligten für Aufgaben und Ziele eines leistungs- und entwicklungsfähigen Sicherheitskonzeptes. In einem weiteren Vorbereitungsschritt werden für die Kerngeschäfte des Unternehmens

- die für die Leistungsprozesse relevanten Daten ermittelt und nach verschiedenen Kriterien wie Aufwand und Kosten einer Wiederbeschaffung und den Informationswert für Konkurrenzunternehmen in verschiedene Sicherheitsklassen eingeteilt. Für diese Maßnahme ist es unerheblich, ob es sich um personenbezogene oder rein sachorientierte Daten handelt. Im Vordergrund der Betrachtungen steht hier das Interesse des Unternehmens an einer umfassenden Informationssicherheit.
- die tragbaren und maximal tolerierbaren Ausfallzeiten diskutiert. Zeithorizont für die Bestimmung der maximal tolerierbaren Ausfallzeit ist die Existenzgefährdung des Unternehmens infolge Nichtverfügbarkeit von Daten und / oder anderen Ressourcen der IT, die für die Leistungserbringung in den Kerngeschäften unverzichtbar sind und nicht in einer akzeptablen Zeit wieder verfügbar gemacht werden können.

Die richtige Bewertung der Kritikalität von Daten ist ein Problem in vielen Unternehmen. Beispielsweise schützt ein Unternehmen den Zugang zm Speiseplan im Intranet mit der gleichen Technologie wie den Zugang zu persönlichen Daten über Mitarbeiterportale. Die Informationssicherheit ist in diesem Falle für den Speiseplan zu hoch und den Schutz personenbezogener Informationen zu gering. [ ] Es gilt der Grundsatz, dass das aus dem Schutzbedarf der Daten und der für die Speicherung, Verarbeitung und Übermittlung eingesetzten Systeme das Anforderungsprofil für angemessene Sicherheitsmaßnahmen zu entwickeln ist. Nur dann kann eine RoSI-Berechnung auf Basis valider Daten durchgeführt werden.

Bei der Ermittlung und Bewertung von Risiken herrscht oft Hilflosigkeit vor. Investitionsentscheidungen für IT-Sicherheit beruhen daher oft auf Furcht, Unsicherheit und Zweifel. Die von Unternehmensberatern oft und gerne durchgespielten Worst Case-Szenarien und der permanente Hinweis auf gesetzlich definierte Sicherheitsanforderungen sind kontraproduktiv, weil sie Ängste und Zweifel nicht beseitigen, sondern verstärken.

Die Analyse von Schadenswirkungen, die durch externe oder interne Angriffe erzeugt werden können, beruht in den meisten Fällen nur auf Annahmen, da es an eigenen historischen Daten mangelt. Statistiken über Anzahl und Folgewirkungen von Schäden, die jedes Jahr in breiter Fülle auf den Markt geschwemmt werden, liefern nur schlichte Erkenntnisse darüber, welche Risiken in einem bestimmten Zeitraum in welcher Häufigkeit aufgetreten sind. Die Bulletins des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und andere Informationsquellen im Internet bieten hier ein deutliches Mehr an aktueller Information. Dies gilt besonders für Angriffe, die durch Viren & Co und Hacker erfolgen. Sie stellen eine permanente Bedrohung mit einer hohen Eintrittswahrscheinlichkeit dar. Da diese Angriffe wie alle anderen Störungen des ordnungsgemäßen Systembetriebes technische und / oder organisatorische Schwachstellen als Einfallstor benutzen, ist es zweckmäßig, zunächst diese Schwachstellen zu ermitteln. Hierfür wie für die weiteren Aktionen zur Ermittlung und Analyse von Risiken bieten sich Szenarien als instrumentale Möglichkeiten einer ganzheitlichen Problemsicht an. Verwertbare Aussagen zu den Wirkungsgrößen eines Schadens können nur im Dialog mit den Informationseigentümern, also den verantwortlichen Fach- bzw. Geschäftsbereichen, gewonnen werden.

Die rechnerische Ermittlung des Risikowertes nach der Formel "Risikowert = Eintrittswahrscheinlichkeit * Schadenshöhe" setzt den Schlusspunkt unter die aufwändigen, aber notwendigen Vorarbeiten. Die rein quantitative Ermittlung des Risikowertes berücksichtigt nicht die Forderungen, die das Aktiengesetz, das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, die Datenschutzgesetze und sonstige Rechtsvorschriften an die Herstellung und kontinuierliche Fortentwicklung der IT-Sicherheit stellen. Bei der Abschätzung der Risiken und der Folgen eines Störfalls sind daher zusätzlich die gesetzlichen Anforderungen an den ordnungsgemäßen und damit sicheren Betrieb der IT, die Haftungsfragen, die sich aus gesetzlichen und vertraglichen Regelungen ergeben und die Anforderungen von Geschäftspartnern und Endkunden an das "Vertrauensprinzip" im elektronischen Geschäftsverkehr zu berücksichtigen.

Die Ergebnisse der Risikobewertung werden in Risiko-Portfolilos präsentiert. Aus den Portfolios ist nicht nur erkennbar, welche Sicherheitsmaßnahmen vordringlich zu realisieren sind, sondern auch, welche "Wanderbewegungen" in der Entrittswahrscheinlichkeit zu erwarten sind und welche Auswirkungen sich darauf auf die Schadenshöhe ergeben. Typische Veränderungen sind zum Beispiel die wachsende Zahl von Viren-, Wurm- und Trojaner-Attacken, oder ein verstärktes Risiko durch ein sich verschlechterndes Sozialklima im

Unternehmen mit der Folge, dass die Zahl der internen Angreifer zunimmt.

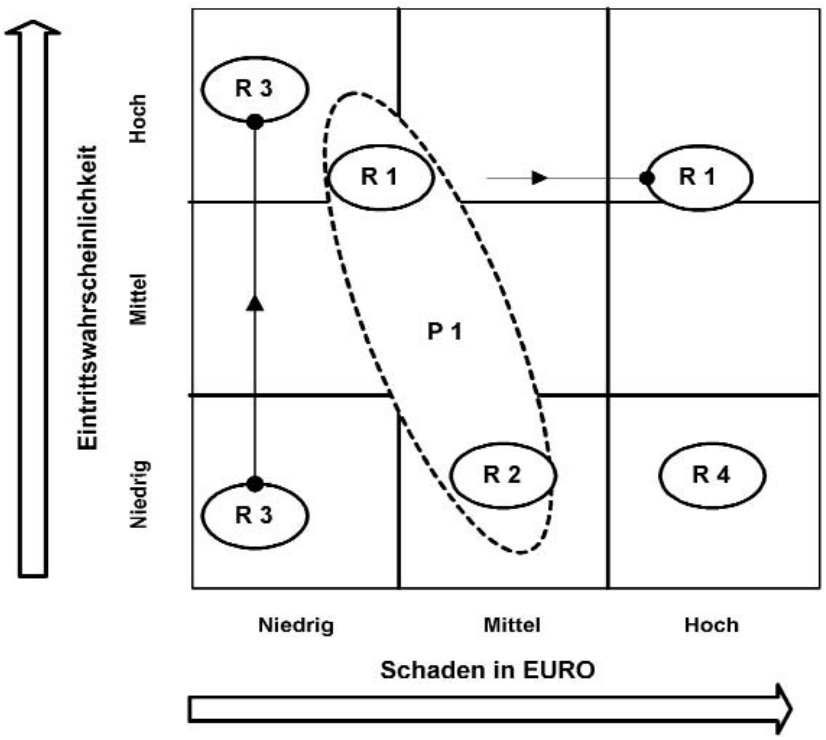


Abb. 1 Risiko-Portfolio

Die "Wanderbewegungen" sind durch Pfeile markiert. Über das Portfolio kann als weitere Sicht die Zuordnung von Risiken zu definierten Prozessen erfolgen (Prozess P1 ist den Risiken R1 und R 2 ausgesetzt).

Das Gesamtrisiko ergibt sich aus der Summation der Einzelrisiken. Kritische Erfolgsfaktoren für die Aussagekraft der Risiko-Portfolios sind die Vollständigkeit analysierter Bedrohungs-Szenarien, die Ermittlung der realistischen Eintrittswahrscheinlichkeiten und die Berechnung der Schadenshöhe.

3. Schritt: Wirtschaftlichkeitsbetrachtung

Kosten für Sicherheitsmaßnahmen erhöhen anfangs den Schutz sprunghaft, ab einer einer frühen Grenze steigt der Schutz allerdings nur noch linear. Eine höhere Eintrittswahrscheinlichkeit eines Angriffs führt zur Erhöhung der notwendigen Kosten für ein vergleichbares Sicherheitsniveau.

Mit den einmal getätigten Investitionen ist es nicht getan. Für IT-basierte Sicherheitsprodukte gilt das Gleiche wie für jede andere Hardware und Software: die Lebenszyklen werden kürzer, neue Technologien bringen deutliche Mehrwerte in der Abwehr von Angriffen gegenüber vorhandenen Sicherheitsbarrieren. Kostentreiber sind aber auch neue oder erweiterte Handlungsfelder der IT-Nutzung und die sich daraus entwickelnden Risikopotenziale. Wichtig ist, dass bei der Auswahl von Sicherheitsmaßnahmen und der Bewertung ihrer Schutzwirkung gegenüber Angriffen nicht nur auf Einzelmaßnahmen abgestellt wird, sondern eine ganzheitliche Betrachtung angestrebt wird. Einzelne Maßnahmen für sich haben häufig nur einen begrenzten Schutzwert. Oft wird erst durch die Kombination von einzelnen Maßnahmen das definierte Sicherheitsprofil erfüllt.

Die Kosten für ein konkretes Bedrohungs-Szenario können durch gezielte Maßnahmen zur Risikovermeidung, Risikoverminderung durch Prävention und Risikoüberwälzung reduziert werden. Durch die Beseitigung von Schwachstellen in der Geschäfts- und Prozessorganisation werden Risiken vermieden. Präventive Maßnahmen wie ein effizientes Risiko-Management oder eine hochverfügbare Firewall-Architektur bewirken eine Risikoverminderung. Eine Risikoüberwälzung auf Versicherungen entlastet im Schadensfall das Budget zur Abdeckung von Folgekosten, die durch Aufwände zur Herstellung eines stabilen und konsisten Betriebszustandes entstehen. Risikoakzeptanz wird durch eien transparente Informationspolitik erreicht, die nicht vermeidbare Risiken diskutiert. Risikoakzeptanz ist aber auch die Bereitschaft, in notwendige Sicherheitsmaßnahmen zu investieren. Am Ende bleibt das Restrisiko.

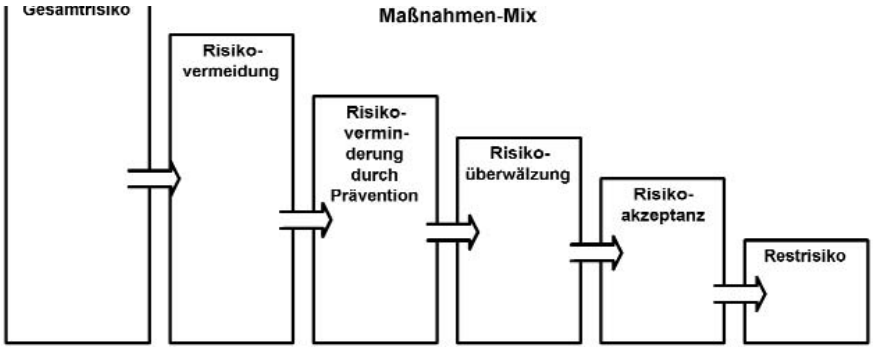


Abb. 2 Massnahmen-Mix zur Kostenreduzierung

An zwei einfachen Beispielen soll deutlich gemacht werden, welche direkten Kosten durch Schäden in fast alltäglichen Störfällen entstehen können:

1. Während eines nächtlichen Gewitters schlug in einen Baukran der Blitz ein. Sein weiterer Weg ins Erdreich führte ihn dann an Telefonkabeln vorbei. Die entstandene Überspannung breitete sich gleichmäßig aus und erreichte auch die Telefonanlage eines großen Maklerbüros, dessen Räume auf dem Nachbargrundstück lagen. Die Telekommunikationsanlage des Maklerbüros konnte zwei Tage nicht benutzt werden, der vom Maklerbüro insgesamt ermittelte Schaden wurde mit 17.000 EUR bewertet.
2. Durch einen nicht erklärbaren Systemabsturz gingen Daten verloren. Weil der für die Datensicherung zuständige Mitarbeiter in Urlaub war, unterblieb die sonst übliche Datensicherung, weil Anweisungen zur Datensicherung einfach fehlten. Man musste auf eine frühere Sicherung zurückgreifen und die fehlenden Daten manuell ermitteln und erneut eingeben. Die Zeitdauer der Nichtverfügbarkeit eines konsistenten und aktuellen Datenbestandes betrug mehrere Tage. Die Kosten nur für die Wiederherstellung wurden mit 2.000 EUR beziffert. [ ]

Beide - bewusst einfach gewählte - Beispiele sind so genannte Alltagsfälle. Neben den Kosten ist der nicht monetär bewertbare Schaden zu berücksichtigen, der durch Vertrauensverlust von Kunden und Mitarbeitern in die Verlässlichkeit und Stabilität der elektronischen Helfer entstanden ist. Und hier kommt eine Positivargumentation für die Investition in Sicherheitsmaßnahmen ins Spiel. IT-Sicherheit im Unternehmen gilt eben nicht nur als Schutzmaßnahme gegen Bedrohungen oder als Instrument zur Kostenreduktion, sondern auch als Mittel zur Pflege und Intensivierung von Beziehungen zu Geschäftspartnern und Kunden. So können zum Beispiel die eMails eines Geschäftspartners fast bedenkenlos geöffnet werden, wenn bekannt ist, dass sich das Unternehmen mit aktuellen Sicherheitslösungen wirksam schützt.[ ]

Aufwändige Berechnungen sind nicht immer sinnvoll. Für überschaubare IT-Infrastrukturen und die darauf aufsetzenden Sicherheitskonzepte können einfache mathematische Verfahren angewendet werden. Sie liefern im Ergebnis allerdings nur Aussagen über Kostengrößen und allenfalls eine grobe Nutzeneinschätzung, argumentativ "verkaufbare" Nutzwerte müssen in einer gesonderten Analyse ermittelt werden.

Eine einfache Amortisationsrechnung liefert bereits verwertbare Erkenntnisse über die Kostenersparnisse, die durch eine Investition in Sicherheitsmaßnahmen erzielt werden. Dabei wird die Differenz zwischen den Investitions- und laufenden Kosten für Sicherheitsmaßnahmen und der Höhe der vermiedenen Schäden ermittelt und anschließend der Amortisationszeitpunkt berechnet.. Beispiel: Ein Intrusion Detection-System (IDS) zur Erkennung und Abwehr von Angriffen aus dem inneren Netz kostet 40.000 EUR. Die Wirksamkeit des Systems wird mit 85 % Abwehrleistung geschätzt. Ohne den IDS-Einsatz wird ein Schaden in Höhe von linear 100.000 EUR/Jahr erwartet. Der jährliche "Gewinn" aus der Investition beträgt damit 45.000 EUR/Jahr. Die Beschaffung hat

sich damit innerhalb eines Jahres amortisiert.

Ein weiteres Verfahren dient der Ermittlung des relativen Nutzens einer Sicherheitsmaßnahme durch Ermittlung der Kostendifferenz der Risikowerte und Subtraktion der Investitionskosten von der Kostendifferenz.. Ist das Ergebnis > 0, wird der Einsatz der Sicherheitsmaßnahme unter Kostengesichtspunkten positiv bewertet. Die Anwendung erfolgt in mehreren Schritten:

- Ermittlung des Risikowertes ohne Sicherheitsmaßnahme (R0) nach der bekannten Formel
  R0 = S0 * W0

- Ermittlung des Risikowertes (R) mit Sicherheitsmaßnahme (R1) nach der bekannten Formel
  R1 = S1 * W1

- Ermittlung des relativen Nutzens (NS) der Sicherheitsmaßnahme
  NS = (R0 - R1) - Ks

Beispiel: Die Ausgangssituation ist ein angenommener Schaden von 100.000 EUR für den Fall eines Virusbefalls. Die Eintrittswahrscheinlichkeit beträgt 30 % pro Jahr, der erwartete Verlust dementsprechend 30.000 EUR. Man geht davon aus, dass man die Eintrittswahrscheinlichkeit durch eine Antivirus-Software um zwei Drittel senken kann. Die Kosten der Softwarebeschaffung betragen 12.000 EUR/Jahr.

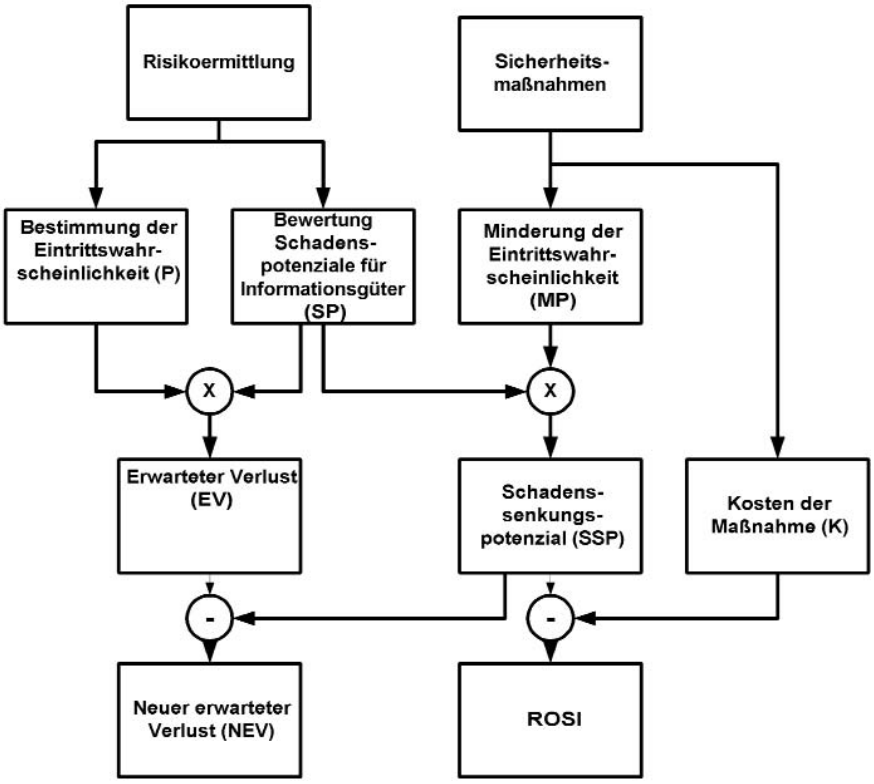


Abb. 3 Berechnungsmodell RoSI

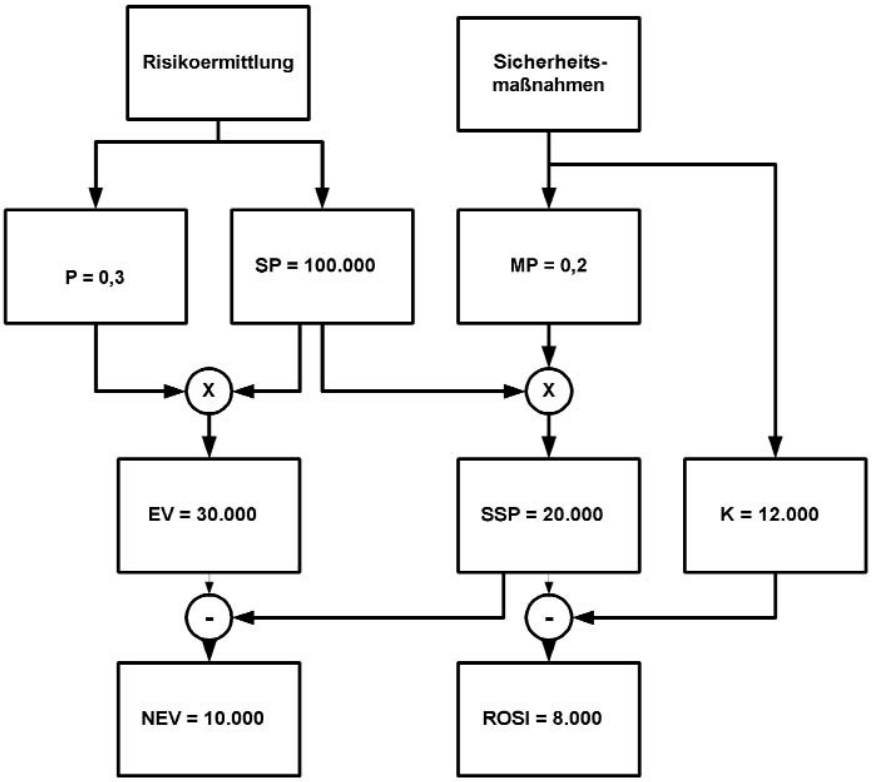


Abb. 4 RoSI-Berechnungsbeispiel

R0 = S0 * W0
30.000 € = 100.000 EUR * 0,3

R1 = S1 * W1
10.000 € = 100.000 EUR * 0,1

NS = (R0 - R1) - Ks
8.000 € = (30.000 EUR - 10.000 EUR) - 12.000 EUR

Bei der Anwendung eines Berechnungsschemas, das eng an die "Return on Investment" (RoI)-Systematik angelehnt ist, ergibt sich zwar rechnerisch das gleiche Ergebnis. Die Berechnungsfaktoren sind jedoch aussagefähiger, das Modell liefert insgesamt bessere Erkenntnisse in der schrittweisen RoSI-Ermittlung.

Überträgt man das oben beschriebene Beispiel in das RoSI-Berechnungsmodell, so ergibt sich Abbildung 4.

Das Risiko für das Unternehmen wird sich durch die Einführung der Antivirus-Software entscheidend senken. Die Investition lohnt sich, weil ein positiver RoSI von 8000 EUR errechnet wurde.

Fazit

Mit RoSI lassen sich die Erträge des in IT-Sicherheit investierten Kapitals kalkulieren. Die Berechnung liefert eine unentbehrliche Argumentationshilfe bei Diskussionen über die Notwendigkeit von Investitionen in IT-Sicherheit. Von der IT-Sicherheit hängt heute die Existenzfähigkeit eines Unternehmens im selben Ausmaß ab wie etwa ein produzierender Betrieb von der Qualitätssicherung.

➲ Prüfung eines Network Attached Server-Systems (NAS)

In der Informationstechnologie gespeicherte Daten entwickeln sich, je nach Schutzbedarfsklasse, immer stärker zu wichtigem und schützenswertem Vermögen. Seriöse Analysen haben aufgezeigt, dass die Nichtverfügbarkeit wichtiger Daten schon bei einer Ausfallzeit von mehr als vier Stunden zu hohen Schäden für ein Unternehmen führen kann.

Dipl.-Betriebswirt
Axel Hirsch,
CISA, IT-Revisor bei der
Deutsche WertpapierService
Bank AG, Frankfurt am Main

Technisch erfolgt die Speicherung der Daten immer mehr in separaten (Fibre Channel) Speichernetzen bzw. in dedizierten Massenspeichergeräten. Hier sind neben der Gewährleistung einer hohen Zugriffsgeschwindigkeit auch die Integrität und die Vertraulichkeit der Daten von hoher Bedeutung. Bezüglich Speicherkapazität und Zugriffsgeschwindigkeit vollziehen diese Systeme eine rasante Entwicklung mit der (unerwünschten) Folge, daß die Betrachtung von Sicherheitsfragen der Entwicklung hinterher läuft. In Folge dessen hat die Fachwelt begonnen, sich des Themas anzunehmen und Sicherheitsempfehlungen zu erarbeiten.

Auch der IT-Revisor sieht sich mit der Frage konfrontiert, mit welchen Prüfungsansätzen er an solche - mit hohem Bruttorisiko versehene - technisch komplexe Systeme herangehen soll. Im nachfolgenden Artikel werden, aus der Erfahrung mit der Prüfung eines NAS-Systems heraus, revisorische und technische Prüfungsfragen strukturiert erarbeitet und in Form einer Checkliste zur Verfügung gestellt.

Grundlagen

Ist es nun ein File-Server-Cluster, ein Network Attached Server (NAS) oder ein Storage Area Network (SAN)? Diese oder ähnliche Fragen stellen sich dem Prüfer als Ausgangspunkt der Betrachtung. Im nachfolgenden soll der Unterschied zwischen den gängigsten Systemen NAS und SAN kurz erläutert werden.

Network Attached Server (NAS)

In einem NAS verwaltet ein einzelner NAS-Server den Zu-

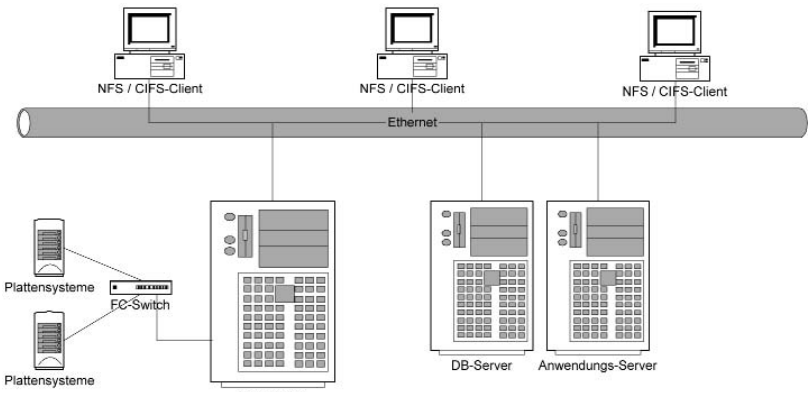


Schaubild 1: NAS-System

gang zum Fibre Channel Netz. In sein Betriebssystem sind alle Platten eingebunden. Er stellt diese über ein exklusives Backbone-Netz den anderen Servern über Netzwerkzugriff zur Verfügung. Ein NAS-Server muß nicht übermäßig dimensioniert sein, da er selbst keine Daten verarbeitet, sondern nur den Zugriff bereit stellt.

Storage Area Network (SAN)

Ein Storage Area Network setzt darauf auf, daß sich alle Massenspeichergeräte in einem separaten (Fibre Channel) Netz befinden. Es bietet ein hohes Maß an Flexibilität, da Platten nicht mehr an Server angeschlossen, sondern nur noch im SAN eingebunden werden.

Prüfungsansätze

Die Prüfungsansätze reflektieren die aus der Prüfung eines NAS-Systems, implementiert auf Windows2003-Server, gewonnenen Erfahrungen.

Möglich wäre die Durchführung eines Basis-Sicherheitschecks nach der Methode des Bundesamtes für Sicherheit in der Informationstechnik (BSI), wobei das Thema Speichernetze / dedizierte Speichergeräte (SAN oder NAS) im Grundschutzhandbuch noch nicht explizit in einem Baustein behandelt wurde. Deswegen müssen das Prüfungsobjekt tangierende Bausteine wie z.Bsp. "Vernetzte Systeme" oder "Infrastruktur" angewandt werden kombiniert z.Bsp. mit den Empfehlungen des "Microsoft Windows Server 2003-Sicherheitshandbuches".

Für eine Erstprüfung sollen hier jedoch dem Prüfer Ansätze in Form einer Checkliste an die Hand gegeben werden mit dem Ziel, eine allzu lange Vorbereitung auf die Prüfung durch Einarbeitung in die Methodik des BSI-Basissicherheitschecks zu vermeiden. Dadurch soll er in die Lage versetzt werden, eine Prüfung möglichst effizient durchführen zu können.

Ein strukturierter Prüfungsansatz sollte die nachfolgenden Schwerpunkte abdecken:

- Hard- und Softwareausstattung des Systems
- System und Servermanagement
- Ausfallsicherheit und Lastverteilung
- Sicherheitsmaßnahmen.

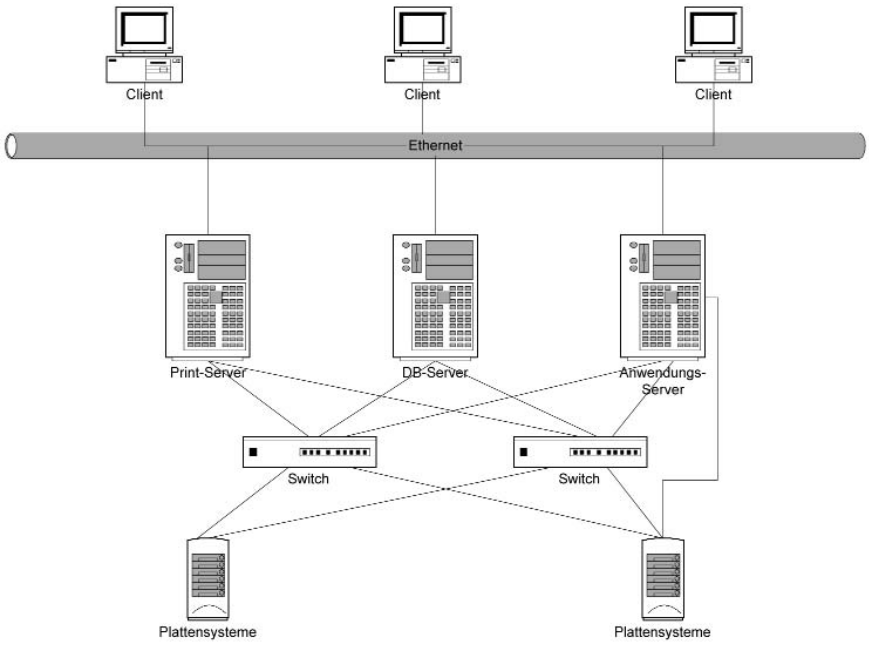


Schaubild 2: SAN-System

Hard- und Software-ausstattung des Systems

Zu Beginn der Prüfung und als Grundlage für weitere Prüfungshandlungen sollte der IT-Revisor die Hard- und Softwareausstattung des Systems kennenlernen und beurteilen. Er erhält dadurch einen Überblick über die Konfiguration des Systems sowie des Netzes. Auf diesen Erkenntnissen aufbauend können dann die nachgelagerten Prüfungsschwerpunkte risikoorientiert verfeinert werden.

Mindestens nachfolgende Fragen sollten in diesem Prüfungsschwerpunkt beantwortet werden:

- Ist das eingesetzte Betriebssystem gehärtet?
- Sind die wichtigsten System- und Netzkomponenten redundant ausgelegt?
- Lagen der redundanten Auslegung Risikobetrachtungen zugrunde?
- Werden Raidsysteme eingesetzt?
- Wie erfolgt die Verwaltung von Speicherplatz?
- Wird mit Datenträgerkontingenten gearbeitet?
- Bestehen Wartungsverträge?
- Wurde bei der Auswahl des Systems darauf geachtet, nur erprobte Technik einzukaufen?
- Wurden während des Auswahlprozesses entsprechende Referenzen gesucht und befragt?

System und Servermanagement

In diesem Prüfungsschwerpunkt ist primär das Vorhandensein von formellen Regelungen zu prüfen, die jedoch in einem weiteren Schritt auch unter materiellen Gesichtspunkten beurteilt werden müssen. Je nachdem, ob die Leistung in Eigenregie oder durch einen IT-Dienstleister erbracht wird, sind auch noch Service Level Agreements und deren Erfüllungsgrad zu prüfen. Fragen zur Wirtschaftlichkeit des Outsourcings von IT-Leistungen sind hier nicht Gegenstand der Betrachtung.

Folgende Fragen sind hier zu beantworten:

- Sind die Aufgaben und Verantwortlichkeiten geregelt?
- Existieren Regelungen zum Netz- und Systemmanagement?
- Existieren Regelungen zum Überwachen (Monitoring) des Systems und der Server?
- Erfolgen statistische Auswertungen?
- Existieren Service Levels?

Ausfallsicherheit und Lastverteilung

Wie auf dem Schaubild 1 unschwer zu erkennen ist, werden alle administrativen Probleme auf einen einzigen NAS-Server beschränkt. Dies ist somit der kritische Punkt des Systems. Fällt dieser Rechner aus, kann keines der Serversysteme mehr auf die Daten im Fibre Channel Netz zugreifen.

Daher sollten NAS-Systeme als Clustersysteme konfiguriert werden. Ein Cluster besteht im einfachsten Fall aus zwei Rechnern, die sich wie ein einziger, virtueller Server im Netzwerk darstellen. Fällt einer der beiden Clusterrechner aus, wird der virtuelle Zugriff auf die Daten immer noch vom anderen Clusterrechner zur Verfügung gestellt.

Ein weiterer kritischer Punkt wäre der Ausfall des FC-Switches. Risikomindernd könnte hier (im Schaubild 1 nicht eingezeichnet) z.Bsp. eine Direktverbindung des NAS-Systems zu einem der Massenspeichersysteme wirken. Im Fehlerfall kann dann immer noch darüber auf die dort lagernden Daten zugegriffen werden.

Folgende Fragen sollten deshalb geklärt werden:

- Kommt ein Clustersystem zum Einsatz?
- Ist die Konfiguration vollständig dokumentiert?
- Welche Funktionen / Dienste gewährleisten die Ausfallsicherheit?
- Welche Funktionen / Dienste gewährleisten die Lastverteilung?

Sicherheitsmaßnahmen

Bei dem Prüfungsobjekt handelte es sich um Windows2003-Server, die als NAS-Cluster-system konfiguriert wurden. Die nachfolgenden Fragen fokussieren deshalb im wesentlichen auf Windows2003-Server, können jedoch im Grundsatz auch auf andere Systeme angewandt werden.

- Gibt es Sicherheitsrichtlinien für die Konfiguration von Servern?
- Sind alle nicht benötigten Systemdienste (z.B. DNS, DHCP) abgeschaltet?
- Laufen die Dienste unter dedizierten Dienstkonten?
- Sind die dedizierten Dienstkonten für den interaktiven

Zugang zum System gesperrt?
- Sind für die Verzeichnisse und Dateien Risikoklassifizierungen vorgenommen worden?
- Arbeiten Benutzer mit verschlüsselten Ordnern und Dateien (Encrypting File System)?
- Sind für Verzeichnisse und Dateien bedarfsgerechte Zugriffsberechtigungen vergeben?
- Wie sind die Zugriffsberechtigungen auf Verzeichnisse und Dateien organisiert (z.B. über globale und lokale Gruppen)?
- Kommen Überwachungsrichtlinien zum Einsatz?
- Werden die Protokolldateien regelmäßig ausgewertet?
- Welche lokale Konten existieren?
- Ist das Administratorkonto umbenannt?
- Ist das Gastkonto deaktiviert?
- Sind die Administrator-Berechtigungen angemessen vergeben?
- Erfolgt bei dem lokalen Administrator-Konto ein regelmässiger Paßwortwechsel?
- Ist mit dem Snap-In "Sicherheitskonfiguration und -analyse" der aktuelle Status der Systemsicherheit mit der Sicherheitsvorlage sicherer Dateiserver (ocfiless.inf) verglichen worden?
- Welche Sicherheitseinstellungen kommen über Gruppenrichtlinien zum Tragen und sind diese nachvollziehbar dokumentiert?

Ein Großteil der Fragen kann vom IT-Revisor toolgestützt durch Einsatz von Tools (z.Bsp. den Microsoft Baseline Security Analyzer oder den LANguard Network Security Scanner) analysiert werden.

Ein Großteil der vorgenannten Fragen kann vom IT-Revisor toolgestützt durch Einsatz von Tools (z.Bsp. den Microsoft Baseline Security Analyzer oder den LANguard Network Security Scanner) analysiert werden. Diese zeigen dem technisch versierten IT-Revisor nicht nur die Schwachstellen, sondern bieten teilweise auch konkrete Maßnahmenempfehlungen zur Minderung der Risiken an.

Fazit und Ausblick

Dedizierte Speichergeräte, in diesem Fall ein NAS-System, sind komplexe technische IT-Systeme, die an einen IT-Revisor hohe Anforderungen stellen. Er sollte sich dem System in einer Erstprüfung "nähern" und Erfahrungen sammeln, auf diesen aufbauen und die Prüfungsansätze in Folgeprüfungen risikoorientiert verfeinern. Im Spannungsfeld zwischen Qualitätsanspruch, knappen Zeit-Ressourcen und Zielvorgaben bezüglich des einzuhaltenden Prüfungsplanes ist dies kein leichtes Unterfangen. Die von mir aufgezeigten Prüfungsansätze sollen dem IT-Revisor zeigen, was bei einer Erstprüfung schwerpunktmäßig zu prüfen ist und es ihm ermöglichen, effizient zu arbeiten. Bleibt er dabei in dem von mir empfohlenen Scope, kann er im Rahmen einer Erstprüfung ein qualitativ gutes Prüfungsergebnis erreichen.

Technisch komplexe IT-Systeme verlangen ein nicht zu unterschätzendes Spezialwissen, das oftmals ad hoc nicht verfügbar ist. Daraus ergeben sich Fragen nach den Prüfungsansätzen, der Prüfungstiefe, der Aus- und Weiterbildung sowie der Hinzuziehung von Spezialisten für die Prüfung. Diese zu beantworten wird in naher Zukunft für alle im Prüfungswesen handelnden Personen eine große Herausforderung darstellen. Auch in den Standesorganisationen (IIR und ISACA) wird man sich darüber Gedanken machen müssen.

Für die Zukunft bleibt abzuwarten, wie sich das Berufsbild des IT-Revisors weiter entwickeln bzw. verändern wird. Der IT-Revisor muß eine Strategie entwickeln, wie er auch in Zukunft seine Akzeptanz im Unternehmensumfeld behaupten kann. Daran wird er letztendlich gemessen werden.

Literaturhinweise

D.H. Traeger / A. Volk, Praxis lokaler Netze

SNIA Storage Security Industry Forum, The Best Practices for Ensuring Enterprise Storage

➲ Revision von RACF

Die oft als Dinosaurier bezeichneten Großrechner sind noch lange nicht ausgestorben. Sie werden noch über Jahre ihre Dienste bei bewährten "Altverfahren" versehen. Auch wenn die Großrechner über einige Sicherheitsmechanismen verfügen, reichen diese jedoch nicht aus, um die Sicherheit in der Informationstechnologie zu gewährleisten. Zusätzliche Softwareprodukte wie RACF von IBM, ACF2 und TOP SECRET von Computer Associates bieten die Möglichkeit, durch ihren organisierten Einsatz die Sicherheit zu erhöhen. Die genannten Softwarelösungen kommen bei den meisten IBM-Großrechnern zum Einsatz.

Thomas Daniel Schmidt,
Rheinland Versicherung,
Neuss

Bei der Prüfung von RACF sind dem Prüfer ohne tieferes Wissen von RACF und seiner Arbeitsweise die Hände gebunden. Zu vielfältig sind die Möglichkeiten an Rechte zu gelangen und zu umfangreich die Rechtevergabe. Auch die Möglichkeiten die RACF-Protokolle aus dem SMF (System Management Facility) zu deuten ist fast unmöglich.

Die für den Revisor vorgesehenen Standardhilfsmittel reichen nicht aus um einen Revisionsauftrag RACF durchzuführen. Sicher ist es sinnvoll vor Durchführung eines solchen Auftrages eine entsprechende Schulungsmaßnahme durchzuführen um gestärkt mit aktuellen Wissen der Aufgabe "RACF" zu begegnen.

Sofern ein Unternehmen eines der auf dem Mark befindlichen RACF-Administrationsprodukte einsetzt, wie z.B. SAM, Control SA usw. sind Sie aus Prüfer in der glücklichen Lage, mehr Informationen in aufbereiteter Form zu bekommen.

Sofern Sie aber nur mit den Standardmöglichkeiten von RACF auskommen müssen - wünsche ich Ihnen schon heute viel Spaß bei Ihrer Prüfung.

Was Sie jedoch weder mit Hilfsmitteln oder den Standardmöglichkeiten erkennen können sind die Schwachstellen/Fehler die RACF selber hat. Hier gibt es einige die zu beachten sind.

Meine Empfehlung hier wäre - werden Sie Mitglied in der RACF-Arbeitsgruppe. Hier werden diese Probleme behandelt und einer Lösung zugeführt - wenn die Lösung auch manchmal lange auf sich warten lässt.

Nachfolgend einige Informationen, Aktionen und Möglichkeiten, wie Sie dennoch eine Prüfung von RACF durchführen können - viel Spaß dabei.

Wenn mehrere Personen die gleichen Informationen benutzen müssen, dann muß die Kontrolle darüber gewährleistet sein, wer die Informationen benutzt und wann und wie sie benutzt werden. Diese Kontrolle kann eine physische Einrichtung, eine Funktion der Maschine sein. Bei einer Maschine kann es notwendig sein, einen Schlüssel einzustecken, bevor die Maschine läuft. In einem Computersystem kann diese Kontrolle auch durch Software wahrgenommen werden. RACF ist eine Software, die einem

Unternehmen hilft, den Zugriff auf Informationen zu steuern.

RACF verwendet in etwa die gleiche Struktur wie ein Unternehmen. Es erlaubt, daß Einzelpersonen und Gruppen eingerichtet werden und daß angegeben wird, was jede Einzelperson (User) und Gruppe tun darf. Einige Einzelpersonen und Gruppen haben einen großen Autoritätsbereich, während andere nur eine sehr eingeschränkte Autorität besitzen.

Der jeweilige Umfang der Berechtigungen ist durch den Aufgabenbereich bestimmt. Wenn sich die Anforderungen ändern, dann können sich auch die Berechtigungen ändern. Es ist beispielsweise auch möglich, daß bestimmte Berechtigungen nicht ständig, sondern nur für die Durchführung bestimmter Aufgaben erforderlich sind. Ein Benutzer sollte dann zu einer Gruppe gehören, die die notwendigen Berechtigungen besitzt. Wenn sich die Arbeitsanforderungen ändern, kann er aus der Gruppe entfernt werden.

RACF ist ein Sicherheitssystem, das jeden Benutzer eindeutig identifiziert und festhält, was er innerhalb des Systems tut. RACF verwendet Benutzerattribute, Gruppenautorisierungen und Zugriffsberechtigungen für Ressourcen, um die Benutzung des Systems zu kontrollieren.

RACF hält außerdem fest, was innerhalb des Systems geschieht, so daß nachvollzogen werden kann, was die einzelnen Mitarbeiter tun und ob versucht wurde, unerlaubte Tätigkeiten durchzuführen. Die von RACF erzeugten Berichte sollen als Abschreckung für unerlaubte Versuche, auf Informationen zuzugreifen, dienen. Darüber hinaus ist RACF auch in der Lage festzustellen, ob ein Benutzer Zugriff auf mehr Informationen benötigt, um seine Aufgaben effektiver zu erledigen. Wenn aus den RACF-Berichten hervorgeht, daß ein Benutzer ständig ohne Erfolg versucht, auf bestimmte Daten zuzugreifen, kann der RACF-Administrator den Grund dafür erfragen. Es kann sein, daß der Benutzer die Informationen für die Erledigung seiner Aufgaben benötigt. Der Sicherheitsadministrator kann die Berechtigung des Benutzers so ändern, daß sie seinen Erfordernissen entsprechen.

Eine Vielzahl der Anwendungen / Systeme des Großrechners können so installiert werden, dass ein "external security manager" eingesetzt wird. Dies bedeutet, dass Sicherheitsabfragen bei Zugriffen auf Ressourcen durch ein externes Sicherheitssystem wie RACF bearbeitet werden.

Die drei Basisfunktionen von RACF sind:

Benutzeridentifizierung und Authentifizierung,
Zugriffs- bzw. Benutzerkontrolle und Protokollierung.

Standardmäßig geht RACF von dem Prinzip "Erlaubt ist, was nicht verboten wird" aus. Bei geeigneter Konfiguration kann aber weitgehend das datenschutzgerechtere Prinzip "Verboten ist, was nicht ausdrücklich erlaubt wird" realisiert werden.

Die für verschiedene Sicherheitsfunktionen notwendigen Daten und Informationen werden in RACF-Profilen in einer oder mehreren speziellen Datenbanken, den RACF-Databases gespeichert. Aus diesen Profilen können Informationen über die Benutzer als auch über die geschützten Ressourcen wie Plattendateien, Bänder, Datenstationen, Transaktionen usw. entnommen werden.

Die Benutzerprofile beschreiben die den Benutzern zugeordneten Rechte (Attribute); die Ressourcenprofile enthalten im wesentlichen die jeweiligen Zugriffs- bzw. Benutzungsregeln in Form einer Zugriffsliste.

RACF ist ein flexibles Werkzeug zum Aufbau und zur Erhaltung eines Sicherheitssystems und geht davon aus, dass in einer Installation eigene Zielvorstellungen für die Sicherheit aufgestellt werden, die dann unter Einsatz von RACF unter bestmöglicher Berücksichtigung der Installationsgegebenheiten realisiert werden.

Obwohl die Sicherheitsanforderungen von Installation zu Installation unterschiedlich sein können, sind bestimmte Rollen oder Aufgaben von RACF-Anwendern überall gleich. Allen Installatio-

nen ist gemeinsam, dass unterschiedliche Benutzer in verschiedenem Maße Verantwortung für die Sicherheit tragen oder auf die Ressourcen des Systems in unterschiedlicher Weise zugreifen müssen. Es gibt Personen, die sehr viel Sicherheitsverantwortung tragen, wohingegen andere nur wenige oder gar keine Verantwortung haben.

Manche Benutzer benötigen nahezu uneingeschränkte Zugriffsmöglichkeiten auf Ressourcen, wohingegen andere nur einen beschränkten Zugriff brauchen und wieder andere sogar von der Benutzung des Systems ausgeschlossen sein können.

Das Benutzerattribut bestimmt im RACF in erster Linie die Verantwortung eines Benutzers für die Sicherheit. Ein Benutzerattribut ist ganz einfach Teil der RACF-Definition, in der für die Installation festgelegt wird, was ein bestimmter Benutzer tun darf. Das Benutzerattribut SPECIAL wird zu Beispiel normalerweise dem Sicherheitsadministrator zugeordnet. Ein Benutzer mit dem Attribut SPECIAL kann sämtliche RACF-Funktionen mit Ausnahme derer, die einem Benutzer mit dem Benutzerattribut AUDITOR vorbehalten sind, ausführen.

Das Benutzerattribut OPERATIONS wird zum Beispiel normalerweise den Mitarbeitern zu Verfügung gestellt, die die Produktionsabläufe starten oder die die Verwaltung über die Platten durchführen. Das Benutzerattribut OPERATIONS erlaubt dem Benutzer Lese-, Änderungs- und Lösch-Zugriffe auf alle mit OPERATIONS=Yes gekennzeichneten Ressource-Klassen und deren Ressourcen ohne das von RACF weitere Prüfungen durchgeführt werden.

Die Trennung der Funktionen im RACF ist dringend notwendig, denn es ist die Aufgabe des Sicherheitsadministrators, RACF-Kontrollen einzurichten, wohingegen der Auditor dafür Sorge tragen muß, dass diese Kontrollen auch angemessen und effektiv sind.

Mit der Umsetzung der Revisionsziele sollen die Kunden/ Vertragspartner und Mitarbeiter des Unternehmens Vertrauen in die korrekte und zuverlässige Implementierung und Wirksamkeit der IT-Sicherheitsmaßnahmen gewinnen. Die Kunden/Vertragspartner und Mitarbeiter des Unternehmens sollen die Überzeugung gewinnen, daß ihre materiellen und ideellen Interessen unter Beachtung der Angemessenheit optimal durch die ausgewählten IT-Sicherheitsmaßnahmen des Unternehmens gewürdigt werden. Die Qualität der Dienstleistung IT-Sicherheit soll zu einem Wettbewerbsfaktor werden.

Die Ziele der Revision müssen den externen und internen Vorgaben genügen und Konformität zu den gesellschaftlichen und betrieblichen Zielen herstellen.

Zu diesen Zielen gehören:

- Gewährleistung der Nachvollziehbarkeit aller Geschäftsvorfälle
- Festlegung der Anforderung bezüglich Nachvollziehbarkeit und Beweispflicht
- Lückenlose Ermittlung und Erzeugung von Daten zur Nachvollziehbarkeit
- Sichere Aufbewahrung der beweisrelevanten Informationen

Zudem ist die Revision Ansprechpartner, wenn die Sicherheit als Schutz der Kunden/Vertragspartner und Mitarbeiter durch folgende Maßnahmen erfüllt werden soll:

- Festlegung von Sicherungsverfahren
- Schutz der Kunden/Vertragspartner und Mitarbeiter vor ungerechtfertigter Verdächtigung
- Vermeidung von Interessenskonflikten für Mitarbeiter durch geeignete organisatorische und technische Maßnahmen
- Vermeidung missbräuchlicher Nutzung von Geschäftsvorfällen
- und zugehörigen Prozessen durch Kunden/Vertragspartner oder Mitarbeiter

Schutz der Geschäftsvorfälle, zugehöriger Prozesse und Ressourcen, insbesondere die

- Gewährleistung der Vertraulichkeit
- Gewährleistung der Integrität
- Gewährleistung der Verfügbarkeit

- Zugriffs-/Zugangskontrollen zu Ressourcen
- Identifikation aller Benutzer und Subjekte
- Authentisierung aller Benutzer und Subjekte

Einhaltung von Konventionen und Regeln durch

- Fortschreibung und Anpassung der zugehörigen Konventionen und Regeln
- Regelmäßiger Nachweis und Dokumentation der Einhaltung von Konventionen und Regeln

Die Ziele der Revision stellen einen integralen Bestandteil der Geschäftspolitik dar. Sie helfen dabei, die Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit der Geschäftsprozesse durchzusetzen und die Sensibilität und Akzeptanz der Betroffenen zu fördern.

Gegenstand eines Revisonsauftrages RACF ist u.a. das Vertrauen von Kunden/Vertragspartnern und Mitarbeitern zu gewinnen und die IT-Sicherheitsziele zu erreichen, die an einem Geschäftsvorfall direkt oder auch indirekt beteiligten Benutzer und Ressourcen zu schützen und zu sichern. Die für die Durchführung der Geschäftsvorfälle unmittelbar bzw. unmittelbar erforderlichen Prozesse müssen nicht in ihrer Gesamtheit Gegenstand der Revision sein. Zugrunde gelegt werden insbesondere die Prozesse, die für die Ziele der Nachvollziehbarkeit der Geschäftsvorfälle, der Sicherheit der Interessen von Kunden/Vertragspartner und Mitarbeitern und des Schutzes der Prozesse und Ressourcen maßgeblich sind. Die für diese Prozesse identifizierbaren sicherheitsrelevanten Ereignisse sind Gegenstand der Revision.

Die Ergebnisse der Revision müssen auch in Bezug zu den geplanten bzw. umgesetzen IT Sicherheitszielen und -maßnahmen gestellt werden. Insofern überwacht die Revision auch regelmäßig die Umsetzung der IT Sicherheitsziele und -maßnahmen und deren Wirksamkeit im Rahmen eines Soll - Ist Vergleiches.

Um sich als Revisor ein Bild über den Ist-Zustand von RACF machen zu können sollten folgende Hilfsmittel vorhanden sein:

- TSO Terminal mit Zugang zu den zu untersuchenden Systemen und Anwendungen
- RACF-Benutzerkennzeichen mit normaler Berechtigung
- RACF-Benutzerkennzeichen mit System-Auditor Berechtigung
- Lesezugriff auf die Systemdateien (z.B. SYS1.RACF)
- Zugriff auf die Protokollierungedaten (SMF) der vergangenen Monate

Sofern vorhanden sollten die Dienstanweisungen / Arbeitsanweisungen für die Administration und für alle weiteren Benutzer vorhanden sein

- Übersicht über die eingesetzten Geräte des Rechnersystems.
- Übersicht über die eingesetzte Software

Im Rahmen des Revisionsauftrages sind folgende Aktivitäten Gegenstand der Prüfung:

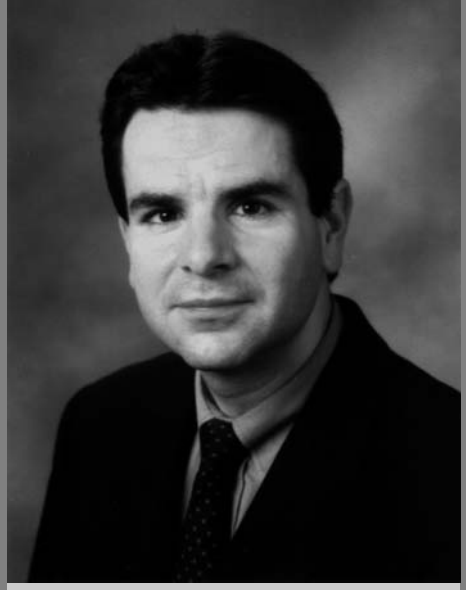
- Zugangsschutz / Nutzung der IT-Systeme
- Schützenswerte Ressourcen der IT
- Konventionen und Regeln zur IT Sicherheit
- Sicherheitsrelevante Ereignisse
- Umsetzung der IT Sicherheitsziele und - maßnahmen
- Interne Schnittstellen des Auditing
- Betriebsrat
- Datenschutzbeauftragter
- Revision
- Administration der Benutzer, Ressourcen und Berechtigungen
- IT Sicherheitsmanagement
- Personalverwaltung
- Verwaltung

Folgende Voraussetzungen, sofern vorhanden, erleichtern dem Prüfer die Untersuchung:

- Einsatz eines effektives Auditing
- Kompetenzregelung und ausreichende technische/personelle Ausstattung
- Dokumentation des IT Sicherheitskonzeptes
- Kategorisierung der IT Ressourcen in "Schutzklassen"
- Kategorisierung Benutzer in "Schutzklassen"
- Melde-/Alarmverfahren für ausgewählte sicherheitsrelevante Ereignisse
- Sicherung aller für das Auditing eingesetzten Programme und Systeme
- Protokollierung der sicherheitsrelevanten Ereignisse
- Sicherung aller für das Auditing erzeugten Informationen und Daten ✤

➲ IT-Prüfung von SAP R/3® im kommunalen Bereich

Die Einführung von SAP R/3 in Verbindung mit der Branchenlösung für den öffentlichen Sektor IS-PS (Industry Solution - Public Sector) stellt kommunale Prüfungseinrichtungen vor neue Herausforderungen. Die Besonderheit von SAP R/3 IS-PS besteht in der parallelen Abbildung der kameralistischen Buchführung der öffentlichen Verwaltungen und der kaufmännischen Buchführung.



Dr. Ralf Daum,
Abteilungsleiter Technische und IT-Prüfung,
Rechnungsprüfungsamt der Stadt Mannheim

Rechtliche Grundlagen und Aufgaben der IT-Prüfung

Die rechtlichen Grundlagen und Aufgaben der IT-Prüfung auf kommunaler Ebene ergeben sich aus der Gemeindeordnung, der Gemeindeprüfungsordnung und der Gemeindekassenverordnung der jeweiligen Bundesländer. Auf das Handels- und Steuerrecht wird nur zurückgegriffen, wenn das Haushalts- und Kassenrecht Begriffe (z.B. Ordnungsmäßigkeit) nicht weiter erläutert. Für den Bereich der finanzwirksamen Verfahren in Kommunalverwaltungen gibt es aber keinen Rechtfertigungsgrund von handels- und steuerrechtlichen Bestimmungen, z.B. Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), abzuweichen. Kommunale Prüfungseinrichtungen sollten sich deshalb bei IT-Prüfungen von diesen Grundsätzen leiten lassen.

Zu den so genannten Pflichtaufgaben eines Rechnungsprüfungs- bzw. Revisionsamtes im Bereich der IT-Prüfung gehören die Programmprüfung und die Anwendungsprüfung. Bei der Programmprüfung ist festzustellen, ob Programme für automatisierte Verfahren zur Abwicklung von Vorgängen

- der Haushalts-, Kassen- und Rechnungsführung,
- der Wirtschaftsführung und des Rechnungswesens sowie
- der Vermögensverwaltung

eine ordnungsgemäße Abwicklung gewährleisten. Die Anwendungsprüfung als Teil der sachlichen Prüfung untersucht bei automatisierten Verfahren des Finanzwesens beispielsweise, ob die eingesetzten Programme gültig, dokumentiert und freigegeben sowie gegen unbefugte Eingriffe hinreichend gesichert sind. Diese pauschale Abgrenzung der Prüfungsbereiche zwischen Programm- und Anwendungsprüfung greift bei SAP R/3 nicht mehr. Vor allem wegen des Einflusses von Customizing-Einstellungen und Parametereinstellungen auf den Programmablauf berührt nahezu jede IT-Prüfung (z.B. Berechtigungs- und Systemprüfung) sowohl Aspekte der Programmprüfung als auch Aspekte der Anwendungsprüfung.

Herausforderungen für kommunale Prüfungseinrichtungen

Die Einführung von SAP R/3 in Verbindung mit der Branchenlösung für den öffentlichen Sektor IS-PS (Industry Solution -

Public Sector) stellt kommunale Prüfungseinrichtungen vor neue Herausforderungen. Die Besonderheit von SAP R/3 IS-PS besteht in der parallelen Abbildung der kameralistischen Buchführung der öffentlichen Verwaltungen und der kaufmännischen Buchführung. Während Buchungen weiterhin kameralistisch erfolgen, läuft im Hintergrund die doppelte Buchführung mit. Das bedeutet, dass ständig ein Abgleich zwischen beiden Bereichen stattfinden muss. Neben dieser grundsätzlichen Neuerung, erhöht die Flexibilität von SAP R/3 (z.B. anwenderbezogene Konfiguration des SAP R/3-Systems durch Customizing) die Komplexität der Prüfungsmaterie und führt zu einer Zunahme des Prüfungs- und Kontrollaufwandes. Gleichzeitig können bewährte Prüfungsansätze (z.B. Unterscheidung in Programm- und Anwendungsprüfung) auf SAP R/3 nicht übertragen werden.

Den meisten Kommunen fehlen zumindest in der Anfangszeit detaillierte Kenntnisse und umfangreiche Erfahrungen mit SAP R/3 sowohl aus Anwender- als auch aus Prüfungssicht. Außerdem kommt hinzu, dass die von SAP zur Verfügung gestellten Hilfsmittel, z.B. Sicherheitsleitfaden, verschiedene Reports oder das Audit Information System, für umfassende SAP R/3-Prüfungen in vielen Fällen nicht ausreichen. Häufig sind prüfungsrelevante Auswertungen bzgl. der Gebiete Systemsicherheit und Berechtigungskonzept u.a. wegen des großen Datenvolumens überhaupt nicht oder nur mit erheblichen Prüfungsaufwand möglich. Im Gegensatz zu der klassischen Haushalts- und Finanzsoftware, die Kommunen bisher einsetzten, unterliegt ein SAP R/3-System fortwährend Änderungen. Regelmäßig kommen erweiterte oder neue Funktionalitäten hinzu. Ständig arbeiten neue Mitarbeiter mit SAP R/3, wechseln den Aufgabenbereich oder scheiden aus. Die Beurteilung, welche Berechtigungen nach dem Prinzip der minimalen Berechtigungen und unter Berücksichtigung der Funktionstrennung die Benutzer benötigen, erweist sich als äußerst komplex. Bei Prüfungshandlungen ist in der Regel eine genaue Abgrenzung des Prüfungsumfangs erforderlich, was grundsätzliche Aussage zu Ordnungsmäßigkeit und Sicherheit des Systems erschwert.

Lösungsansatz der Stadt Mannheim

Neben intensiven Schulungen der IT-Prüfer begegnete die Stadt Mannheim diesen Revisionsherausforderungen insbesondere mit zwei Maßnahmen:

- Einrichtung der Arbeitgruppe "Systemsicherheit"
- Beschaffung einer Software für die System- und Berechtigungsprüfung

Die Arbeitgruppe "Systemsicherheit" beschäftigt sich mit kritischen Systemeinstellungen in SAP R/3 (z.B. Tabellenprotokollierung) und kritischen Berechtigungen (z.B. elektronisches Radieren) ausgewählter Benutzergruppen. Ihr gehören Vertreter des Fachbereiches Informationstechnologie, des Outsourcing-Partners (Rechenzentrum), der Stadtkämmerei (zuständig für den Haushalt sowie die Finanz- und Wirtschaftsverwaltung einer Kommune) und des Rechnungsprüfungsamtes an. Die Aufgabe der Arbeitsgruppe besteht in der Erarbeitung von Empfehlungen für den Umgang mit dem SAP R/3-System, die sowohl Revisionsgesichtspunkte (z.B. Ordnungsmäßigkeit, Rechtmäßigkeit und Sicherheit) als auch Praktikabilität und notwendige Flexibilität berücksichtigen. Bisher hat die Arbeitsgruppe die Einstellung mehrerer Systemparameter, Verfahren für die Protokollierung mit dem Security Audit Log, den Umgang mit ausgewählten kritischen Berechtigungen usw. festgelegt. Beispielsweise wurden verschiedene kritische Berechtigungen in einer eigenen Rolle zusammengefasst, die ein Benutzer nur in besonderen Situationen zeitweise erhält. Während dieser Zeit wird der Security Audit Log für diesen Benutzer aktiviert. Die in der Arbeitgruppe getroffenen Regelungen dienen als eine Art "Leitfaden" für den Umgang mit kritischen Berechtigungen und Systemeinstellungen in allen produktiven SAP R/3-Systemen der Stadt Mannheim.

Der Einsatz einer Software für die System- und Berechtigungsprüfung soll einerseits mit den

vorhandenen personellen Ressourcen des Rechnungsprüfungsamtes eine effiziente, effektive und qualitativ hochwertige Prüfung von SAP R/3 ermöglichen. Dabei geht es nicht nur um eine wirtschaftliche und aussagekräftige Durchführung von Prüfungshandlungen, sondern auch um das in der Software hinterlegte Prüfer- und Beraterwissen bzgl. SAP R/3 (z.B. Umsetzung von Gesetzesmäßigkeiten und Ordnungsmäßigkeitsvorgaben). Anderseits soll die Software auch die für die Systemadministration und Berechtigungsverwaltung zuständigen Dienststellen unterstützen. Deshalb wurden an der Auswahl der Software alle betroffenen Dienststellen (Fachbereich Informationstechnologie, Stadtkämmerei und Rechnungsprüfungsamt) in Form einer Projektgruppe beteiligt. Diese Projektgruppe hat unterschiedliche Informationsquellen (Fachzeitschriften, Internetrecherchen sowie Gespräche mit Revisoren und Wirtschaftprüfern) ausgewertet, gemeinsam einen Kriterienkatalog für die Auswahl der Software erstellt und diesen an sieben Anbieter von Prüfsoftware verschickt. Drei Produkte kamen in die engere Wahl, aber nur die Software CheckAud® for SAP R/3 der IBS Schreiber GmbH wurde den Anforderungen der Stadt Mannheim gerecht und schließlich auch beschafft.

Wirksamkeit der Software

Die Software erhöht wesentlich die Effizienz der Aufgabenerfüllung. CheckAud® for SAP R/3 enthält über 1000 vorgegebene kritische Berechtigungen, die das System automatisiert überprüft. Das Programm ermöglicht, eigene für die Stadtverwaltung Mannheim kritische Berechtigungen zu definieren und in die automatische Prüfung zu übernehmen. Durch diese Funktionalität können auch Besonderheiten der Branchenlösung für den öffentlichen Sektor, z.B. in Bezug auf die kameralistische Buchführung, abgedeckt werden. Bei jeder Aufnahme des SAP R/3-Systems handelt es sich um eine Vollerhebung, die alle Berechtigungen zum Aufnahmezeitpunkt abbildet. Verschiedene Dienststellen nutzen diese Funktionalität als Basis für die Dokumentation des Berechtigungskonzeptes.

Voll- und halbautomatisierte Analysewerkzeuge erleichtern die Auswertung der Daten. Die Prüfungen der beteiligten Dienststellen haben erwiesen, dass CheckAud® for SAP R/3 den Prüfungsaufwand erheblich reduziert. So konnte zum Beispiel bei der Erstprüfung des Mannheimer SAP R/3-Systems (500 Benutzer) der Prüfungszeitraum von ca. 15 Tagen auf zwei Tage verkürzt werden, weil die aufwendige Erhebung der benötigten Daten durch manuelle Abfragen im SAP R/3-System entfallen ist. Die kurze Prüfungsdauer gestattet eine zeitnahe Reaktion auf Schwachstellen. Kritische Prüfungsfeststellungen werden bei der Stadt Mannheim umgehend in der Arbeitsgruppe "Systemsicherheit" besprochen und die dort erarbeiteten Lösungsvorschläge schnellstens im SAP R/3-System umgesetzt. Darüber hinaus steigert CheckAud® for SAP R/3 die Prüfungsqualität in Hinblick auf Ordnungsmäßigkeit, Rechtmäßigkeit und Sicherheit. Die Software erlaubt prüfungsrelevante Auswertungen in Bezug auf Berechtigungen und Systemsicherheit, die mit herkömmlichen in SAP R/3 zur Verfügung stehenden Hilfsmitteln überhaupt nicht möglich wären.

Nutzung von CheckAud® for SAP R/3 für die Risikofrüherkennung

Die Gemeindekassenverordnung stellt zahlreiche Anforderungen an automatisierte Verfahren im kommunalen Kassenwesen (z.B. Gewährleistung von Vollständigkeit und Richtigkeit der Daten, Vorkehrungen gegen unbefugtes Eingreifen, Datensicherheit). Verstöße gegen diese gesetzlichen Auflagen sind in SAP R/3 auf vielfältige Weise, z.B. durch Änderung von Zugriffsrechten, möglich. Die Prüfung der Einhaltung dieser Vorgaben ist deshalb kein einmaliger Vorgang. Vielmehr müssen ständige Kontrollen im Rahmen eines Risikofrüherkennungssystems sicherstellen, dass die Vorgaben nicht umgangen werden können. Diese Kontrollen sollen einerseits präventiv wirken und im Vorfeld zu einer Fehlervermeidung füh-

ren. Andererseits sollen sie auch bereits aufgetretene Fehler entdecken.

Die Stadtkämmerei, der Fachbereich Informationstechnologie und das Rechnungsprüfungsamt erstellen gemeinsam ein solches Risikofrüherkennungssystem für das SAP R/3-System der Stadt Mannheim auf der Basis von CheckAud® for SAP R/3. Als Teil des Internen Kontrollsystems soll das Risikofrüherkennungssystem in regelmäßigen Abständen (z.B. monatlich) verschiedene kritische Berechtigungen und Systemeinstellungen prüfen, um möglichst frühzeitig potenziellen Verletzungen von Ordnungsmäßigkeit, Rechtmäßigkeit und Sicherheit entgegenzuwirken. Diese Zusammenstellung von Abfragen wird regelmäßig durch das Rechnungsprüfungsamt in Form von benutzerdefinierten Analysebäumen für CheckAud® for SAP R/3 hinterlegt und allen betroffenen Dienststellen für voll- und halbautomatisierte Prüfungen zur Verfügung gestellt. Die automatisierten Prüfungsmöglichkeiten mit CheckAud® for SAP R/3 reduzieren den für die Risikofrüherkennung benötigten Personalbedarf erheblich. Durch das Ampelsystem von CheckAud® for SAP R/3, das Prüfungsfeststellung entsprechend des Gefahrenlevels hervorhebt, ergibt sich nur bei kritischen Situationen Handlungsbedarf. Neben den regelmäßigen Prüfungen finden auch nach umfangreichen Änderungen im System, z.B. neue oder geänderte Rollen bzw. Rollenzuweisungen, Analysen mit CheckAud® for SAP R/3 statt, um eventuell auftretende Berechtigungsprobleme frühzeitig zu erkennen. Jede Aufnahme steht über ein gemeinsames Laufwerk allen an der Risikofrüherkennung beteiligten Dienststellen für eigene Auswertungen zur Verfügung. Dadurch können auch jederzeit verschiedene Aufnahmen miteinander verglichen werden. Die dadurch möglichen Kontrollen durch Soll-Ist-Vergleiche vermindern ebenfalls die Wahrscheinlichkeit für das Auftreten von Fehlern bzw. erhöhen die Wahrscheinlichkeit vorhandene Fehler aufzudecken.

fungsinstanz liegen, sondern muss in der gesamten Organisation gelebt werden. Dazu bedarf es Regelungen, die sowohl den Ansprüchen der Praktikabilität im laufenden Betrieb als auch der Sicherheit genügen. Die Stadt Mannheim hat dazu organisatorische und systemtechnische Maßnahmen miteinander kombiniert. In der AG Systemsicherheit treffen unterschiedliche Sichtweisen auf das SAP R/3-System aufeinander. Basierend auf dem gemeinsamen Einsatz von CheckAud® for SAP R/3 findet ein Erfahrungsaustausch über kritische Einstellungen im System statt. Prüferinnen und Prüfer

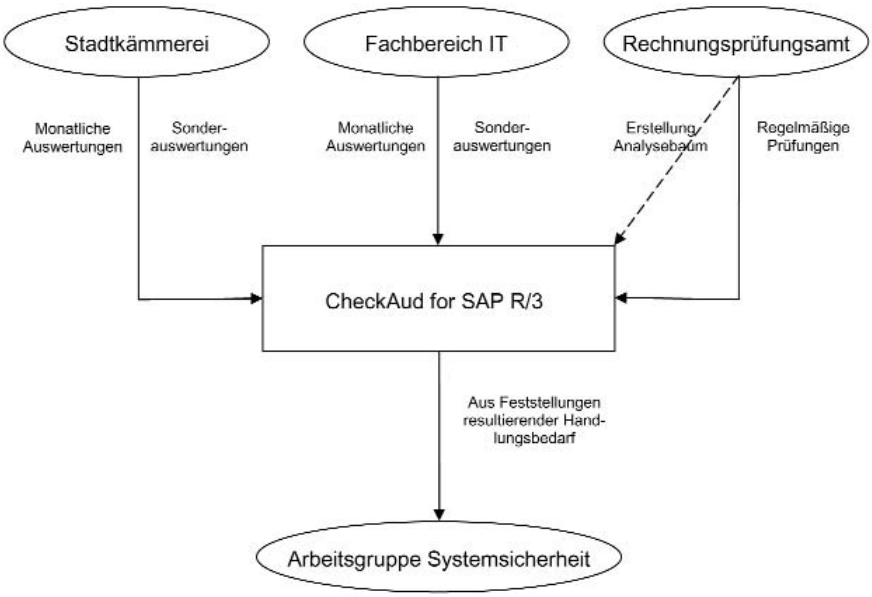


Abb.: Risikofrüherkennung bei der Stadt Mannheim

Zusammenfassung

Der Umfang und die Vielschichtigkeit eines SAP R/3-System verlangen einen ganzheitlichen Prüfungsansatz. Das Thema Sicherheit darf dabei nicht in alleiniger Zuständigkeit der Prü-

bleiben über aktuelle Entwicklungen und Problemstellungen im SAP R/3-System auf dem Laufenden, System- und Berechtigungsadministratoren beziehen durch die Diskussionen im Arbeitskreis frühzeitig Sicherheitsfragen in ihre Überlegungen mit

ein. CheckAud® for SAP R/3 hat sich als wertvolles Werkzeug für vielseitige und zeitnahe SAP R/3-Prüfungen erwiesen. Außerdem hat die Nutzung der Software in mehreren Bereichen dazu beigetragen, dass die Sensibilität für Risiken bei der Informationsverarbeitung mit SAP R/3 (z.B. Manipulation, unberechtigte Einblicke oder unbeabsichtigte Eingriffe) wesentlich gestiegen ist. ✤

➲ CheckAud® for SAP R/3® 2.8 - Auswertung von Zugriffsrechten auf Geschäftsprozesse

Thomas Tiede,
Geschäftsführer
IBS Schreiber GmbH,
Hamburg

Die Anforderungen an die Sicherheit von ERP-Systemen wachsen in zunehmenden Maße. Durch die Gesetzgebung werden vermehrt Kontrollmechanismen gefordert, die Gesetzesverstöße und dolose Handlungen verhindern sollen. Als erstes einschneidendes Gesetz fordert z.B. der Sarbanes-Oxley-Act in der Section 404 die Implementierung eines internen Kontrollsystems, dessen Wirksamkeit vom CEO und CFO sowie von den Abschlussprüfern bestätigt werden muss.

In den ERP-Systemen sind daher entsprechende Kontrollmechanismen zu integrieren. Ein wesentliches Kontrollinstrument stellen hier natürlich die Zugriffsrechte dar. Durch die Implementierung von Funktionstrennungen innerhalb von Prozessabläufen kann eine wirksame Absicherung erreicht werden.

Voraussetzung hierfür ist eine transparente Abbildung der Geschäftsprozesse im ERP-System. Im Zuge der Umsetzung der Sarbanes-Oxley-Anforderungen stellt dies einen der ersten Schritte dar. Hierfür können Tools wie z.B. das SAP MIC (Management of internal control) genutzt werden. Sollen innerhalb dieser Prozesse nun Funktionstrennungen implementiert werden, so bedeutet dies für SAP R/3®, dass zu den einzelnen Prozessschritten die genutzten Transaktionen ermittelt werden müssen, damit Rechte hierfür dann getrennt zugeordnet werden können. Hieraus lässt sich dann wiederum eine Kontrollmatrix ableiten, in der dargestellt ist, welche Transaktionen nicht in Kombination vergeben werden dürfen. Oder: Welche Zugriffsrechte in Kombination gegen das interne Kontrollsystem verstoßen.

Als Vorgehensweise zur Erstellung solch einer Kontrollmatrix können als Ausgangspunkt die genutzten Prozesse verwendet werden. Den einzelnen Prozessschritten werden die in SAP R/3® genutzten Transaktionen zugeordnet. Tabelle 1 zeigt stark vereinfacht den Warenbeschaffungsprozess mit den zugehörigen Transaktionen.

Prozess	**Transaktion**
Bestellanforderungen anlegen	ME51N Anlegen
Bestellanforderungen freigeben	ME54 Einzelfreigabe ME55 Sammelfreigabe
Bestellung anlegen	ME21N Anlegen
Bestellung freigeben	ME28 Freigeben
Wareneingang buchen	MIGO Warenbewegungen
Rechnung buchen (über Logistik Rechnungsprüfung)	MIRO Rechnung erfassen
Zahllauf starten	F110 Zahllauf

Tabelle 1: Warenbeschaffungsprozess mit zugehörigen Transaktionen

Im nächsten Schritt ist hier anhand des internen Kontrollsystems zu definieren, wo innerhalb dieser Prozesskette Funktionstrennungen einzuhalten sind (Tabelle 2).

Aktion	Darf nicht vergeben werden mit
Bestellanforderung anlegen ME51N	Bestellanforderung freigeben ME54
Bestellanforderung anlegen ME51N	Bestellanforderung freigeben ME55
Bestellanforderungen anlegen ME51N	Bestellung anlegen ME21N
Bestellung anlegen ME21N	Bestellung freigeben ME28
Bestellung anlegen ME21N	Wareneingang buchen MIGO
Wareneingang buchen MIGO	Rechnung buchen MIRO
Bestellung anlegen ME21N	Rechnung buchen MIRO
Rechnung buchen MIRO	Zahllauf starten

Tabelle 2: Definition der Funktionstrennungen im Warenbeschaffungsprozess

Die so definierte Matrix stellt nun den Ausgangspunkt für die Rechtevergabe gemäß dem internen Kontrollsystem dar. Es ist nun sicherzustellen, dass diese Kombinationen keinem Benutzer zugeordnet werden. Um dieser Anforderung gerecht zu werden bietet CheckAud® for SAP R/3® die Möglichkeit, solch eine Matrix zu importieren, evtl. anzupassen und automatisiert zu überprüfen.

Voraussetzung ist die Abbildung dieser Vorgaben in einer tabellarischen Form, z.B. in MS Excel. Hier werden zeilenweise die Transaktionen angegeben, die nicht in Kombination vergeben werden dürfen. Die Anzahl der Transaktionen ist hierbei nicht begrenzt. Es ist daher auch möglich, 20 Transaktionen oder mehr in Kombination zu überprüfen.

Abb. 1 zeigt die Umsetzung der in Tabelle 2 aufgelisteten Funktionstrennungen (Zeile 1 - 8). In den Zeilen 9 - 11 wurden zusätzlich komplexere Kombinationen hinterlegt um überprüfen zu können, ob Benutzer große Teile des Prozesses oder den gesamten Prozess ausführen können.

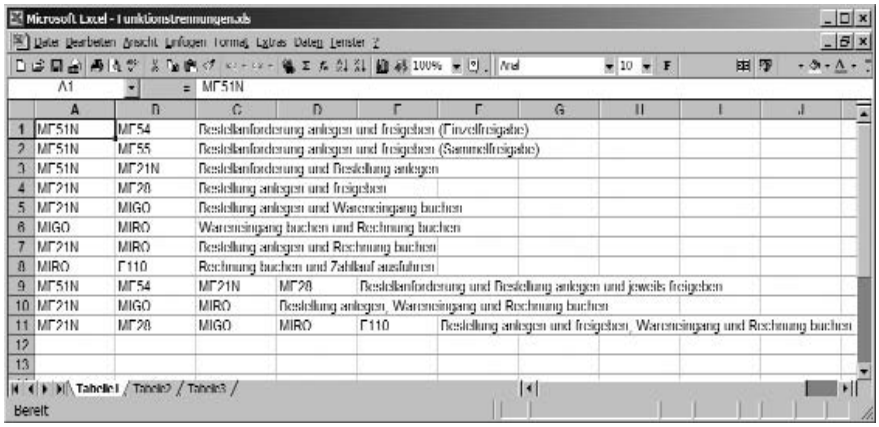


Abb. 1: Definition der Funktionstrennungen in MS Excel

Diese Datei kann nun direkt in CheckAud® for SAP R/3® importiert werden. Beim Import (Abb. 2) kann noch definiert werden, ob die Datei nur die Folgen von Transaktionen enthält, oder ob pro Zeile noch jeweils eine Beschreibung hinterlegt ist, wie in Abb. 1.

Abb. 2: Import der Transaktionsmatrix in CheckAud® for SAP R/3®

Beim Import liest CheckAud® for SAP R/3® nun diese Datei zeilenweise aus. Zu den einzelnen Transaktionen werden die jeweils dazugehörigen Berechtigungsobjekte ermittelt. Die Transaktionen werden dann mit einem logischen UND verknüpft, und es wird pro Zeile eine Berechtigung erstellt. Diese Berechtigungen werden in einem neuen Analysebaum dargestellt (siehe Abb. 3).

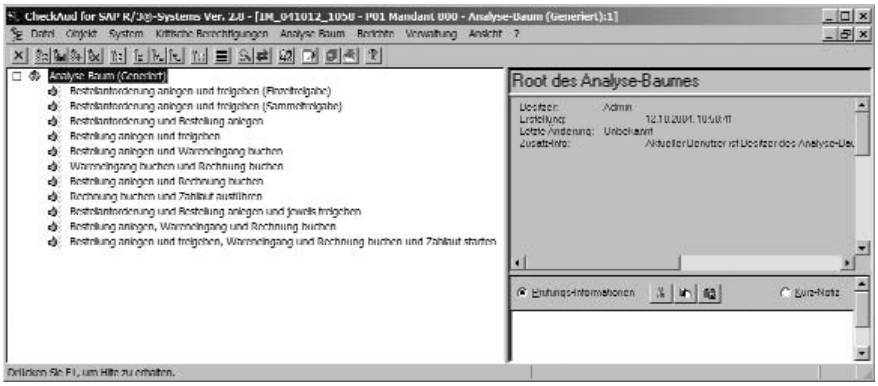


Abb. 3: Importierte Transaktionsmatrix in CheckAud® for SAP R/3®

Gerade in größeren Unternehmungen sind komplexe Geschäftsprozesse nicht in einem einzigen R/3-System abgebildet, sondern in mehreren Systemen. Häufig ist z.B. ein Logistik-System vom Finanzbuchhaltungssystem getrennt. In dem Fall muss die Matrix des internen Kontrollsystems um das System bzw. den Mandanten der jeweiligen Aktion erweitert werden. In Tabelle 3 ist z.B. aufgezeigt, das der Zahllauf in der letzten Zeile im System P02 stattfindet, der eigentliche Warenbeschaffungsprozess aber in P01. Hier sind die Zugriffsrecht somit system- und mandantenübergreifend auszuwerten.

Aktion	System	Darf nicht vergeben werden mit	System
Bestellanforderung anlegen ME51N	P01	Bestellanforderung freigeben ME54	P01
Bestellanforderung anlegen ME51N	P01	Bestellanforderung freigeben ME55	P01
Bestellanforderungen anlegen ME51N	P01	Bestellung anlegen ME21N	P01
Bestellung anlegen ME21N	P01	Bestellung freigeben ME28	P01
Bestellung anlegen ME21N	P01	Wareneingang buchen MIGO	P01
Wareneingang buchen MIGO	P01	Rechnung buchen MIRO	P01
Bestellung anlegen ME21N	P01	Rechnung buchen MIRO	P01
Rechnung buchen MIRO	P01	Zahllauf starten F110	P02

Tabelle 3: Definition der Funktionstrennungen über Systemgrenzen hinweg

In der Entwurfsansicht in Abb. 4 ist zu erkennen, dass zu den einzelnen Transaktionen auch die zugehörigen Berechtigungsobjekte ermittelt wurden. Organisationselemente wie Werke oder Buchungskreise sind nicht fest definiert. Diese werden erst beim Auswerten der Berechtigung abgefragt. Natürlich können auch hier die Standardfunktionalitäten genutzt werden, wie z.B. die automatische Analyse aller Berechtigungen. Diese Funktionalität gestattet daher auf einfachste Weise eine vollständige Überprüfung der Vorgaben des internen Kontrollsystems.

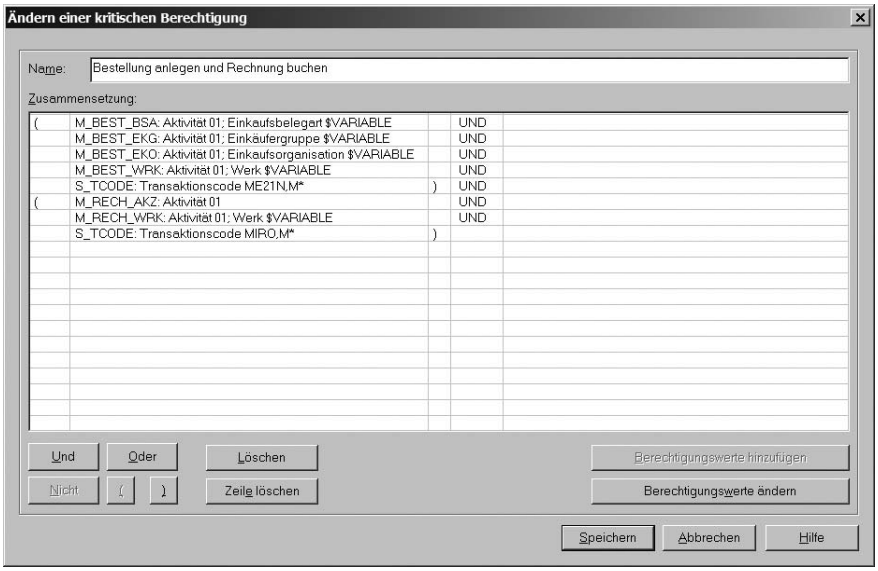


Abb. 4: Entwurfsansicht einer Berechtigung in CheckAud® for SAP R/3®

In dem Fall sind die Vorgaben um die Informationen System und Mandant zu erweitern. CheckAud® for SAP R/3® bietet hier die Möglichkeit, bereits bei der Definition der Matrix Ordnerstrukturen zu definieren,

in denen die Berechtigungen dann innerhalb eines Baumes abgelegt werden. Abb. 5 zeigt die Definition der Prozesse. Vor den einzelnen Transaktionen ist jeweils auch das System und der Mandant anzugeben. Hier sind dann auch sehr viel komplexere Möglichkeiten gegeben als bei der Transaktionsmatrix zuvor. Transaktionen, die zeilenweise hintereinander angegeben werden, werden mit einem logischen ODER verknüpft. Untereinanderstehende Transaktionen werden mit einem logischen UND verknüpft. Die Kombination

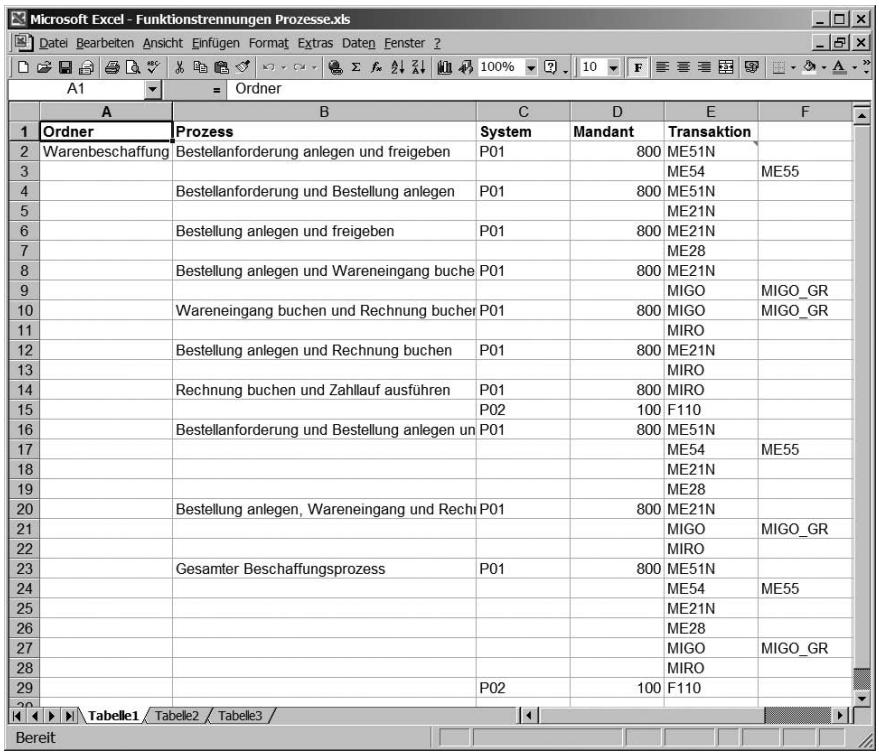
ME51N	
ME54	ME55
ME21N	
ME28	
MIGO	MIGO_GR
MIRO	
F110	

wird daher in CheckAud® for SAP R/3® folgendermaßen zusammengesetzt:

ME51N	UND
(ME54 ODER ME55)	UND
ME21N	UND
ME28	UND
(MIGO ODER MIGO_GR)	UND
MIRO	UND
F110	

Für den Fall, dass einzelne Prozessschritte in unterschiedlichen Systemen / Mandanten ausgeführt werden, kann hier für jede Zeile das betreffende System angegeben werden:

P01 Mandt. 800	ME51N	UND
P01 Mandt. 800	(ME54 ODER ME55)	UND
P01 Mandt. 800	ME21N	UND
P01 Mandt. 800	ME28	UND
P01 Mandt. 800	(MIGO ODER MIGO_GR)	UND
P01 Mandt. 800	MIRO	UND
P02 Mandt. 100	F110	



	A	B	C	D	E	F
1	Ordner	Prozess	System	Mandant	Transaktion	
2	Warenbeschaffung	Bestellanforderung anlegen und freigeben	P01	800	ME51N	
3					ME54	ME55
4		Bestellanforderung und Bestellung anlegen	P01	800	ME51N	
5					ME21N	
6		Bestellung anlegen und freigeben	P01	800	ME21N	
7					ME28	
8		Bestellung anlegen und Wareneingang buche	P01	800	ME21N	
9					MIGO	MIGO_GR
10		Wareneingang buchen und Rechnung bucher	P01	800	MIGO	MIGO_GR
11					MIRO	
12		Bestellung anlegen und Rechnung buchen	P01	800	ME21N	
13					MIRO	
14		Rechnung buchen und Zahllauf ausführen	P01	800	MIRO	
15			P02	100	F110	
16		Bestellanforderung und Bestellung anlegen un	P01	800	ME51N	
17					ME54	ME55
18					ME21N	
19					ME28	
20		Bestellung anlegen, Wareneingang und Rechi	P01	800	ME21N	
21					MIGO	MIGO_GR
22					MIRO	
23		Gesamter Beschaffungsprozess	P01	800	ME51N	
24					ME54	ME55
25					ME21N	
26					ME28	
27					MIGO	MIGO_GR
28					MIRO	
29			P02	100	F110	

Abb. 5: Definition systemübergreifender Prozesse für CheckAud® for SAP R/3®

Nach dem Import in CheckAud® werden diese Berechtigungskombinationen, genannt Prozesse, in einem separaten Baum dargestellt (Abb. 6). Dort werden unterhalb der Bezeichnung des Prozesses die Systeme angezeigt, in denen die Berechtigungen ausgewertet werden sollen. Unterhalb der Systeme werden die Berechtigungen aufgelistet. Jede Berechtigung stellt eine Zeile aus der Matrix dar. Die einzelnen Berechtigungen, in denen teilweise die Transaktionen mit ODER verknüpft sind, werden automatisch untereinander mit einem logischen UND ausgewertet.

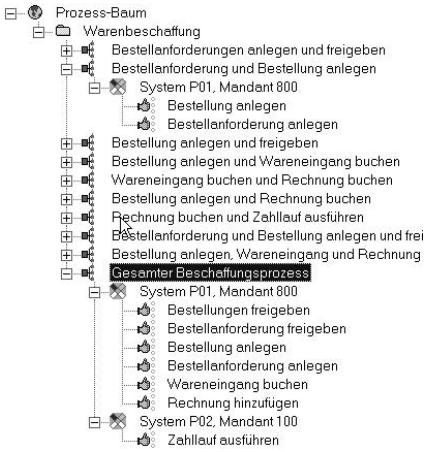


Abb. 6: Importierte Prozesse in CheckAud® for SAP R/3®

Ab sofort erhältlich

❑ **Titel: Ordnungsmäßigkeit und Prüfung des SAP R/3® Systems**
2. erweiterte und überarbeitete Auflage 2004

Autor: Thomas Tiede
ISBN: 3-930291-24-X
Seiten: 900
Preis: 64,90 €

Inhalt:

Das Buch "OPSAP - Ordnungsmäßigkeit und Prüfung des SAP R/3®-Systems" ist inzwischen zum Standardwerk für alle geworden, die sich mit dem Thema R/3®-Sicherheit befassen. Die 2. Auflage wurde nun angepasst an die R/3- Releasestände 4.6C und Enterprise. Alle Kapitel wurden neu überarbeitet und teilweise sehr umfassend ergänzt.

Viele neue Themen, die für eine Prüfung bzw. für ein Sicherheitskonzept unerlässlich sind, sind hinzugekommen (z.B. das Transportwesen). Wieder sind umfassende Checklisten enthalten zusammen mit den Hinweisen, wie jeder einzelne Punkt zu prüfen ist.

Bestell-Fax 040/69 69 85-31

Name: ..... PLZ/Ort: .....

Vorname: ..... Tel.: .....

Firma: ..... E-Mail: .....

Abteilung ..... Ort/Datum: .....

Straße: ..... Unterschrift .....

Ottokar Schreiber Verlag GmbH
Revision • Controlling • Informatik • PPP
Friedrich-Ebert-Damm 145
22047 Hamburg
Tel.: +49 40 69 69 85-14
Fax: +49 40 69 69 85-31
www.osv-hamburg.de
sales@osv-hamburg.de

Ab sofort erhältlich

❑ **Titel: Praxisleitfaden für SAP R/3® FI**

Autor: Marie-Luise Wagener
ISBN: 3-930291-25-8
Seiten: 600
Preis: 69,90 €

Inhalt:

Basierend auf den gesetzlichen Anforderungen befasst sich dieses Buch mit den Prüfungsanforderungen und deren Umsetzungen zur Einrichtung einer ordnungsmäßigen Finanzbuchhaltung in SAP R/3® Systemen. Resultierend aus den spezifischen Anforderungen des geprüften ERP Systems ist der Aufbau dieses Fachbuches maximal praktisch ausgerichtet. Sämtliche Prüfschritte sind ausführlich erläutert und werden durch referenzierende Checklisten ergänzt.

Neben den relevanten Prüfbereichen wie Organisationseinheiten, Kreditoren-, Debitoren- und Sachkontenbuchhaltung werden genauso die Verbuchungsprinzipien, die automatischen Abläufe, das Customizing, Maßnahmen zum Forensic Accounting und Monitoring behandelt.

Ein besonderer Schwerpunkt ist den speziellen Anforderungen zur Berechtigungskonzeption gewidmet. Zusammen mit erklärenden Ausführungen werden Sie durch dezidierte Handlungsanweisungen bei der direkten Verprobung am System unterstützt. Selbstverständlich ist auch die relevante Schnittstelle zur Materialwirtschaft integriert. Mit diesem Praxisleitfaden können Sie sämtliche Prüfungshandlungen selbstständig am SAP R/3® System durchführen.

Bestell-Fax 040/69 69 85-31

Name: ..... PLZ/Ort: .....

Vorname: ..... Tel.: .....

Firma: ..... E-Mail: .....

Abteilung ..... Ort/Datum: .....

Straße: ..... Unterschrift .....

Ottokar Schreiber Verlag GmbH
Revision • Controlling • Informatik • PPP
Friedrich-Ebert-Damm 145
22047 Hamburg
Tel.: +49 40 69 69 85-14
Fax: +49 40 69 69 85-31
www.osv-hamburg.de
sales@osv-hamburg.de

Bei der Auswertung eines Prozesses werden nun die Berechtigungen in den jeweiligen Systemen / Mandanten (welche vorher gescannt werden müssen) geprüft. Danach werden die Benutzer ermittelt, die in den Systemen die jeweiligen Berechtigungen besitzen. Diese werden als Ergebnismenge angezeigt (Abb. 7). Die Darstellung zu den Benutzern ist identisch zur herkömmlichen Darstellung. Auch hier wird zu jedem einzelnen Recht jeweils die Herkunft mit angezeigt.

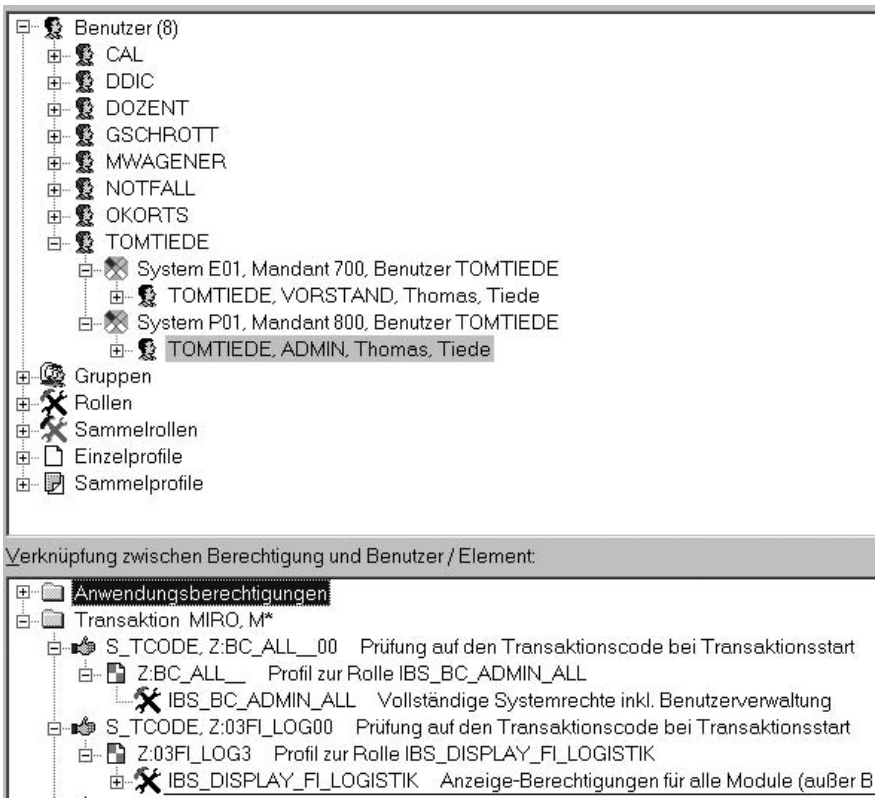


Abb. 7: Auswertung von Prozessen in CheckAud® for SAP R/3®

In einem Prozess in CheckAud® for SAP R/3® können beliebig viele Systeme / Mandanten mit zugehörigen Berechtigungen definiert werden. Die Prozesse können auch direkt in CheckAud® erstellt werden, ohne vorherige Definition in einer Tabelle. Die Einsatzmöglichkeiten sind dabei unbegrenzt. So ist diese Systematik auch anwendbar innerhalb einer einzigen Systemlandschaft, z.B. um zu ermitteln, wer im Entwicklungssystem entwickeln und Entwicklungen freigeben und diese dann ins QS- und Produktivsystem importieren darf. Unterschiedliche Benutzernamen in verschiedenen Systemen stellen kein Problem bei der Auswertung dar, da die Benutzer über Zuordnungslisten auch nach beliebigen Benutzereigenschaften (z.B. Vor- und Zuname) ermittelt werden können. Natürlich können auch existierende Benutzerzuordnungslisten importiert werden.

Mit der systemübergreifenden Prozessauswertung sind hier erstmalig Auswertungen möglich, die vorher nur mühselig und mit viel manueller Arbeit zu bewältigen waren waren. CheckAud® for SAP R/3® stellt mit der Prozessauswertung Wege zur Verfügung, das interne Kontrollsystem effektiv und umfassend zu überprüfen. Insbesondere die Überwachung des internen Kontrollsystems wird auch in der Entwicklung von CheckAud® in 2005 weiter beachtet. Folgende Features werden u.a. verwirklicht:

Dialoganbindung an SAP R/3 zur Nutzung der R/3-eigenen Auswertungsmöglichkeiten (Transaktionen, Reports, Tabellen) sowie zur Nutzung der CheckAud®-Funktionalität in Echtzeit am System

Berechtigungs-Monitoring (Warnmeldungen, wenn Rollenzuordnungen gegen die IKS-Matrix verstoßen)

Rollen-, Benutzer- und Arbeitsplatzsimulation (virtuelle Änderungen von Rollen bzw. Rollenzuordnungen und Abgleich mit der IKS-Matrix)

Automatisierung von Scan, Übertragung und Auswertung für vollautomatisierte Auditings: ✤

➲ Risikoorientierte Prüfungsplanung in kleinen Revisionsstäben - Anforderungen an eine Systematisierung

Christoph Wildensee,
Stadtwerke Hannover AG

Die ‚Risikoorientierte Prüfungsplanung' ist bereits seit geraumer Zeit ein wichtiger Teil der Betrachtung revisorischer Leistungserbringung, nicht zuletzt durch gesetzliche Anforderungen an eine Ausgestaltung interner Überwachungssysteme. Entsprechende Vorgaben aus Standards der Wirtschaftsprüfer und nationaler und internationaler Institutionen (ISACA, IIA, IIR) weisen hier konkretisierend den Weg (IDW PS 321/330/340, EPS 523, COBIT etc.).

Einführung

Insbesondere für Banken bestehen gesetzliche Anforderungen an die Ausgestaltung des Revisionsgeschäftes und ihrer Prüfaktivitäten, die dazu führen, dass sie meist einen umfangreichen Stab an Mitarbeitern aufweisen. Größenordnungen von 30 bis mehr als 50 Revisoren in weltweit operierenden Konzernrevisionen sind durchaus anzutreffen. Entsprechend wird dort (und auch in anderen Branchen) z.B. über REDIS ® oder QSR ® sowohl der Einsatz der Revisoren als auch die Definition der Prüffelder/Prüflandkarten gesteuert. Es existieren bereits vordefinierte umfangreiche Prüffelddefinitionen, die beliebig erweiterbar, jedoch stark 'bankenlastig' sind. Dies ist für das Softwareunternehmen mehr als sinnvoll und macht letztendlich auch das Know-how aus, da sie vollständige/umfassende Leistungen insbesondere im Finanzbereich anbieten kann - somit zählen Banken zu den größten Nutzern.

Für Unternehmen [anderer Branchen], die sich nur wenige Mitarbeiter in der Revision erlauben, ist der Einsatz einer solchen Software schwierig - die vorhandenen Prüffelddefinitionen sind en Detail nur marginal nutzbar, so dass der Einsatz eines solchen Softwarepaketes aus wirtschaftlichen Überlegungen heraus kaum zu rechtfertigen ist. Zudem muss ein solches System auch nachhaltig gepflegt werden. Bei Revisionsstäben mit weniger als 10 Mitarbeiterkapazitäten bedeutet dies einen zu hohen Verlust an Arbeitsleistung und Aufbau von Overhead, insbesondere weil hier die DV-gestützte Mitarbeitereinsatzplanung nicht zwingend erforderlich ist.

Trotzdem wird auch hier inzwischen erwartet, dass die auf das Unternehmen wirkenden Risiken erkannt, analysiert, revisorisch bewertet und in einen Risiko-Aktivitäten-Kontext gebracht werden. Um hier eine möglichst objektive, nachhaltige und mit einer Historie versehene Beurteilungsmöglichkeit zu schaffen, ist es unausweichlich, die risikoorientierte Planung der Revisionsaktivitäten DV-gestützt erfolgen zu lassen. Der nachfolgende Artikel soll grob die Anforderungen an eine Softwareunterstützung speziell aus Sicht eines kleinen Revisionsbereiches darlegen.

Risiken des Unternehmens

Bevor man sich mit einer detaillierten Beurteilungs- und Analysemöglichkeit auseinandersetzt, ist zu klären, was das Unternehmen als Risiko klassifiziert und ob diese Definition aus Revisionssicht übernommen werden kann.

Risiken stellen aus Sicht des Unternehmens grundsätzlich eine Aggregation vorhandener, vornehmlich monetär bewertbarer Faktoren dar, die auf die Ertragskraft und Handlungsfähigkeit des Unternehmens wirken - sowohl im Kerngeschäft als auch bei Innovationsprozessen im Sinne der Auswirkung einer "Chance". Dabei spielt die potentielle Schadenhöhe und die Eintrittswahrscheinlichkeit eine entscheidende Rolle (Einbezug von mathematischen Bewertungsmethoden). Häufig wird nicht das Risiko selbst definiert, sondern auf eine Beschreibung der charakteristischen Risikoeigenschaften und deren Wirkung zurückgegriffen (vgl. KREY, S. 33.). Risiken müssen analysiert, klassifiziert und im Risikomanagement eingebettet sein, so dass sich hieraus Handlungsrahmen/Reaktionspläne (Notfall-/Krisenmanagement u.a.) ableiten lassen. Innerhalb einer solchen Betrachtung liegen auch Risiken im Fokus, die nicht aus dem Unternehmen heraus steuerbar sind, z.B. politische Gegebenheiten, die Mitbewerbersituation, Katastrophenszenarien (z.B. auch Terrorismus u.ä.) oder Umwelteinflüsse.

Die Interne Revision wandelt diese Unternehmenssicht ab. Zum einen klammert sie die aus dem Unternehmen heraus nicht steuerbaren Risiken überwiegend aus, und zum anderen bricht sie Risiken auf die operative Ebene herunter und bildet einen Extrakt, der die Einflussfaktoren beinhaltet, die in der Internen Revision mit überwiegendem Blick auf Zweckmäßigkeit, Organisation, Wirtschaftlichkeit, Ordnungsmäßigkeit und Sicherheit geprüft werden können (vgl. KREY, S. 115ff.).

Dies ist jedoch keine erschöpfende Sicht, vielmehr "kommt es nicht mehr nur darauf an, Risiken zu vermeiden, [...der Fokus liegt] auf der Beurteilung der Effektivität von Management und Kontrolle dieser Risiken. Erst die Kenntnis der Risikopotentiale versetzt die Interne Revision in die Lage, die Funktionsfähigkeit der Überwachungssysteme des Unternehmens zu prüfen. Die Konsequenz ist eine Ausrichtung der Revisionsaktivitäten auf die Risikobereiche des Unternehmens." (KREY, S. 20.) Entsprechend integriert die Interne Revision neben der Vermögenssicherung weitere "Zielvorstellungen [wie] das Generieren von Potentialen zur Effizienzsteigerung sowie von Synergieeffekten (u.a. optimaler Ressourceneinsatz) [und] die Überwachung und Sicherung der Zuverlässigkeit von Informationen der Unternehmensführung für das Risikomanagement." (KREY, S. 89.) So entsteht eine systematische Zusammenstellung von Prüfungsobjekten, also eine Prüffeldübersicht oder Prüflandkarte, die die im Unternehmen operativ beeinflussbaren Risiken darstellt. Prüffelder sind somit zu verstehen als Zusammenfassung von gleichartigen Risikoeinflussgrößen - (in Kombination) prozess- und funktionsorientiert (vgl. KREY, S. 117ff.).

Prüffeldbezeichnung
[...]
Datensicherung / Recovery / Ausfallsicherheit / Notfallkonzepte IT
Entwicklung von eigenständigen Anwendungen (Programmiersprache, Entwickl.umgeb., CASE etc.)
Installation, Betrieb und Wartung von IT-Komponenten
Kundenabrechnungsprozess
Leistungsverrechnung von IT-(Dienst) Leistungen / IT-Controlling
Manipulation / Missbrauch / Privatnutzung von firmeneigenen IT-Komponenten
Projektmanagement
Organisation und Support bei IT-Prozessen
Risikomanagement (KonTraG)
SAP R/3 - Einsatz/Betrieb und
Sicherheit
[...]

Tab. 1: Auszug aus Beispiel-Prüffelderliste

Anforderungen an die Beurteilung

"Ein risikoorientierter Prüfungsansatz [...] sollte als Reaktion auf moderne Unternehmensstrukturen die Ausrichtung der Revisionstätigkeit auf die unternehmerischen Risikobereiche und eine daran orientierte Ausgestaltung der Revisionsaktivitäten zum Gegenstand haben. Das erfordert den Übergang von der vergangenheitsorientierten, nur feststellenden [...] zur zukunftsorientierten, innovativen Internen Revision. Dies bedeutet eine Verbesserung der Beratungsfunktion für Management und Fachabteilungen durch zielführende und praktikablere Verbesserungsvorschläge und Anregungen." (KREY, S. 21.)

"Die Risikoorientierung führt zu einer Strategie der ‚Prüfung der wesentlichen Risikobereiche' des Unternehmens. Risikoorientierung heißt in diesem Kontext:

- Ausrichtung von Prüfungsgegenstand und -umfang an den Fehlerquellen des Unternehmens - Analyse der Unternehmensrisiken
- Ausrichtung an den Fehlermöglichkeiten der Internen Revision - Gestaltung des Prüfungsprozesses zur Gewährleistung der erwarteten Qualität und Sicherstellen der notwendigen Qualifikation der Revisoren." (KREY, S. 41.)

Dies darf jedoch nicht dazu führen, dass weniger risikobehaftete Felder keine Beachtung finden. Vielmehr ist für eine Ausgewogenheit zwischen risikoorientiertem Ansatz und einer turnusorientierten Beachtung von Prüffeldern zu sorgen (vgl. KREY, S. 78ff, 203f.).

So ergibt sich bei einer Systematisierung die Notwendigkeit, dass Prüffelder einerseits einer iterativen Risikobetrachtung unterzogen und andererseits mit einem Mindest-Prüfungsabstand definiert werden, der aussagt, innerhalb welches Zeitraumes mindestens eine Prüfung erfolgen muss (Turnusbestimmung). Weiterhin ergänzt die Definition von Mehrjahresprüfplänen den Einbezug des Turnusansatzes, so dass eingesehen werden kann, welche Prüffelder innerhalb eines Zeitraumes bereits geprüft wurden und welche noch ausstehen.

Bewertung von Prüffeldern

Die Bewertung von Prüffeldern gilt als eine besondere Herausforderung, da zum einen Beurteilungskriterien vorhanden sein müssen, die eine [zumindest ansatzweise] objektive Würdigung erlauben und zum anderen durch die Verschiedenartigkeit der Prüffelder eine Ausprägungseinschätzung dieser Kriterien bei der Bewertung oftmals schwierig ist. Als Grundlage für die objektive Beurteilung ist die Definition von Gewichtungsstufen zu sehen, die eine realistische und dauerhafte Abgrenzung der Kriterien untereinander bewirken soll (vgl. KREY, S. 163, 176.).

Weiterhin ist zu klären, welchen Beurteilungsmodus die Interne Revision wählt. Es ist sinnvoll, dass Prüffelder jedes Jahr aufs Neue - jeweils vor Beginn des nächsten Prüfungsjahres - bewertet werden, da sich Risiken durch externe Einflüsse sukzessive verändern (vgl. KREY, S. 164f.), so dass sich jedes Jahr ein komplett neuer Beurteilungslauf für alle Prüffelder ergibt. So ist es möglich, die Entwicklung der Risikoeinschätzung über mehrere Jahre zu beobachten.

Es ist auch denkbar, dass jedes Prüffeld nur initial bei Erstaufnahme bewertet wird und sich die zukünftigen Bewertungen und damit Rangfolgepositionen der Prüffelder ‚maschinell' als Fortschreibung aus den Ergebnissen der Prüfungen, die sich auf Prüffelder beziehen, jährlich neu ergeben.

Des weiteren ist festzulegen, ob bei der Beurteilung bestimmte Prüfkriterien bei ausgesuchten Prüffeldern ausgeblendet werden können oder ob alle Prüffelder mit allen Prüfkriterien bewertet werden müssen (bei Ausblendung besteht die Gefahr des unqualifizierten Vergleiches). Außerdem sollten bei Prüffeldern, aus denen sich jährlich eine Prüfung ergeben muss (z.B. aus einer gesetzlichen Verpflichtung heraus), Bewertungen nicht möglich sein, denn es ergibt sich bereits aus dem Zwang, jährlich zu prüfen, die höchste Rangposition - eine Bewertung und somit Positionsbestimmung ist hier unnötig.

Prüfkriterium
Beachtung im Risikomanagement
Wettbewerbsbedingungen: Abhängigkeit von... Lieferanten/Kunden/Marktveränderungen
Abhängigkeit von der IT
Eindeutige Regelungen/Kompetenzen/Verantwortung/Prozesse...Schnittstellen zu anderen FB...Kontrollen
Ergebnis der letzten Prüfung
Zeitpunkt der letzten Prüfung
Mitarbeiterzufriedenheit / -fluktuation
Kapazitätsauslastung: Auslastung u/o Veränderung der rel. Auslastung im Zeitvergleich
Einhaltung der definierten Bereichsziele
Aufbau- und Ablauforganisation: Änderungen in der Org. in der letzten Zeit u/o Komplexität der Prozesse

Tab. 2: Beispiel-Prüfkriterienliste

Vorausgesetzt, dass die Prüffelder und -kriterien identifiziert sind und die Gewichtung der Kriterien eine sinnvolle Abgrenzung untereinander zulassen, ergeben sich für den Beurteilungsprozess folgende Anforderungen:

Jedes Prüffeld ist mit einer Ausprägung jedes Kriteriums zu bewerten. Ausnahme: Wie oben erwähnt dürfen jährlich zu prüfende Prüffelder nicht bewertet werden, da sie aufgrund der jährlichen Prüfnotwendigkeit bereits die höchste Priorität erhalten (müssen). "Die Gefahr eines Risikoeintritts (ausgedrückt durch die Bewertung der Risikofaktoren) und das Ausmaß der Beeinträchtigung der Unternehmensziele (wiedergegeben in der Gewichtung der Risikofaktoren entsprechend deren Bedeutung zur Prozess-/Unternehmenszielerreichung) determinieren damit die Art und Weise des Erreichens der Revisionsziele." (KREY, S. 183.)

Weiterhin müssen Prüffelder erweiterbar sein, dabei darf es keinen Verlust an Vergleichbarkeit geben, das Hinzufügen neuer oder Ändern bestehender Prüffelder ist zu historisieren. Gleiches gilt für Prüfkriterien. Prüffeldern sind Mindest-Prüfungsabstände in Jahren zuzuweisen, die definieren, in welchen Abständen die Prüffelder mindestens geprüft werden sollen (Turnusbestimmung). Ihnen sollten auch fachlich zuständige Abteilungen des Unternehmens zugewiesen werden. Die Beurteilung eines Prüffeldes sollte grundsätzlich dauerhaft durch eine Person erfolgen, ein (regelmäßiger/häufiger) Wechsel führt zur Änderung von Wertmaßstäben. Dabei sollten einem Revisor als verantwortlichen Beurteiler ca. 20 Prüffelder zugewiesen werden, da ansonsten diese Art der Risikodarstellung ggf. zu komplex wird (vgl. KREY, S. 169f, S. 176.)

Es ist ein Rollenkonzept und ein gesichertes Login zu implementieren, dass die Rollen Administrator, Revisor und Leiter beinhaltet. Die Rollenverteilung darf nicht auf eine je Mitarbeiter begrenzt sein. Die Administrationsrolle sollte in der Revision ausgeübt werden. Änderungen an Benutzerstammsätzen wie Hinzufügen, Löschen, Namensänderung oder die Kennwortänderung eines Benutzers durch den Administrator sind zu historisieren.

Während der Beurteilungsphase darf kein Revisor die Rangfolgeposition der ihm zugewiesenen Prüffelder gegenüber denen seiner Kollegen einsehen können, da dies die Beurteilung beeinflusst. Der Beurteilungsprozess für ein neues Planungsjahr sollte bis zu einem bestimmten Datum im alten Jahr, z.B. bis Ende November, abgeschlossen sein. Danach muss die Ermittlung der Rangfolgepositionen der Prüffelder erfolgen, die als "Maß der Prüfungsdringlichkeit interpretiert werden" (KREY, S. 183.), so dass die Revisionsleitung in der Lage ist, gemeinsam mit jedem einzelnen Revisor aus der Rangliste heraus das individuelle Prüfprogramm des Folgejahres abzuleiten.

Mit realistischem Blick werden die Prüffelder markiert, aus

denen sich eine Prüfung ergibt. Sofern in der Rangfolge hoch angesiedelte Prüffelder keine Prüfung ergeben (z.B. durch fehlende Ressourcen), ist eine Begründung für das Ausbleiben einer Prüfung zu hinterlegen. Prüffelder müssen als Prüfungsvormerkung in der Zukunft markierbar sein. Prüfungsvormerkungen aus der Vergangenheit und Review-Vereinbarungen müssen als Prüfung wählbar sein.

Automatische Prüfungszuweisungen darf es jedoch nicht geben, weil Ressourcenengpässe in kleinen Revisionsstäben Automatismen kaum zulassen. Gleichwohl muss es möglich sein, die Prüffelderrisikosicht und die Übersicht der Prüffelder, die außerhalb ihres definierten Prüfungsturnus' liegen, gegenüber zu stellen, um beide Darstellungen ausgewogen in die Auswahl der Prüfthemen einfließen zu lassen.

Die folgende Tabelle zeigt die Vor- und Nachteile einer solchen Beurteilungsmöglichkeit auf (vgl. KREY, S. 183f.):

Vorteil	Nachteil
Grundsätzlich Förderung systematischer Problembearbeitung	Monetär bewertbare Kriterien verlieren durch Scoring ihre Genauigkeit, können jedoch angemessen berücksichtigt werden
Möglichkeit zur Berücksichtigung verschiedener Zielgrößen mit unterschiedlichen Dimensionen.	Möglichkeit zur Erfassung der Prüfungsziele in Scoringwerten (Dynamik der Unternehmensumwelt)
Fundierte Bestimmung der Risikofaktoren anhand ihres Einflusses auf das Prüfungsrisiko	Erfahrung und Know-how des Revisors bestimmen die Qualität der Prognosen, so werden ggf. "beliebte" Themen bevorzugt, während bagatellisierte/marginalisierte Themen ausgeklammert werden
Flexibilität bei der Zahl der Risikofaktoren je Prüffeld, wobei zum Schutz der Vergleichbarkeit jedes Prüffeld mit jedem Kriterium beurteilt werden sollte	Transparenz der Subjektivität von Entscheidungen
Trotz Komplexitätsreduktion ausreichend große Anzahl von Beurteilungsobjekten und -maßstäben	

Tab. 3: Vor- und Nachteile eines Scoring-Verfahrens mit Bezug zur Nutzwertanalyse

Entsprechend gilt es, ein Scoring-Verfahren zu entwickeln, das mit (ggf. mit der Unternehmensleitung) abgestimmten Beurteilungskriterien und einer angemessenen Abstufung untereinander dauerhaft ein Höchstmaß an Objektivität ermöglicht.

Prüfungsableitung

Nach der Beurteilung der Prüffelder definiert jeder Revisor mit dem Revisionsleiter aus der Beurteilungsmatrix die Prüfungen des Folgejahres als Soll-Vorgabe. So definierte Prüfungen werden im Laufe des Prüfungsjahres mit entsprechenden Echtdaten versehen. Dies können z.B. sein:

- Konkreter Prüfungstitel, Zusammenfassung bzw. Prüfberichttext, Kenntlichmachung einer Unterstützung durch Externe und Name des Dienstleisters
- Wann wurde die Prüfung eingeplant?
- Handelt es sich um eine Prüfung aus einer Bewertung heraus oder um ein Review?
- Wann wurde die Prüfungsvorbereitung begonnen?
- Wann wurde die Prüfung dem Fachbereich angekündigt?
- Wann wurde die Prüfung begonnen?
- Wann wurde dem Fachbereich ein Fragenkatalog übergeben und wann erhielt die IR diesen wieder ausgefüllt zurück?
- Wann wurde die Prüfung beendet ?
- Seit wann liegt der Prüfbericht vor?
- Wann fand die letzte Schlussbesprechung mit den beteiligten Fachbereichen statt ?
- Für welches Jahr wurde ein Review aus dem Bericht heraus eingeplant?

- Wann lag dem Vorstand der Bericht vor bzw. fand die Besprechung beim Vorstand statt?
- Hinterlegung eines Prüfungs-status' (in Bearbeitung oder beendet)
- Hinterlegung eines kurzen Gesamtergebnisses
- Hinterlegung div. Differenzen zwischen bestimmten Ereignissen, z.B. zwischen ‚Prüfung begonnen' und ‚Prüfung beendet', ‚Prüfung begonnen' und ‚Bericht an Vorstand' usw.

Werden vereinbarte Prüfungen nicht durchgeführt, müssen diese als ‚nicht durchgeführt' zu erkennen sein und eine Ersatzprüfung ist ggf. zu wählen. Dies muss sich später im Soll-Ist-Vergleich widerspiegeln.

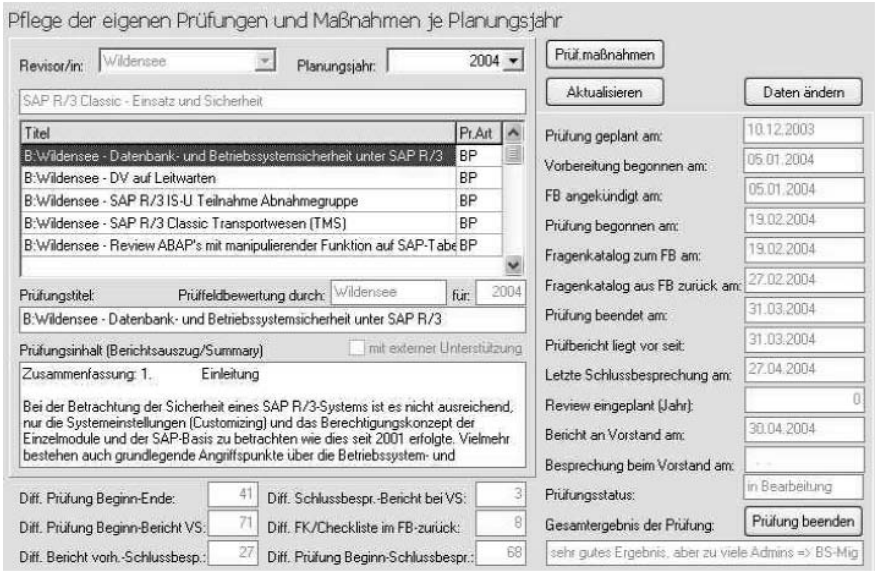


Abb. 1: Beispiel Prüfungsdaten

Beginn und Ende einer Prüfung sind als alleinige Muss-Felder zu definieren, bevor sie beendet werden kann. Es ist möglich, dass eine Prüfung als Beratung endet und sich kein Bericht ergibt, so dass die Berichtsvorlage nicht als zwingend erachtet werden kann.

Die interne Beratung - auch in Projekten - stellt neben der Prüfung den zweiten, als eigenständige Aufgabe wichtigen Aspekt der Internen Revision dar, der gleichsam ein elementarer Bestandteil des Führungsprozesses des Unternehmens ist (vgl. HUNECKE, S. 51, 64.). "Die Interne Revision kann aufgrund fehlender Anordnungsbefugnis nur eine Unterstützungsfunktion bei der Umsetzung von Verbesserungsvorschlägen übernehmen." (HUNECKE, S. 126.) Dies hat sie mit externen Beratungsdienstleistern gemein. Dabei ist es unternehmensabhängig, welche Akzeptanz eine interne Beratung gegenüber einer externen aufweist, wobei eine externe Beratung im Nachhinein selten belastbar ist und nicht immer an den tatsächlichen betrieblichen Erfordernissen gespiegelt werden kann (vgl. HUNECKE, S. 127ff.). Dem gegenüber stellt die IR bei ihren Empfehlungen die Realisierbarkeit in den Mittelpunkt - so berücksichtigt sie unternehmensspezifische Gegebenheiten im allgemeinen sinnvoller, d.h. prozessnäher, während hier der Einbezug außerbetrieblicher Erfahrungen problematisch ist (vgl. HUNECKE, S. 200f., vgl. SCHWEIGER, S. 246ff).

Sofern die Beratungsleistungen der Revisoren dokumentiert werden sollen, ist auch die Beratung jedes einzelnen Revisors als Prüffeld aufzunehmen.

Anforderungen an die Maßnahmenverfolgung

Die Maßnahmenverfolgung, d.h. die Überprüfung der Umsetzung von Fachbereichsaktivitäten aus einem Prüfbericht heraus (Follow-Up-Konzept), ist eine wesentliche Forderung für eine Systematisierung revisorischer Arbeitsleistung. Bei der Definition von Maßnahmen wird ein Termin gesetzt, zu dem die Vereinbarung durch einen Verantwortlichen spätestens umgesetzt sein muss. "Bei Erreichen dieser vorgegebenen zeitlichen Meilensteine der Prüfungsempfehlungen sind die wesentlichen Risiken daraufhin zu untersuchen, inwieweit diese auch tatsächlich im Fachbereich aufgegriffen wurden." (KREY, S. 241.)

Dabei ist zu gewährleisten, dass der zuständige Revisor nach Verstreichen des Umsetzungszeitpunktes Kenntnis über die fehlende Umsetzung erhält, so dass er im Fachbereich Gründe für das Ausbleiben einholen und ggf. eine Nachfrist setzen oder aber nach vollzogener Umsetzung die Maßnahme als umgesetzt markieren kann. "Haben Unternehmensführung bzw. die Verantwortungsträger [...] Prüfungsempfehlungen nicht aufgegriffen, besteht die wesentliche Aufgabe des Follow-Up zu überprüfen, ob dem Management das Risiko einer unterlassenen Korrektur bewusst ist." (KREY, S. 241.) Dementsprechend sind die nicht umgesetzten Empfehlungen zu erfassen und gesondert mit Erläuterung herauszustellen.

Entsprechend muss es möglich sein, sowohl eine komplette Maßnahmendarstellung eines Jahres zu erhalten als auch ausstehende Maßnahmenumsetzungen innerhalb einer Datumseingrenzung anzeigen zu lassen. Des weiteren sollten Maßnahmen nach Verantwortung sortiert werden können.

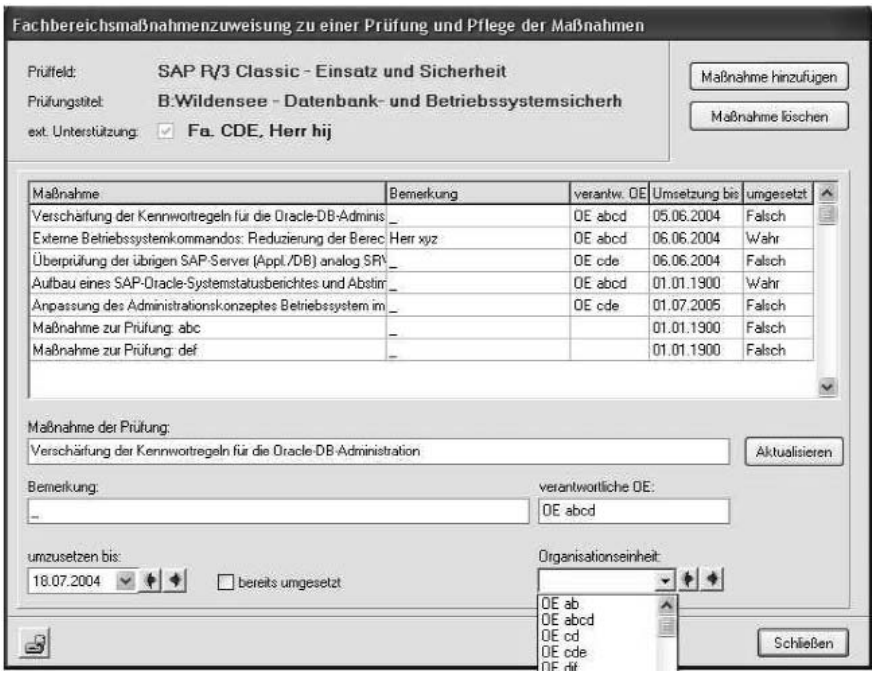


Abb. 2: Maßnahmen einer Prüfung

Auswertungsanforderungen

Eine Systematisierung bedeutet gleichsam, dass umfangreiche Auswertungsmöglichkeiten zur Verfügung stehen, die verschiedene Informationsbedarfe befriedigen.

Folgende Auswertungen sind hier als sinnvoll beispielhaft zu nennen:

- Übersicht über alle Revisoren incl. deren Rechte, Übersicht über zugewiesene Prüffelder jedes einzelnen Revisors, hieraus Übersicht über zugewiesene Organisationseinheiten, hieraus Übersicht über alle der OE zugewiesenen Prüffelder
- Übersicht über - alle Prüffelder, - alle Prüfkriterien und deren Gewichtung, - alle OE's
- Übersicht über Prüfungen zur Organisationseinheit
- Übersicht über Prüfungen je Jahr und je Jahr/je Revisor
- Darstellung der Ursprungsprüfung(en) zu einer Prüfung (z.B. bei Review)
- Suche nach bestimmten Begriffen in Prüfungen
- Übersicht über bisher durch Prüfungen nicht berührte Organisationseinheiten
- Übersicht über Maßnahmen je Jahr und je Jahr/je Revisor, sortiert nach Prüfung oder nach verantwortlichem Bereich
- Übersicht über Maßnahmen innerhalb einer Datumseingrenzung (Umsetzungszeitpunkt)
- Übersicht über bewertete Prüffelder je Jahr und je Jahr/je Revisor
- Übersicht über bewertete Prüffelder über mehrere Jahre
- Übersicht über bisherige Prüfungen zum ausgewählten Prüffeld
- Übersicht über Prüffelder, die außerhalb ihres definierten Prüfungsturnus' liegen
- Darstellung eines Prüfungen-Soll-Ist-Vergleiches je Jahr/Revisor (Revisoren dürfen nur ihren eigenen Soll-Ist-

Vergleich sehen, der Leiter sieht auch einen Komplett-Soll-Ist-Vergleich)

- Übersicht über Prüfungen mit fehlerhaften/unplausiblen Datumseingaben
- Darstellung der Benutzerhistorie und der Historie weiterer Objekte (Prüffelder, Kriterien etc.)
- Übersicht über Prüffelder, die jährlich zu prüfen sind, aber nicht zu einer Prüfung führten
- Übersicht über gelöschte Prüfungen

Fazit

Es ist nachvollziehbar, dass eine Analyse-/Beurteilungsunterstützung der revisorischen Risikobetrachtung notwendig ist. Dabei kann auch mit einer Systematisierung dieser Planungs- und Dokumentationsaufgaben das Problemfeld "einer objektiven Bewertung allein durch Anwendung (komplexer) mathematischer Verfahren nicht behoben werden, solange die zugrundeliegenden Daten auf einer subjektiven Einschätzung beruhen." (KREY, S. 169.)

Durch die Bereitstellung umfassender Auswertungs- und Nachbearbeitungsmöglichkeiten, die flexibel anpassbar sind, stellt die datenbankgestützte Systematisierung eine maßgebliche Dokumentations- und Legitimationsunterstützung revisorischer Leistungserbringung zur Verfügung.

Trotzdem ist insbesondere für kleine Revisionsstäbe die Systematisierung der Arbeitsleistung in der beschriebenen Form als Möglichkeit zu sehen, die Entscheidungsfindung des Aktivitäten- / Jahresprüfplanes der Revisoren zu historisieren und im Nachhinein nachvollziehbar darzustellen. Sie ist ein "fundiertes Auswahlinstrument als ein weniger systematisches einfaches Ranking der bewerteten Risikofaktoren." (KREY, S. 183.) Zusätzlich wird nicht nur die gesamte Leistungserbringung der Revisoren, sondern auch das Optimierungspotential der Unternehmensbereiche und das schlüssige Handeln in Risikobereichen dokumentiert. Durch die Bereitstellung umfassender Auswertungs- und Nachbearbeitungsmöglichkeiten, die flexibel anpassbar sind, stellt die datenbankgestützte Systematisierung eine maßgebliche Dokumentations- und Legitimationsunterstützung revisorischer Leistungserbringung zur Verfügung.

Literatur / Internet-Seiten

Hunecke, Jörg:
Interne Beratung durch die Interne Revision
Diss., Schriftenreihe Rechnungslegung - Steuern - Prüfung,
Band 5, Technische Universität München, 2. Auflage 2003.

Krey, Sandra:
Konzeption und Anwendung eines risikoorientierten Prüfungsansatzes in der Internen Revision,
Diss., KPMG, Berlin, 2001.

Schweiger, Elmar:
Beratung durch die Interne Revision - Ihre Rolle, hre Risiken und ihre Chancen
In: Zeitschrift Interne Revision (ZIR), 6/2003.

http://www.theiia.org/
The Institute of Internal Auditors

http://www.isaca.org/
Information Systems Audit and Control Association

http://www.idw.de/
Institut der Wirtschaftsprüfer

http://www.iir-ev.de/
Deutsches Institut für Interne Revision e.V.

http://www.auditplan-xp.de/
AuditPlan XP

Noch immer aktuell:

❑ **Titel:** **Baurevision**

Autor: Hans-Günter Wenzel
ISBN: 3-930291-16-9
Seiten: 600
Preis: 65,45 €

Inhalt:

Hans-Günther Wenzel hat in dem vorliegenden Buch „Baurevision“, das sich am Ablauf von Baumaßnahmen orientiert, seine Erfahrungen und Kenntnisse beschrieben. Von den ersten Planungsschritten bis zur Beseitigung von Gewährleistungsmängeln werden Möglichkeiten aufgezeigt, die in der Praxis häufig zur Schädigung des Bauherrn führen, sowie entsprechende Maßnahmen aufgezeigt, die dies verhindern sollen. Die technische Revision hat ganz besonders im Bauwesen zur Aufdeckung von erheblichem Risikopotenzial in den verschiedenen Bauphasen geführt. Für Bauherren ist es wichtig, die eigenen Möglichkeiten zur Erschwerung von Bestechung und Bauabsprachen zu kennen und zu nutzen. Neben einer ausführlichen Einführung in die Themenbereiche der Baurevision werden die wichtigen Fragen aus der Praxis eingehend beantwortet. Zum Verständnis der Prüfvorgänge und des Buchinhaltes sind bautechnische Kenntnisse nicht notwendig.

H.-G. Wenzel verfügt sowohl über Erfahrungen als Projektverantwortlicher bei Baumaßnahmen als auch über eine 12-jährige Erfahrung als technischer Revisor. Auch aus seiner Tätigkeit als Referent für Baurevision bei einem namhaften Veranstalter von Revisionsseminaren schöpft er die vielfältigen Fragen und Antworten zu den einzelnen Themen der Baurevision..

Bestell-Fax 040/69 69 85-31

Name: ..... PLZ/Ort: .....

Vorname: ..... Tel.: .....

Firma: ..... E-Mail: .....

Abteilung ..... Ort/Datum: .....

Straße: ..... Unterschrift .....

Ottokar Schreiber Verlag GmbH
Revision • Controlling • Informatik • PPP
Friedrich-Ebert-Damm 145
22047 Hamburg
Tel.: +49 40 69 69 85-14
Fax: +49 40 69 69 85-31
www.osv-hamburg.de
sales@osv-hamburg.de

+++ SEMINARE +++

Seminarcode: **R3DP**
11.11-12.11.04

Datenprüfung im Umfeld des SAP-Systems

Inhalte u.a.:

Datenprüfung in Theorie und Praxis
- Werkzeuge der Datenprüfung
- Methoden der Datenprüfung
- Ergebnisinterpretation

Datenprüfung mit SAP
- Reports
- Accounting / Audit Information System
- GDPdU konforme Schnittstellen

Datenprüfung FI
- Kreditoren
- Debitoren
- Anlagen

Datenprüfung MM
- Stammdaten (MARA)
- Materialbewegung
- Inventuren

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **R3SY**
15.11.-17.11.04

Systemprüfung von SAP R/3®

Inhalte u.a.:

Basissicherheit
- Schichten eines SAP-Systems und Gefahrenpunkte
- OSS/SAP Marketplace

Benutzerverwaltung
- Grundkonzeption

Protokollierungskomponenten
- Auditing

Verbuchungsprinzip
- Organisatorische und systemseitige Handhabung

Tabellensteuerung
- Protokollierung
- Technische Konzeption der Änderungsbelege

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **R3BK**
18.11.-19.11.04

Prüfung des Berechtigungskonzeptes von SAP R/3® Systemen

Inhalte u.a.:

Aufbau des Berechtigungskonzeptes
- Objekte / Berechtigungen / Profile
- Transaktionsberechtigungen

Die Problematik des Berechtigungskonzeptes
- Komplexität und Quantität
- Kritische Berechtigungen

Konzepte zur Implementierung des Berechtigungskonzept

Tipps und Tricks beim Umgang mit dem Berechtigungskonzept

Der Profilgenerator

Möglichkeiten zur Prüfung mit externen Werkzeugen

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **R3PB**
22.11.-24.11.04

Prüfungsworkshop zur Sicherheit einer SAP R/3® Systemlandschaft

Inhalte u.a.:

Einführung
- Prüffelder zur SAP R/3® Systemprüfung
- Prüfleitfaden (organisatorische und systemseitige Vorgaben)

Workshopthema
- Prüfung der Sicherheit einer SAP R/3® Systemlandschaft

Prüfprozedur
- Erstellung eines Handlungsleitfaden
- Durchführung der Prüfungshandlungen
- Dokumentationen der Prüfergebnisse
- Präsentation der Prüfprozedur und Prüfergebnisse

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **R3FI**
25.11.-26.11.04

Revisionsworkshop „Finanzbuchhaltung" von SAP R/3® Systemen

Inhalte u.a.:

Aufbau, Funktionalität und Organisation
- Gesamtsystem
- Datenaufbau und Datenfluss
- Abbildung buchhalterischer Abläufe im SAP-System

Modul FI
- Transaktionen
- Plausibilitätsprüfungen
- Kreditoren und Rechnungsprüfung

Auswertungsmöglichkeiten mit SAP-Mitteln
- Standardreports
- Reportmodifizierung
- Überwachung der Tabellen-protokollierung

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **R3MM**
29.11.-30.11.04

Revisionsworkshop Material-wirtschaft - MM von SAP R/3® Systemen

Inhalte u.a.:

Vorbemerkungen

Bedarfsplanung/Prognose

Bestellanforderungen

Anfragen/Angebote

Bestellungen/Kontrakte

Bestandsführung/Bewertung

Rechnungseingang

Inventur

Bilanzbewertung

Übergreifende Themen
- Lieferantenbeurteilung
- Informationssysteme

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

+++ SEMINARE +++

Seminarcode: **GMEI**
10.11.-12.11.04

Prüfen des Einkauf

Inhalte u.a.:

Einführung
- Gefährdungspotenzial des Einkaufs
- Der Prozess des Einkaufs

Risiken im Beschaffungsprozess und Risikosteuerung
- Risikopotential + -ranking
- Risiko-Steuerungsmaßnahmen

Kommunikationsfluss
- Richtlinien/Verfahrensanweisungen für den Einkauf
- Der Kommunikationsweg von der Anforderung bis zur Liefreung und Abnahme und Rückkopplung

Fallbeispiele im Zusammenhang

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **GMPM**
15.11.-16.11.04

Prüfmethoden (Workshop)

Inhalte u.a.:

Einführung
- Vom Wesen der Prüfung
- Vorbereitung und Durchführung von Prüfungen

Prüfmethoden
- Abfragen/Interviews
- Vergleich (Benchmark)
- Verprobung (Überschlagsrechnung)
- Vor-Ort-Begehung (Inventur)

Kennzahlen
- Kennzahlensysteme - Übersicht
- Kennzahlen als Meta-Daten des Betriebs
- Kennzahlen als Erkenntnis-Basis für die Revision
- Nutzung des BSC (Balanced Score Card) für die Revision

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **DSAS**
18.11.-19.11.04

Windows 2000 Active Directory Services

Inhalte u.a.:

Einführung und Verzeichnisdienste
- Philosophie
- Protokolle und Standards

Active Directory Services
- Physische und logische Struktur
- Objekte und Objektsicherheit
- technische Hintergründe

Gruppenrichtlinien
- Steuerungsmöglichkeiten
- Prüfungsansätze und Tools
- bekannte Probleme

Migration
- Upgrade versus Neuinstallation
- Client Roll-out
- Prüfungsaspekte

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **DSFW**
25.11.-26.11.04

Prüfen von Firewall-Konzepten

Inhalte u.a.:

Grundlagen der Sicherheit

Sicherheitselemente

Einbindung von Sicherheit in Netzwerke

Sicherheitskonzepte
- Intranet/Internet

Internetprotokoll IP
- Protokoll-Datenstruktur

Firewall-Architekturen

Angriffstest und Revisionen

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **DSUX**
29.11.-30.11.04

UNIX/Linux für Revisoren und Datenschutzbeauftragte

Inhalte u.a.:

Einführung:
- UNIX-Dateiverwaltung
- grundlegende UNIX-Befehle

Zugriffssicherungen
- Zugriffsrechte unter UNIX
- Konfiguration der Dienste

Datensicherheit und Datenschutz
- Das Problem „root“
- UPS-Systeme

Werkzeuge für die IT-Revision
- SAINT (SATAN)
- USEIT
- Exportieren von Auswertungsergebnissen auf den Prüfer-PC
- Checklisten und ihre praktische Anwendung

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

Seminarcode: **GMIR**
02.12.-03.12.04

Einführung in die Interne Revision

Inhalte u.a.:

Einführung:
- Der Betrieb - Prüfgegenstand der Revision
- Vom Wesen der Prüfung

Grundsätze der Internen Revision (IR):
- Ordnungsmäßigkeit
- Wirtschaftlichkeit

Prüfungdurchführung
- Vorbereitung der Prüfung
- Berichterstattung

Risikomanagement unter Revisionsaspekten:

Organisation und Verwaltung der Revision:
- IT-Werkzeuge für die Revision

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145

22047 Hamburg

www.ibs-hamburg.com
seminare@ibs-hamburg.com

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Mitarbeiter situations-gerecht führen

Inhalte u.a.:

- Kompetenz und Motivation
- Welcher Führungstyp bin ich?
- Welche Mitarbeietrtypen gibt es?
- Wie führe ich welchen Mitarbeiter?
- Welche Führungsstile gibt es?
- Schlüsselqualifikationen
- Lob und Kritik
- Durch Fragen führen
- Wie leite ich richtig?
- Die gemeinsame Absprache

Die Referenten:

Thorsten Schildt,
PRAESENTATIO, Rheine

Termin und Ort:

02. - 03. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041161**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Datenschutz im Krankenhaus

Inhalte u.a.:

Aktuell: Verbesserte Situation des DSB nach der BDSG-Novelle 2002?

DSB im Krankenhaus

Im Dickicht der Paragrafen - welche Vorschriften gelten in welcher Art im Krankenhaus?

Typische Schwachstellen

Neue Techniken - neue Herausforderungen

Outsourcing - Wege und Grenzen

Der Referent:

Dr. Eugen Ehmann, Regierungsdirektor

Termin und Ort:

15. Dezember 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041232.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Was muss ein DSB bei vernetzten Systemen beachten?

Inhalte u.a.:

DV-technische Grundlagen
- Sicherheitsaspekte

Datenschutzrechtliche Grundlagen bei vernetzten Systemen
- Schulungserfordernis
- Auskunftserteilung

Umsetzung der Datenschutzbestimmung
- Richtlinien im PC-Bereich

Der Referent

Verschiedene

Termin und Ort:

25. - 26. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041123.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Datenschutz und Bankgeheimnis

Inhalte u.a.:

Das neue SCHUFA-Verfahren

Datenschutz-Klauseln bei Verbundgeschäften

Datenschutz und vorrangige Rechtsvorschriften

Cold Calling

Telefax / E-Mail

Informationsveranstaltungen für Führungskräfte

Die Referenten:

Dipl.-Volksw. Friedhelm Wolf, Kronberg

Termin und Ort:

16. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041124**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Bankbilanzierung

Inhalte u.a.:

Systematik und Grundlagen der bankrechtlichen Regelungen

Ausweis und Bewertung von Krediten

Ausweis und Bewertung von Wertpapieren

Währungsumrechnung nach § 340h HGB

Bilanzpolitische Spielräume

Aktuelle Bilanzierungsfragen

Die Referenten:

WP Horst Butte, Berlin

Termin und Ort:

08. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041141.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Buchführung: Vom Buchungssatz zur Bilanz

Inhalte u.a.:

Die Buchführung als Bestandteil des Rechnungswesens

Grundzüge der doppelten Buchführung

Praxis der Buchhaltung

Die EDV-gestützte Buchhaltung

Die EDV-gestützte Buchhaltung

Lexikon der wichtigsten Begriffe: verständlich definiert

Der Referent:

Dipl.-Betriebswirt Christian Wabenhorst,
Unternehmensberater, Korb bei Stuttgart

Termin und Ort:

15. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041121**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Die Compliance-Organisation im Finanzinstitut

Inhalte u.a.:

Einführung
- Die Entwicklung der Compliance-Philosophie

Die Insider-Regelung des WpHG
Die Compliance-Regeln des WpHG
Die Leitsätze für Mitarbeitdergeschäfte

Der Referent

Wolfgang Gabriel, Rechtsanwalt, Stellvertreter des Compliance-Beauftragten, SEB AG

Termin und Ort:

26. August 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041131.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Betriebswirtschaftliches Grundwissen für kompetente Chefassistenz

Inhalte u.a.:

Unternehmen im Wandel
Grundlagen des Controlling
Grundlagen des Marketing
Grundlagen des Arbeitsrechts
Literatur

Der Referent

Dipl.-Betriebsw. Christian Wabenhorst, Korb bei Stuttgart, Unternehmensberatung für Planung und Controlling

Termin und Ort:

16. - 17. Dezember 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041235.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Das Arbeitsrecht in der betrieblichen Praxis

Inhalte u.a.:

Grundzüge des Arbeitsrechts
Anmahnung des Arbeitsverhältnisses
Befristung von Arbeitsverhältnissen
Grundzüge des neuen Arbeitsgesetzes
Grundzüge des Urlaubsrecht
Mutterschutz / Erziehungsurlaub
Schwerbehindertenrecht
Kündigungsrecht

Der Referent

RA Dr. Ulrich Stoll,
Fachanwalt für Arbeitsrecht, Oberursel

Termin und Ort:

15. - 16. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041146**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Projektmanagement

Inhalte u.a.:

- Projektmanagement
- Management und Instrumente der Projektplanung und -steuerung
- Projektinformationen
- Projektarbeit ist Teamarbeit
- Projektabschluss
- Praxisfälle

Der Referent

Helga Herchenhan, freiberufliche Trainerin, DisKurs, Wuppertal

Termin und Ort:

25. - 26. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041153**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Was muss ein Datenschutzbeauftragter bei vernetzten Systemen beachten?

Inhalte u.a.:

- DV-technische Grundlagen
- Datenschutzrechtliche Grundlagen bei vernetzten Systemen
- Umsetzung der Datenschutzbestimmungen

Die Referenten:

Daniel Groß,
T-Systems International GmbH, Nürnberg
Dipl.-Volkswirt Friedhelm Wolf,
Externer Datenschutzbeauftragter, Königstein

Termin und Ort:

25. - 26. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041123**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Krisen-PR für Praktiker

Inhalte u.a.:

- Übung
- Prolog: Ethik des Glaubens
- Was ist eine Krise?
- Krisenfelder: Lokalisierung
- Krisenfelder: Prävention
- Krisenfelder: Früherkennung
- Aktive Krisen-PR
- Die Nachbereitung
- Sieben Ratschläge und acht Todsünden

Der Referent:

Dr. Perry Reisewitz, Geschäftsführender Gesellschafter der Compass Communications, Agentur für Unternehmenskommunikation, München

Termin und Ort:

25. - 26. November 2004
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **041158.**

Horváth & Partners (Hrsg.)

Balanced Scorecard umsetzen

Schäffer-Poeschel Verlag,
517 S., ISBN 3-7910-2268-7
49,95 €

Die Balanced Scorecard (BSC), ein Anfang der 90er Jahre von Professor Robert S. Kaplan und David P. Norton entwickeltes Managementsystem, hat zwischenzeitlich seinen festen Platz in der Unternehmenspraxis.

Dieses Werk stellt die Erfahrungen bei der Implementierung und laufenden Nutzung der BSC dar und stellt eine konsequente Ergänzung des Fachbuchbestsellers von "Kaplan/ Norton, Balanced Scorecard" dar. Die Autoren vermitteln in erster Linie für den Unternehmenspraktiker Praxistipps aus ihrer Beratungserfahrung, die durch eine Vielzahl von Unternehmensbeispielen sowie aus dem Öffentlichen Bereich veranschaulicht werden. Sowohl der Manager, der für die Strategiefindung und -umsetzung verantwortlich ist, als auch der Koordinatior der BSC-Einführung erhalten mit diesem Werk einen konkreten Leitfaden an die Hand.

In der nunmehr 3. Auflage erfolgt eine durchgehende Überarbeitung, insbesondere werden die Unternehmensbeispiele aktualisiert und um neue Erkenntnisse aus der Praxis ergänzt; die Ergebnisse einer von Horváth & Partners erstellten BSC-Praxisstudie runden die Erfahrungswerte aus der Unternehmenspraxis ab. Darüber hinaus erfolgt zur weiteren Illustration die Integration von Strategy Maps.

Péter Horváth (Hrsg.)

Die Strategieumsetzung erfolgreich steuern

Schäffer-Poeschel Verlag,
413 S., ISBN 3-7910-2317-9
59,95 €

Immaterielle Werte gelten als Faktor für den Unternehmenserfolg. Grundlage dafür ist eine erfolgreiche Strategieumsetzung, die mit innovativen Konzepten erreicht werden kann.

In diesem Werk, das die Beiträge des "Stuttgarter Controllerforum 2004" beinhaltet, werden innovative Konzepte zur Steuerung der Strategieumsetzung und erfolgreiche Praxislösungen aufgegriffen. Die einzelnen Beiträge befassen sich u.a. mit folgenden Fragestellungen: Wie steuert und gestaltet man den Weg von immateriellen Werten zum materiellen Erfolg? Welche Instrumente werden hierzu benötigt und wie werden diese in der Praxis angewandt? Wie gestaltet man einen Strategieumsetzungsprozess effektiv und effizient? Welchen Stellenwert haben Strategy Maps bei der Beschreibung, Messung und Organisation von Strategien? Wie integriert man das Risikomanagement in die strategische Steuerung? Und: Welche Auswirkung hat dies auf das Spannungsverhältnis von internem und externem Rechnungswesen? Wie ist das Wertmanagement von immateriellen Werten zu gestalten? In welcher Form kann dies durch standardisierte oder individuell angepasste IT-Instrumente unterstützt werden?

Das Werk stellt konkrete Vorschläge bei der Lösung dieser hochaktuellen Fragestellungen dar und gibt praxisrelevante Hilfestellungen bei der Umsetzung in der Unternehmenspraxis.

Péter Horváth / Ronald Gleich (Hrsg.)

Neugestaltung der Unternehmensplanung

Schäffer-Poeschel Verlag,
665 S., ISBN 3-7910-2107-9
79,95 €

Planung und Budgetierung sind zentrale Instrumente zur erfolgsorientierten Unternehmenssteuerung. In vielen Unternehmen wurden sie mit der Zielsetzung von zukünftigen Prognosen, der Schaffung von Leistungsanreizen, als Entscheidungshilfe etc. zu einem umfangreichen und komplexen System entwickelt. Trotz der hohen Bedeutung von traditionellen Ansätzen der Planung und Budgetierung sind diese unter massive Kritik geraten. Die Kritik bezieht sich beispielsweise auf einen, im Verhältnis zu einem in vielen Fällen nur eingeschränk-

ten Nutzen unverhältnismäßigen Ressourcenaufwand, der fehlenden Verbindung von strategischer und operativer Planung, der Eindimensionalität der Planung (d.h. Ausrichtung primär auf finanzielle Aspekte) und der Akzeptanz der Planung. Diese Kritikpunkte und verschiedene internationale Impulse zur Neugestaltung der Planung (z.B. "Beyond Budgeting") erfordern neue Ansätze zur Leistungssteigerung von Planung und Budgetierung. Vor diesem Hintergrund ist es Zielsetzung dieses Werkes, anhand von Praxisbeispielen nicht nur die wesentlichen Problemfelder aufzuzeigen, sondern vielmehr Lösungskriterien für die Neugestaltung der Planung und Budgetierung zu erläutern. Dazu gehören neben der Erhöhung der Flexibilität, die Erweiterung im einen Prozessfokus, eine nicht zu große Detaillierung, die Betrachtung wesentlicher Leistungsebenen sowie die Berücksichtigung nichtfinanzieller Aspekte in der Planung und Budgetierung. Die einbezogenen Praxisbeispiele basieren auf Beratungsprojekten und stammen aus unterschiedlichen Branchen.

Sven Hayn / Georg Graf Waldersee

IFRS / US-GAAP / HGB im Vergleich

Schäffer-Poeschel Verlag,
336 S., ISBN 3-7910-2155-9
39,90 €

IFRS und US-GAAP haben sich mittlerweile in der deutschen Bilanzierungspraxis fest etabliert. Den Jahresabschluss 2005 müssen börsennotierte Konzerne nach IFRS aufstellen. Damit wird die Implementierung von IFRS/ US-GAAP in den Unternehmen bereits zum Stichtag 31.12.2003 / 31.12.2004 notwendig. Wegen der Vergleichbarkeit des Zahlenmaterials werden auch mittelständische Unternehmen die neuen Rechnungslegungsvorschriften umsetzen müssen. Der in der Praxis bewährte Band wird durch die Darstellung aller drei Rechnungslegungssysteme zum Leitfaden für die Umstellung. Durch die Gegenüberstellung von HGB und internationalen Rechnungslegungsvorschriften wird deutlich, welche Ergebnisauswirkung die Umstellung haben wird. Die Unterschiede zwischen den einzelnen Rechnungslegungssystemen werden in dem Buch in Form einer Synopse dargestellt. Das Werk ist nach einzelnen Sachgebieten gegliedert. Schwerpunkte werden gesetzt bei Bilanzierungs-, Bewertungs- und Offenlegungsvorschriften. Die Darstellungen erfolgen getrennt für den Einzel- und den Konzernabschluss. Der Band setzt kein Spezialwissen voraus und soll zugleich als Leitfaden im Rahmen der Umstellung auf IRS oder US-GAAP und als übersichtliches Nachschlagewerk dienen.

Aktualisierungen für die 4. Auflage erfolgen hauptsächlich im Bereich IFRS und DRS. Erstmals enthalten ist außerdem ein Kapitel zur Umstellung auf IFRS in den Unternehmen unter besonderer Berücksichtigung der dabei anfallenden praktischen Probleme. Das Kapitel enthält ebenso Hinweise auf die Umstellung auf US-GAAP.

Rolf Bolten / Peter Pulte

Aufbewahrungsnormen und -fristen im Personalbereich

Datakontext Fachverlag,
336 S., ISBN 3-89577-319-0
46,00 €

Jeder Betrieb hat als Arbeitgeber mit vielen Schriftstücken, Dokumentationen und Unterlagen zu arbeiten, ohne die ein ordnungsmäßiger Betriebsablauf nicht möglich und die Erfüllung der arbeitgeberseitigen Fürsorge- und Sorgfaltspflichten nicht sichergestellt ist. In der 6. Auflage dieses überarbeiteten und erweiterten Werks über die Rechts- und Organisationsdokumentation der Aufbewahrungsnormen und -fristen für den Personalbereich sind die zahlreichen gesetzlichen Neuerungen eingearbeitet und dargestellt. Der Hauptteil des Buches enthält eine alphabetisch lexikalische Übersicht der aufzubewahrenden Urkunden, den Aufbewahrungsgrund und die Rechtsgrundlage. Dieser umfasst beispielsweise die Bereiche: Altersversorgung, Arbeitsanweisungen, Arbeitszeitkonten, Beitragsunterlagen, Bilanzen und viele weitere Sonderthemen.

ABO-Bestellung für ReVision

Ein Abo von ReVision beinhaltet folgende Verlagsdienstleistungen:

- Zugriffsfreigabe auf umfassende Informationen unter **www.revision-hamburg.de** mit allen jeweils erschienenen ReVisions-Beiträgen und Zusatzinformationen, abrufbar und selektierbar
- Zusendung vertiefender Hinweise und Unterlagen zu Beiträgen auf Anfrage

Das Jahresabonnement gilt für 4 Folgeausgaben ab Abo-Bestellung und verlängert sich jeweils um ein Jahr (d.h. um zusätzlich 4 Ausgabefolgen), wenn nicht gekündigt wird. Kündigung ist mit Ablauf des jeweiligen Jahresabo-Termins einen Monat vorher möglich.

ReVision erscheint quartalsweise
(jeweils Anfang Februar/Mai/August/November)

Kosten für ein Jahresabonnement: € 47,00 (inkl. 7% MwSt).

Bestell-Fax

Tel. +49 40 69 69 85-14 • Fax +49 40 69 69 85-31

Oder bestellen Sie online unter www.revision-hamburg.de

Hiermit bestelle ich das Journal ReVision im Jahresabonnement zum nächstmöglichen Zeitpunkt. Ein Jahresabonnement (4 Ausgaben) kostet € 47,00 inkl. 7% MwSt. Die Abo-Gebühren zahle ich

❑ nach Rechnungsstellung durch den Verlag.
❑ per Bankeinzug. Bitte belasten Sie fällige Beiträge:

Konto-Nr.: _____ BLZ: _____

Bank: _____ Kontoinhaber: _____

Falls ich nicht spätestens 1 Monat vor dem jeweiligen Beginn meines Jahresabonnements kündige, verlängert sich das Abonnement automatisch um ein weiteres Jahr.

Name: _____ Vorname: _____

Firma: _____ Telefon: _____

Abteilung: _____ eMail: _____

Straße: _____ PLZ/Ort: _____

Ort, Datum: _____ Unterschrift: _____