Interne Revision

Prüfen in SAP®

IT-Revision

Beilage: IBS-Prüfmanual "Mobile Sicherheit"

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:
OSV Ottokar Schreiber Verlag GmbH
eMail: sales@osv-hamburg.de

DTP-Produktion

Grafik/Illustration: Alexandra Palandrani, OSV Hamburg
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

PRev

August 2006

Redaktions-/ Einsendeschluss für diese Ausgabe:

17.07.2006

Beilagen dieser Ausgabe:

- IBS Schreiber GmbH "Jahresfachkonferenz Sicherheit und Prüfung von im Gesundheitswesen"
- IBS Schreiber GmbH "Roadshow 2006"
- IBS-Prüfmanual
- Datakontext Fachverlag "IKS-Management"

➲ Grundlagen und Ansätze der Internen Revision

Liebe Leserinnen und Leser,

bei vielen Prüfungen müssen wir leider feststellen, dass sich der Stellenwert der Internen Revision innerhalb ihrer jeweiligen Unternehmen in den letzten Jahren zwar gesteigert hat, aber von vielen Fachbereichen häufig doch zwiespältig betrachtet wird. Deshalb wird im folgenden Beitrag die Notwendigkeit - und daraus resultierend der hohe Stellenwert - der Internen Revision aus KonTraG (Gesetz zur Kontrolle und Transparenz von Unternehmen), DCGK (Deutscher Corporate Governance Kondex) und SOA (Sarbanes Oxley Act) abgeleitet. Alle Beteiligten, das sind der Vorstand, die Fachbereiche und die Interne Revision selber, sind in diesem Sinne gefordert!

Begründet aus der praktischen Prüfertätigkeit wird der Stellenwert der Internen Revision mit dem Prüfbericht. PRev stellt Ihnen in dieser Ausgabe alle relevanten Soll-Vorgaben für einen Prüfbericht nach IIR und IDW zusammen. Im Prüfbericht dokumentiert sich die - hoffentlich erfolgreiche - Tätigkeit der Internen Revision; er ist die "Visitenkarte" der Internen Revision! In PRev III wird dieses Thema fortgesetzt: "Der Prüfbericht als Prüfobjekt". Hier stellen wir formale, inhaltliche und stilistische Aspekte des Prüfberichts zur Diskussion.

Ich hoffe auf Ihr reges Interesse und auch auf Ihre Kritiken und Beiträge.

Ihr

Ottokar R. Schreiber

➲ Notwendigkeit der Internen Revision oder

Was wäre das Unternehmen ohne seine Interne Revision?

Dipl.-Ing.
Ottokar R. Schreiber
IBS Schreiber GmbH

Einführung

Seit KonTraG im Jahre 1998 und in verstärktem Masse befördert durch die Diskussion und Verabschiedung des DCGK (Deutscher Corporate Governance Kodex) und in diesem Sinne weiter verstärkt durch den SOA (Sarbanes Oxley Act) prägt sich die Interne Revision (IR) als die zentrale, im "Querschnitt" wirkende, interne Kontrollinstanz eines Unternehmens aus.

DCGK, KonTraG/AktG § 91 und SOA Section 406

Dass der Vorstand uneingeschränkt zum Wohle seines Unternehmens zu handeln und zu wirken hat, scheint kein Selbstverständnis zu sein. Denn im DCGK (Deutscher Corporate Governance Kodex), der keinen Gesetzescharakter hat, heißt es unter 4.1:

4.1.1 Der Vorstand leitet das Unternehmen in eigener Verantwortung. Er ist dabei an das Unternehmensinteresse gebunden und der Steigerung des nachhaltigen Unternehmenswertes verpflichtet.

4.1.2 Der Vorstand entwickelt die strategische Ausrichtung des Unternehmens, stimmt sie mit dem Aufsichtsrat ab und sorgt für ihre Umsetzung.

4.1.3 Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen zu sorgen und wirkt auf deren Beachtung durch die Konzernunternehmen hin.

4.1.4 Der Vorstand sorgt für ein angemessenes Risikomanagement und Risikocontrolling im Unternehmen.

Diese Vorgaben sind, um einen Informatik-Begriff zu benutzen, redundant, d.h. ohne Informationsgehalt und damit eigentlich überflüssig. Denn dass ein Vorstand

- das Unternehmen in eigener Verantwortung zu führen hat (s. AktG § 76 Abs 1),
- eine Unternehmensstrategie zu entwickeln hat und
- für die Beachtung (Einhaltung wäre fordernder und damit angemessener für Gesetze gewesen) der gesetzlichen Bestimmungen zu sorgen hat,

sind für jeden Kleinunternehmer und Handwerksmeister Selbstverständlichkeiten! Mit der letzten Forderung ergibt sich die Schnittstelle zum KonTraG (AktG § 91 Abs 2), in dem es heißt, der Vorstand einer Aktiengesellschaft ist verpflichtet, "geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden".

Gem. SOA Section 406 ist vom Vorstand und leitenden Angestellten ein "code of ethics" einzuhalten, nach dem ehrliches Verhalten, Beachtung gesetzlicher Vorschriften und korrekte Berichterstattung an die SEC (Securities and Exchange Commission) gefordert werden.

DCGK und SOA Section 302

Erst mit der direkten "Inverantwortungsnahme" des Vorstands für das Wohl und Wehe des eigenen Unternehmens ist dieser in der Bredouille, seine

Freiheitsgrade hinsichtlich "politischer" Entscheidungen, evtl. begründet in persönlicher Egomanie oder gar persönlicher Bereicherung, der Verantwortbarkeit von Risiken unterzuordnen: "Verletzen sie (Vorstand und Aufsichtsrat) die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters bzw. Aufsichtsratsmitglieds schuldhaft, so haften sie der Gesellschaft gegenüber auf Schadensersatz." (DCGK 3.8) SOA Section 302 geht noch einen Schritt weiter, indem CEO (Chief Executive Officer) und CFO (Chief Financial Officer) verpflichtet werden, eine eidesstattliche Erklärung (Certification) für periodisch bei der SEC eingereichte Berichte abzugeben.

Daraus leitet sich der gewachsene Stellenwert der Internen Revision im Unternehmen, der Kontrollinstanz des Vorstands, direkt ab, denn: Was wäre der Vorstand unter den Vorgaben von KonTraG, DCGK und SOA ohne seine Interne Revision?

- Er wäre auf die Aussagen und Berichte seiner Fachbereiche angewiesen (Self Assessment), und diese sind i.d.R. interessensgefärbt.
- Mängel und Fehler würden häufig erst durch die Abschlussprüfer aufgedeckt werden mit einem entsprechenden Überraschungswert für den verantwortlichen (!) Vorstand.
- Oder der Vorstand müsste externe Prüfer beauftragen, die einerseits keine Intimkenntnisse der Unternehmensphilosophie und der Unternehmensabläufe haben, und die andererseits Unternehmenswissen nach außen tragen könnten. "Outsourcen" der Internen Revision kann kein Ziel des Vorstands sein. Nach DCGK 4.3.2 "dürfen Vorstandsmitglieder und ihre Mitarbeiter im Zusammenhang mit ihrer Tätigkeit weder für sich noch für andere Personen von Dritten Zuwendungen oder sonstige Vorteile fordern oder annehmen oder Dritten ungerechtfertigte Vorteile gewähren." - Die engsten Mitarbeiter des Vorstands sollten die Internen Revisoren sein!

KonTraG/HGB § 317 und SOA Section 404

SOA Section 404 (management assessment of internal control) impliziert einen hohen Implementierungsaufwand für das Unternehmen; denn jeder Jahresbericht muss einen Bericht über das interne Kontrollsystem der Finanzberichterstattung enthalten. Deshalb muss durch entsprechend ausgeprägte Maßnahmen verhindert werden, dass mangelhafte Kontrollen und dadurch bedingte falsche und/oder unvollständige Informationen den Finanzbericht verfälschen.

Bei der Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91,2 AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann.

Dieser Ansatz korrespondiert mit KonTraG und den entsprechend angepassten HGB-Gesetzen § 317 ff.

§ 317 HGB (Gegenstand und Umfang der Prüfung)

> ....Dabei ist (vom Abschlussprüfer) auch zu prüfen, ob die Risiken der zukünftigen Entwicklung zutreffend dargestellt sind.

Bei der Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91,2 AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann.

§ 321 HGB (Prüfungsbericht)

> Der Abschlussprüfer hat über Art und Umfang sowie das Ergebnis der Prüfung schriftlich und mit der gebotenen Klarheit zu berichten .....
>
> In einem besonderen Abschnitt des Prüfungsberichtes sind Gegenstand, Art und Umfang der Prüfung zu erläutern.
>
> Ist im Rahmen der Prüfung eine Beurteilung nach § 317, Abs. 4 abgegeben worden, so ist deren Ergebnis in einem besonderen Teil des Prüfungsberichtes darzustellen. Es ist darauf einzugehen, ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern.

§ 322 HGB (Bestätigungsvermerk) Auf Risiken, die den Fortbestand des Unternehmens gefährden, ist gesondert einzugehen.

> ...Dabei ist darauf einzugehen, ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind.

In den zahlreichen von SOA Section 404 und KonTraG/HGB § 317 ff getriebenen Projekten in den Unternehmen ist die Interne Revision "ex ante" als Projektrevision umfassend gefordert! Da fast alle Unternehmensbereiche und -prozesse IT-gestützt betrieben werden, ist bei diesen Projekten neben dem "Financial Auditing" insbesondere die IT-Revision gefordert. (siehe hierzu auch GoBS des AWV und PS 330 des IDW)

IKS

Zusammengefasst summieren sich alle Sicherheitsregularien eines Unternehmens im IKS (Internes Kontrollsystem), das vom AWV (Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.), vom IDW (Institut der Wirtschaftsprüfer in Deutschland e.V.) und von AIA (American Institute of Accountants) in entsprechenden Prüfungsstandards beschrieben wird:

GoBS (AWV) definiert*:*

Als IKS wird grundsätzlich die Gesamtheit aller aufeinander abgestimmten und miteinander verbundenen Kontrollen, Maßnahmen und Regelungen bezeichnet, die folgende Aufgaben haben:

- Sicherung und Schutz vorhandenen Vermögens und vorhandener Informationen Bereitstellung vollständiger, genauer und aussagefähiger sowie zeitnaher Aufzeichnungen
- Förderung der betrieblichen Effizienz
- Unterstützung der Befolgung der vorgeschriebenen Geschäftspolitik

IDW PS 260 Das Interne Kontrollsystem im Rahmen der Abschlussprüfung definiert*:*

Unter einem Internen Kontrollsystem werden die von der Unternehmensleitung im Unternehmen eingeführten Grundsätze, Verfahren und Maßnahmen (Regelungen) verstanden, die gerichtet sind auf die organisatorische Umsetzung der Entscheidungen der Unternehmensleitung

...unter der Zielsetzung einer permanenten Verbesserung des IKS subsummiert sich das Handeln der Internen Revision!

- zur Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftstätigkeit,
- zur Ordnungsmäßigkeit und Verlässlichkeit der internen und externen Rechnungslegung sowie
- zur Einhaltung der für das Unternehmen maßgeblichen rechtlichen Vorschriften.

AIA American Institute of Accountants definiert*:*

Das Interne Kontrollsystem umfasst sowohl den Organisationsplan als auch sämtliche aufeinander abgestimmte Methoden und Maßnahmen in einem Unternehmen, die dazu dienen, sein Vermögen zu sichern, die Genauigkeit und Zuverlässigkeit der Abrechnungsdaten zu gewährleisten und die Einhaltung der vorgeschriebenen Geschäftspolitik zu unterstützen.

Fazit für die Interne Revision

Unter der Zielsetzung einer permanenten Verbesserung des IKS subsummiert sich das Handeln der Internen Revision!

Die moderne Revision ist effizient aufgestellt, weil sie risiko-orientiert und deshalb proaktiv tätig ist. Auch die neben "ex ante"-Prüfungen nach wie vor geforderten "ex post"-Prüfungen wirken zukunftsorientiert in der permanenten Verbesserung des IKS mit der Zielsetzung, dolose und dolorose Handlungen auf ein Minimum zu reduzieren. Die plötzlich wieder aktuell aufflackernde "Fraud"-Diskussion, u.a. initiiert durch SOA Abschnitt VIII (Corporate and Criminal Fraud Accountability), sollte durch die effektive Tätigkeit der IR wieder auf ein Normalmaß relativiert werden.

Eine so aufgestellte und agierende Interne Revision muss auch vom eigenen Vorstand gewollt sein. In diesem Sinne stellen der Stellenwert und die Ausprägung der IR, weil direkt implementiert und sanktioniert durch den Vorstand selber, ein Spiegelbild eben dieses Vorstands dar! ✤

➲ Berichterstattung der Internen Revision

Im Prüfbericht mündet die Arbeit des Revisors. Er stellt implizit den gesamten Prüfprozeß dar, beginnend

- mit dem dedizierten Prüfthema über
- die Erhebung der Soll-Vorgaben (beschreibend das normierte Objekt) und über
- die Erhebung des Ist-Zustandes des Prüfobjekts bis hin zur
- Bewertung des festgestellten (gemessenen) Deltas (Mängel) und
- Aussprache von Empfehlungen.

Das heißt der Prüfbericht des Revisors ist ein Ergebnisbericht der jeweiligen Prüfung mit dem Ziel,

- Schwachstellen des Unternehmens aufzuzeigen (Feststellungen),
- diese risiko-orientiert zu bewerten und
- Empfehlungen zu ihrer Eliminierung oder zumindest Minimierung aufzuzeigen (nach dem Verhältnismäßigkeitsprinzip).

Adressat des Prüfberichts sind der Auftraggeber, d.h. der Vorstand bzw. die Geschäftsführung und der geprüfte Fachbereich. Insofern gliedern sich die "Kunden" der Internen Revision in diese beiden Kategorien und der Bericht ist jeweils empfängerorientiert abzufassen.

Dieser Beitrag zur Berichterstattung besteht aus 2 Teilen: Im ersten Teil in dieser Ausgabe von PRev (Ausgabe II/06) werden relevante Soll-Vorgaben aus Gesetzen, Verlautbarungen und Prüfungsstandards für die Berichterstattung zusammenfassend zitiert.

Im zweiten Teil (erscheint in PRev III/06) werden aus der formellen und inhaltlichen (materiellen) Berichtskritik konkrete Vorschläge zur Berichterstattung abgeleitet.

Insofern stellt sich in diesem Beitrag der Prüfbericht selber als Prüfobjekt dar!

Die Soll-Vorgaben zur Berichterstellung nach IDW und IIR

Grundforderung

Jeder Prüfbericht hat über das Ergebnis der Prüfung

- unparteiisch,
- vollständig,
- wahrheitsgetreu und
- mit der gebotenen Klarheit

schriftlich zu berichten.

Entsprechend deklarieren die Grundlagen des Prüfungsberichtes (aus WP-Handbuch Seite 899 ff) im Abschnitt "Allgemeine Berichtsgrundsätze" § 321 HGB wie folgt:

Grundsatz der Unparteilichkeit
Wertungen positiver oder negativer Art sind zulässig und erforderlich. Der Prüfer hat sich aber jeder einseitigen oder persönlich wirkenden Kritik zu enthalten.

Grundsatz der Vollständigkeit
Es ist über wesentliche Tatsachen zu berichten, die die Prüfung erbracht hat. Wesentlich sind solche

Tatsachen, die für eine ausreichende Information der Berichtsempfänger von Bedeutung sind.

Zum Umfang: bei der Abfassung der Berichte und bei der Festlegung des Umfanges der Berichterstattung wird es im Einzelfall erforderlich sein, die Struktur des Empfängerkreises des Berichtes nicht unberücksichtigt zu lassen. Über Sachverhalte, deren Ordnungsmäßigkeit festgestellt wird, ist nur knapp zu berichten. Problematische oder zu beanstandende Sachverhalte sind ausführlicher darzulegen.

Grundsatz der Wahrheit
Dieser Grundsatz wird verletzt, wenn wesentliche Tatsachen weggelassen werden. Meinungsverschiedenheiten über die Würdigung eines Sachverhaltes sind zum Ausdruck zu bringen. Der Bericht darf nicht den Eindruck erwecken, dass der Sachverhalt geprüft wurde, obwohl seine Prüfung (noch) nicht möglich war.

Grundsatz der Klarheit
Gefordert wird eine verständliche und eindeutige Darlegung der Sachverhalte. Der Bericht sollte sich durch eine übersichtliche Gliederung, einfachen und sachlichen Stil auszeichnen. Nicht allgemein geläufige Fachausdrücke, wenig gebräuchliche Fremdwörter und Abkürzungen sollten vermieden werden. Umfangreiche Zusammenstellungen und Zahlentabellen als Anlagen beifügen.

Berichterstattung zur Buchführung
Über bereits behobene Mängel wird dann nicht zu berichten sein, wenn es sich um zufällige Fehler aufgrund menschlicher Unzulänglichkeiten und nicht ausschaltbarer Irrtümer handelt. Das gilt nicht für gewichtige Mängel, die auf organisatorische Schwächen hindeuten.

Es ist stets über festgestellte gravierende Mängel des Internen Kontrollsystems zu berichten. Dies gilt auch dann, wenn die festgestellten Mängel des Systems (noch) zu keinem Fehler geführt haben, aber zu einem Fehler führen können.

Berichterstattung zu negativen Unternehmenssachverhalten
Eine schriftliche Warnpflicht ist schon dann gegeben, wenn sich die Unternehmenslage zum Schlechten wendet oder wenn selbst bei einer positiven Ertragslage bedeutende Verlustquellen des Unternehmens festgestellt werden.

Weitere Kriterien für den Prüfbericht (Soll-Vorgaben) ergeben sich aus

- KonTraG/HGB 321/PS 350 (IDW)
- PS 450 (IDW)
- IIR Revisionsstandard Nr. 3

KonTraG

Nach dem KonTraG sind Vorstände von börsennotierten Aktiengesellschaften verpflichtet, "geeignete Maßnahmen" zu treffen, insbesondere ein Überwachungssystem einzurichten, damit der Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden". (§ 91 (2) AktG)

§ 111 AktG (Aufgaben und Rechte des Aufsichtsrates)
Der Aufsichtsrat hat die Geschäftsführung zu überwachen.
..... Der Aufsichtsrat erteilt dem Abschlussprüfer den Prüfungsauftrag für den Jahresabschluss gemäß § 290 HGB.

§ 317 HGB (Gegenstand und Umfang der Prüfung)
...
..... Dabei ist (vom Abschlussprüfer) auch zu prüfen, ob die Risiken der zukünftigen Entwicklung zutreffend dargestellt sind.
...

Bei der Aktiengesellschaft, die Aktien mit amtlicher Notierung ausgegeben hat, ist außerdem im Rahmen der Prüfung zu beurteilen, ob der Vorstand die ihm nach § 91,2 AktG obliegenden Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgabe erfüllen kann.

§ 321 HGB (Prüfungsbericht)

Der Abschlussprüfer hat über Art und Umfang sowie das Ergebnis der Prüfung schriftlich und mit der gebotenen Klarheit zu berichten .....

In einem besonderen Abschnitt des Prüfungsberichtes sind Gegenstand, Art und Umfang der Prüfung zu erläutern.

Ist im Rahmen der Prüfung eine Beurteilung nach § 317, Abs. 4 abgegeben worden, so ist deren Ergebnis

in einem besonderen Teil des Prüfungsberichtes herzustellen. Es ist darauf einzugehen, ob Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern.

§ 322 HGB (Bestätigungsvermerk)

..... Der Bestätigungsvermerk hat neben einer Beschreibung von Gegenstand, Art und Umfang der Prüfung auch eine Beurteilung des Prüfungsergebnisses zu enthalten.

Die Beurteilung des Prüfungsergebnisses soll allgemeinverständlich und problemorientiert ... erfolgen. ..... Auf Risiken, die den Fortbestand des Unternehmens gefährden, ist gesondert einzugehen.

...Dabei ist darauf einzugehen, ob die Risiken der künftigen Entwicklung zutreffend dargestellt sind.

Prüfungsstandard 350 (IDW) "Prüfung des Lageberichts"

In Kap. 6.1 heißt es:

(21) Gemäß § 321 Abs. 2 Satz 1 und 2 HGB ist im Prüfungsbericht darzustellen, ob der Lagebericht den gesetzlichen Vorschriften und den ergänzenden Bestimmungen des Gesellschaftsvertrags oder der Satzung entspricht. Die für die Aussagen des Lageberichts bedeutenden Annahmen und übrigen Prognoseelemente sind darzustellen und zu würdigen. Entspricht der Lagebericht nach dem Urteil des Abschlussprüfers nicht den gesetzlichen uns gesellschaftsvertraglichen bzw. satzungsmäßigen Bestimmungen, muß der Abschlussprüfer auf diese Mängel im Prüfungsbericht hinweisen, selbst wenn diese Beanstandungen noch nicht zu einer Einschränkung des Bestätigungsvermerks führen.

(22) Auch wenn der Lagebericht den Anforderungen des § 289 HGB entspricht und daher eine ausreichende Lagedarstellung enthält, verlangt § 321 Abs. 1 Satz 2 HGB, dass der Abschlussprüfer zu der Beurteilung der Lage des Unternehmens durch die gesetzlichen Vertreter Stellung zu nehmen hat, wobei insbesondere auf die Beurteilung des Fortbestands und der künftigen Entwicklung des Unternehmens unter Berücksichtigung des Lageberichts einzugehen ist, soweit die geprüften Unterlagen und der Lagebericht eine solche Beurteilung erlauben. Außerdem ist nach § 321 Abs. 1 Satz 3 HGB darzustellen, ob bei Durchführung der Prüfung Unrichtigkeiten oder Verstöße gegen gesetzliche Vorschriften sowie Tatsachen festgestellt worden sind, die den Bestand des geprüften Unternehmens gefährden oder seine Entwicklung wesentlich beeinträchtigen. Der Abschlussprüfer hat seinen Feststellungen zur Beurteilung der Lage durch die gesetzlichen Vertreter erforderlichenfalls eigene Akzente zu setzen und auf ihm wesentlich erscheinende Punkte ggf. ausführlicher einzugehen, als dies im zu veröffentlichenden Lagebericht gefordert werden muß.

Bestätigungsvermerk

(23) Mit dem uneingeschränkten Bestätigungsvermerk wird in Zusammenfassung der sich aus den §§ 317, 321 und 322 HGB zu treffenden Prüfungsfeststellungen zum Ausdruck gebracht, dass der Lagebericht insgesamt nach der Beurteilung des Abschlussprüfers eine zutreffende Vorstellung von der Lage des Unternehmens vermittelt sowie dass die Risiken der künftigen Entwicklung zutreffend dargestellt sind.

(24) Unabhängig davon, ob der Lagebericht eine ausreichende Darstellung ggf. bestehender bestandsgefährdender Risiken enthält, hat der Abschlussprüfer nach § 322 Abs. 2 Satz 2 HGB auf den Fortbestand gefährdende, im Rahmen der Prüfung festgestellte Risiken in dem Bestätigungsvermerk gesondert einzugehen.

(25) Für den Fall, dass der Abschlussprüfer seine Beurteilung von (wesentlichen) prognostischen Aussagen im Lagebericht weitgehend nur auf Erklärungen der Geschäftsführung stützen kann, ist hierauf im Rahmen der Beurteilung des Prüfungsergebnisses nach § 322 Abs. 1 Satz 2 HGB einzugehen.

(26) Der Bestätigungsvermerk ist im Hinblick auf den Lagebericht einzuschränken, wenn Einwendungen zu erheben sind. Dies kann beispielsweise der Fall sein, wenn ein Lagebericht entgegen der gesetzlichen Verpflichtung nicht erstellt wurde, wenn wesentliche Informationselemente (z.B. Angaben zur künftigen Entwicklung, Schlusserklärung zum Abhängigkeits-

bericht nach § 312 Abs. 3 AktG) im Lagebericht fehlen oder im Widerspruch zu den geprüften Unterlagen stehen, wenn der Abschlussprüfer eine wesentliche prognostische Aussage nicht für plausibel hält oder wenn der Abschlussprüfer bestimmte Sachverhalte nicht beurteilen kann.
Zur Einschränkung von Bestätigungsvermerken aufgrund von Mängeln im Lagebericht enthält der IDW Prüfungsstandard: Grundsätze für die ordnungsmäßige Erteilung von Bestätigungsvermerken bei Abschlußprüfungen (IDW PS 400) ergänzende Anforderungen und Formulierungen.

PS 450 (IDW) "Grundsätze ordungsmäßiger Berichterstattung bei Abschlußprüfung"

Hieraus ergeben sich als allgemeine Grundsätze (Attribute) für die Erstellung eine Prüfberichtes:
- gewissenhaft
- wahrheitsgetreu
- tatsächliche Gegebenheiten
- vollständig
- unparteiisch
- verständliche, eindeutige und problemorientierte Darlegung
- übersichtliche Gliederung des Prüfberichts

Unter Berücksichtigung der gesetzlichen Vorgaben wird empfohlen, den Prüfbericht entsprechend den nachfolgend aufgeführten Abschnitten und Bezeichnungen zu gliedern.
- Prüfungsauftrag
- Grundsätzliche Feststellungen
- Gegenstand, Art und Umfang der Prüfung
- Feststellungen und Erläuterungen zur Rechnungslegung
- Feststellungen und Risikofrüherkennungssystem
- Feststellung aus Erweiterungen des Prüfungsauftrags
- Bestätigungsvermerk

Der Prüfungsbericht ist so abzufassen, dass er von den jeweiligen Adressaten des Prüfungsberichts verstanden werden kann. Er ist als einheitliches Ganzes anzusehen.

Der Abschlussprüfer hat im Prüfungsbericht vorweg zur Beurteilung der Lage des Unternehmens durch die gesetzlichen Vertreter Stellung zu nehmen.

Weiterhin hat er darzustellen, ob er bei Durchführung der Abschlussprüfung Tatsachen festgestellt hat, welche die Entwicklung des geprüften Unternehmens wesentlich beeinträchtigen.

Wird die Lagebeurteilung der gesetzlichen Vertreter vom Abschlussprüfer als nicht vertretbar beurteilt, so ist dies im Prüfungsbericht zu erläutern.

Nach § 321 Abs. 1 Satz 3 HGB hat der Abschlussprüfer darzustellen, ob er bei Durchführung der Abschlussprüfung einzelne Tatsachen festgestellt hat, welche die Entwicklung des geprüften Unternehmens wesentlich beeinträchtigen oder seinen Bestand gefährden können.
- Entwicklungsbeeinträchtigung
- Gefährdung des Unternehmensfortbestand

In Einzelfällen kann es notwendig sein, aus Gründen der Eilbedürftigkeit erforderlicher Gegenmaßnahmen vorweg einen gesonderten Teilbericht zu erstatten.

Der Abschlussprüfer hat darüber zu berichten ob Unrichtigkeiten oder Verstöße gegen gesetzliche Vorschriften sowie Tatsachen festgestellt wurden, die schwerwiegende Verstöße von gesetzlichen Vertretern oder von Arbeitnehmern gegen Gesetz, Gesellschaftsvertrag oder Satzung darstellen.
- Negativfeststellung

Der Abschlussprüfer hat die Grundzüge seines jeweiligen Prüfungsvorgehen darzustellen.

Zu den berichtspflichtigen Prüfungsinhalten gehören:
- Prüfungsstrategie
- Prüfungsschwerpunkte
- rechnungslegungsbezogene interne Kontrollsysteme
- stichprobengestütztes Prüfungsverfahren
- Auswirkungen aus dem Vorjahresabschluss auf die Prüfungsdurchführung
- Bestätigungen Dritter
- Untersuchungen Dritter (z.B. Wertgutachten, Ergebnisse der Internen Revision)
- Besonderheiten der Prüfung des Inventars
- Organisatorische Umstellungen

Der Abschlussprüfer hat über festgestellte wesentliche Mängel in den nicht auf den Jahresabschluss

oder Lagebericht bezogenen Bereichen des internen Kontrollsystems zu berichten.

Es ist auszuführen
- ob der Vorstand ein Überwachungssystem in geeigneter Form eingerichtet hat
- ob Maßnahmen erforderlich sind, um das Risikofrüherkennungssystem zu verbessern

Einzelheiten zur Prüfung des Risikofrüherkennungssystems enthält der IDW Prüfungsstandard "Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB".
- gesonderter Abschnitt des Prüfungsberichts
- funktionsfähiges Risikofrüherkennungssystem
- Formulierung im Prüfungsbericht

"Unsere Prüfung hat ergeben, dass der Vorstand die nach § 91 Abs. 2 AktG geforderten Maßnahmen insbesondere zur Einrichtung eines Überwachungssystems in geeigneter Weise getroffen hat und dass das Überwachungssystem geeignet ist, Entwicklungen, die den Fortbestand der Gesellschaft gefährden, frühzeitig zu erkennen."

Ist das Risikofrüherkennungssystem nicht dazu geeignet, hat der Abschlussprüfer dies festzustellen, konkrete Verbesserungsvorschläge sind nicht Gegenstand der Berichterstattungspflicht. Hat der Vorstand kein Risikofrüherkennungssystem eingerichtet, ist hierauf hinzuweisen.

IIR Revisionsstandard Nr. 3 "Qualitätsmanagement in der Internen Revision"

Hier heißt es in Kap. 3.5.2.3 Berichterstattung: Inhalt, Sprache und Form der Berichte sind ein wesentliches Merkmal der Qualität einer Internen Revision.

Der Inhalt und die Sprache müssen den Grundsätzen der Vollständigkeit, der Wahrheit und der Klarheit entsprechen. In dem Begriff Wahrheit ist die Objektivität enthalten.

Alle Berichte müssen zumindest Aussagen enthalten zu:
- Prüfungsziel und -umfang
- Auftragsdurchführung
- Prüfungsobjekt
- Prüfungsergebnis
- Maßnahmen/Empfehlungen (incl. Verantwortlichkeiten, Realisierungsdatum und Priorisierung)

Die Form der Berichte einer Internen Revision ist zu standardisieren, um dem Adressaten die Orientierung zu erleichtern. Die Berichterstattung erfolgt knapp und zeitnah.

Grundlagen der Internen Revision/Basics of Internal Auditing (IIR/IIA)

Standard 2400 - Berichterstattung

Hier heißt es u.a.:
Interne Revisoren sollten mit der gebotenen Vorsicht vorgehen, wenn sie Ergebnisse und Stellungnahmen in die Berichterstattung und Arbeitspapiere aufnehmen, die sich auf Verstöße gegen Gesetze und aufsichtsrechtliche Bestimmungen oder andere rechtliche Fragen beziehen.

Interne Revisoren müssen Nachweise zusammenstellen, analytische Urteile abgeben, über Ergebnisse berichten und sicherstellen, dass korrigierende Maßnahmen eingeleitet werden.

Standard 2410 - Berichterstattungskriterien

Hier heißt es u.a.:
Obwohl Format und Inhalt der Schlussberichte je nach Organisation oder Art des Auftrags variieren können, müssen sie doch zumindest Zweck, Umfang und Ergebnisse des Auftrags enthalten.

Schlussberichte können auch Hintergrundinformationen und Zusammenfassungen enthalten.

Zu den Ergebnissen gehören Feststellungen, Schlussfolgerungen, Beurteilungen, Empfehlungen und Maßnahmenpläne.

Feststellungen sind sachdienliche Tatsachenbeschreibungen.

Feststellungen und Empfehlungen entstehen durch einen Soll/Ist-Vergleich. Falls bei diesem eine Diskrepanz besteht, hat der Interne Revisor eine Basis, auf der er den Bericht aufbauen kann. Wenn

die Gegebenheiten mit den Kriterien übereinstimmen, kann die Anerkennung einer zufrieden stellenden Leistung im Revisionsbericht gerechtfertigt sein.

Die Ansicht der geprüften Einheiten zu den Schlussfolgerungen, Beurteilungen oder Empfehlungen können in den Revisionsbericht aufgenommen werden.

Abschließendes

So viel zu den bestehenden Vorgaben an eine Berichterstellung von Seiten der beiden Institutionen der Internen Revision (IIR) und - wesentlich ausführlicher - der externen Prüfer/Wirtschaftsprüfer (IDW).

Zu ergänzen sind diese grundsätzlich formulierten Vorgaben durch betriebsinterne Regeln zur Dokumentation der Prüfberichte:

- Aufbewahrungsfristen
- Datenbank-basierte Strukturierung und Recherchemöglichkeiten nach
  - Prüfthema
  - Prüfzeitpunkt
  - Prüfer
  - u.a.m.

  mit entsprechendem Deckblatt.

Fortsetzung
2. Teil: Formelle und materielle Berichtskritik ✤

➲ Prüfen in SAP®

Liebe Leserinnen und Leser,

"Remote"-Zugriffe, d.h. Zugriffe von außen auf IT-Systeme, sind ein altes ambivalentes Diskussionsthema in der IT. Einerseits wurde der "Remote"-Zugriff erfunden, um effiziente Fernwartung und -support der IT-Systeme zu ermöglichen, andererseits handelt man sich damit erhebliche Sicherheitsrisiken ein.

Auch auf SAP-Systeme wird i.d.R. über die als Standard ausgeprägte RFC-Schnittstelle zugegriffen, mit allen Vor- und Nachteilen. Die diesbezüglichen Risiken, ihre Prüfung und Empfehlungen zur Minimierung dieser Risiken stehen im Fokus des folgenden Beitrags von Christoph Wildensee.

SAP BW bzw. BI stehen in steigendem Masse in zahlreichen Unternehmen zur Disposition. Die Revision ist deshalb gut beraten, sich mit diesem komplexen Modul rechtzeitig auseinander zu setzen. In dieser Ausgabe von PRev wird von Claus-Dieter Lillich das diesbezügliche Thema mit der Vorstellung der speziellen Berechtigungsobjekte fortgesetzt und in den Folgebeiträgen mit Prüfansätzen vertieft werden.

Viel Freude in der weiteren Vermehrung Ihres SAP-Prüferwissens wünscht Ihnen

Ihr

Thomas Tiede

➲ Externer Zugriff auf SAP® Systeme über RFC

Dipl.-Betriebswirt
Christoph Wildensee
CISM, CIFI, Hannover

Einleitung

Der ‚Remote Function Call' (RFC) bildet die Grundlage für die Integration mehrerer SAP-Systeme, aber auch die bidirektionale Anbindungsmöglichkeit weiterer Systeme mit entsprechender Datenversorgung. Somit bietet diese Technik des entfernten Funktionsaufrufes als Standardschnittstelle die Möglichkeit, Funktionsbausteine in entfernten SAP-Systemen auszuführen - Funktionen und Daten werden für die Verwendung in und aus anderen Systemen verfügbar gemacht. Über RFC wird auch die Kommunikation mit anderen Mandanten desselben Systems hergestellt.

Standardmäßig sind in jedem SAP-System bereits RFC-Verbindungen vorhanden, z.B. für das Transport Management System und die Verbindungen zu allen Applikationsservern. Hinzu kommen naturgemäß die Konsolidierungsverbindungen zwischen den Systemen untereinander wie z.B. IS-U und Classic sowie HR und Classic, sofern die Systeme getrennt gefahren werden.

Risiken

Der Mechanismus des Datenzugriffs in SAP-Systemen ist zweigeteilt. Zum einen wird die Transaktion, d.h. der Aufruf des SAP-Programmpaketes, das einen Arbeitsabschnitt eines Prozesses darstellt, geschützt. Zum anderen werden die Zugriffe auf die eigentlichen Schlüsselinformationen und zumeist der damit verbundene Manipulationsgrad innerhalb der Transaktion über Berechtigungsobjekte gesteuert. Das Gewähren einer Transaktion bedeutet somit nur in Kombination mit den ausgeprägten Berechtigungsobjekten, dass der betriebswirtschaftliche Ablauf mit entsprechenden Daten in SAP vollständig ausgeführt werden kann.

Die Ausprägung der Berechtigungen in den SAP-Systemen erfolgt auf Transaktionsebene üblicherweise restriktiv, während auf Berechtigungsobjektebene meist aus Gründen der Administrationsentlastung durchaus eine "Überversorgung" anzutreffen ist. Ging man bisher davon aus, dass ein Ausnutzen der höheren Rechte nicht möglich ist, wenn Transaktionen nicht gewährt werden, ergibt sich - dies gilt sowohl in den Fachmodulen als auch auf Customizing- und Entwicklungsebene, d.h. dem Entwickeln und Ausführen von Quellcode - über die Nutzungsmöglichkeit externer Connectoren ein anderes Bild. Es ist häufig einer Vielzahl von Mitarbeitern möglich, über die Nutzung der RFC-Schnittstelle und externer Zugriffsprogramme, die frei verfügbar sind, uneingeschränkt auf SAP-Tabellen Zugriff zu nehmen, ohne dabei die Transaktionsberechtigungen innerhalb der Berechtigungsstämme aufzuweisen. Darüber hinaus sind häufig nicht nur uneingeschränkte Lesezugriffe möglich, es kann auch unprotokolliert über RFC ABAP-Quellcode zur Ausführung gebracht werden. Dies sind erhebliche Sicherheitslücken, die es zu schließen oder zumindest sinnvoll zu handhaben gilt.

Gegen die pauschale Unterstellung eines solchen Vorgehens durch Mitarbeiter wird sich jeder verwahren, insbesondere in den als kritisch erachteten SAP-

(Neben)Buchhaltungssystemen sind solche Möglichkeiten jedoch durch die gesetzeskonforme Ausgestaltungsnotwendigkeit und der unzureichenden Protokollierung ausgesprochen prekär. Ich erinnere an dieser Stelle gern an die Problematik des Tabellen-Debuggings und der Nutzung der Replace-Funktion.

Grundlagen

Generell werden RFC-Anmeldungen nicht protokolliert. Über das AuditLog (SM19) besteht die Möglichkeit, erfolgreiche und gescheiterte RFC-Verbindungszugriffe und Funktionsbausteinaufrufe zu protokollieren und über die SAPLogHistorie auszuwerten (s. Tabelle USOBT => SM19 = S_ADMI_FCD mit AUDA und AUDD).

Die zugrunde liegenden Berechtigungen sehen wie folgt aus:

Verwalten von RFC-Verbindungen:

Objekt	notwendige Eingrenzung	
S_TCODE	TCD:	SM59
S_ADMI_FCD	Funktion:	NADM

Aufruf von Funktionsbausteinen:

Objekt	notwendige Eingrenzung	
S_RFC	Aktivität:	16 (Ausführen)
	RFC-Typ:	FUGR (Funktionsgruppe)
	RFC-Name:	<Name der RFC-Funktions gruppe>

Der relevante Systemparameter über RSPARAM / RSPFPAR ist AUTH / RFC_AUTHORITY_CHECK (= 1 [0=keine Prüfung im System], System-Default=1).

SAP® stellt spezifische Funktionsbausteine zur Verfügung, die mittels externer Programmzugriffe aufgerufen werden können. Diese können Tabelleninhalte zurückgeben oder auch ABAP-Quellcode enthalten, die im Zielsystem ohne dezidierte Detail-Protokollierung ausgeführt wird. Es existieren ca. 200.000 Funktionsbausteine und BAPI's, von denen etwa 15.000 remotefähig, d.h. über RFC aufrufbar, sind (TFDIR / TFTIT, ENLFDIR).

Funktionsbausteine sind in Funktionsgruppen zusammengefasst. Sofern einem Benutzer die Berechtigung auf S_RFC mit Aktivität = 16, RFC-Objekt = FUGR und einer Eingrenzung in der Funktionsgruppe (RFC_NAME) zugewiesen wurde, kann er über RFC auf alle Funktionsbausteine der Funktionsgruppe zugreifen.

Ein Beispiel für einen problematischen Baustein ist RFC_ABAP_INSTALL_AND_RUN der Funktionsgruppe SUTL. Mit diesem ist es möglich, einen beliebigen externen Quellcode im Zielsystem auszuführen. So kann auch ein Quellcode übergeben werden, der Daten manipuliert. Diese Berechtigung kann also zum Verstoß gegen § 239 (Radierverbot) und §257 HGB (Aufbewahrung von Unterlagen - Verfahrensdokumentation) genutzt werden.

Ausführen von Quellcode im Zielsystem:

Objekt	notwendige Eingrenzung	
S_RFC	Aktivität:	16 (Ausführen)
	RFC-Typ:	FUGR (Funktionsgruppe)
	RFC-Name:	SYST, SYSU, SRFC und SUTL
S_ADMI_FCD	Funktion:	MEMO (Speicherverwaltung)
S_DEVELOP	Aktivität:	03 (Anzeigen)
	Objekttyp:	PROG (ABAP-Programm)

Für den uneingeschränkten Lesezugriff sind erheblich geringere Berechtigungen als zum unprotokollierten Ausführen von Quellcode notwendig (z.B. FuBa: RFC_READ_TABLE; GET_TABLE_RFC; TABLE_ENTRIES_GET_VIA_RFC).

Die hier problematischen Funktionsgruppen sind somit BDCH, SYSE, SYSU, SYST, SRFC, SR1T, SRTT, SDTX und SUTL, da externe Programme üblicherweise mit den hier enthaltenen Funktionsbausteinen Zugriffe definieren, Stati abfragen und Datenaustausch betreiben...

Uneingeschränkter Lesezugriff:

Objekt	notwendige Eingrenzung	
S_RFC	Aktivität:	16 (Ausführen)
	RFC-Typ:	FUGR (Funktionsgruppe)
	RFC-Name:	SYSE, SYST, SYSU, SRFC und SDTX / SR1T / SRTT / BDCH
S_TABU_DIS	Aktivität:	03 (Anzeigen)
	Berecht.gruppe:	alle bzw. als kritisch erkannte, z.B. aus FI oder HR

Die hier problematischen Funktionsgruppen sind somit BDCH, SYSE, SYSU, SYST, SRFC, SR1T, SRTT, SDTX und SUTL, da externe Programme üblicherweise mit den hier enthaltenen Funktionsbausteinen Zugriffe definieren, Stati abfragen und Datenaustausch betreiben (siehe SE37; Berechtigung zur Anzeige von Informationen aus dem Data Dictionary: RFC1, SDIF*, SG00, SYST und SYSU).

Funktionsgruppe	Kurztext Funktionsgruppe
Name des Funktionsbausteins	Kurztext zum Funktionsbaustein
SYST	System-Interface
ABAP4_LEAVE_TO_TRANSACTION	Fuehrt den ABAP/4-Sprachbefehl LEAVE TO TRANSACTION aus.
RFCPING	RFC-Ping
RFC_TCPIP_CONNECTION_OPEN	Dyn. Verbindung zu RFC-Serverprogramm
SYSTEM_ATTACH_GUI	Startet SAPGUI und verbindet es mit dem aktuellen Modus (interne Verw.
SYSTEM_FORMAT	Bestimmen der Codepage und des Zahlenformats
SYSTEM_GET_UNIQUE_ID	Erzeugt eine eindeutige ID (obsolet -> SYSTEM_UUID_C_CREATE verwenden)
SYSTEM_HOOK_OPEN_DATASET	Hook für OPEN DATASET
SYSTEM_INFO	Auslesen von System-Informationen
SYSTEM_REMOTE_LOGIN	Remote Login
SYSTEM_UUID_CREATE	Erzeugt eine UUID im X-Format
SYSTEM_UUID_C_CREATE	Erzeugt UUID im Character-Format
TABLE_COMPRESS	Interne Tabelle komprimieren
TABLE_DECOMPRESS	IInterne Tabelle dekomprimieren
SRFC	RFC-Verwaltung
RFC_GET_LOCAL_DESTINATIONS	Liefert alle momentan aktiven RFC-Destinations an derselben Datenbank
RFC_GET_LOCAL_SERVERS	Liefert alle momentan aktiven RFC-Destinations an derselben Datenbank
RFC_LOGIN	expliziter Login eines Users.
RFC_PING	RFC-Ping
RFC_PUT_CODEPAGE	Lädt Codepagefile <frompage><topage>.CDP auf Harddisk
RFC_SYSTEM_INFO	Liefert versch. Informationen über das System.
SYSTEM_INVISIBLE_GUI	Lässt aktuellen GUI unsichtbar (interne Verwendung)
SYSTEM_RFC_VERSION_3_INIT	Initialisiert ein RFC-Verbindung auf dem Server (systeminterne Verwend
SDTX	Desktop Access
RFC_READ_TABLE	External access to R/3 tables via RFC
SUTL	Utilities
RFC_ABAP_INSTALL_AND_RUN	Installation und Ausführung eines ABAP/4
SYSU	RFC resource administration
SYSTEM_RESET_RFC_CONNECTION	Free all resources for RFC connection
SYSTEM_RESET_RFC_SERVER	Free all resources for RFC server
BDCH	ALE-Konsistenzprüfungen
CONTROL_DATA_OBJECT_CHECK	Prüfung für Steuerdatenobjekt
MESSAGE_CHECK_TECHNICAL_DATA	Prüfung der technischen Einstellungen für Nachrichtentyp
OBJECT_GET_ENTITY_TABLES	Ermittlung der Entitätstabellen für Steuerdatenobjekt
OBJECT_MODELLING_CHECK	Prüfung der Modellierung für Steuerdatenobjekt
PARTNER_LOGICAL_SYSTEM_GET	Logisches System des Partnersystems holen
TABLE_ENTRIES_GET_VIA_RFC	Tabelleneinträge aus einem anderen System über RFC holen
TABLE_GET_CONTROL_DATA_OBJECTS	Ermittlung der Steuerdatenobjekte für eine Tabelle
TABLE_GET_PRIMARY_OBJECTS	Ermittlung der primären Steuerdatenobjekte für eine Tabelle

Abb. 1: Problematische Funktionsgruppen (Auszug)

Externer Zugriff auf die SAP-Systeme

Das bisher als eher theoretisch behandelte Szenario des Zugriffs auf SAP-Systeme durch externe Programme oder Zugangskanäle erhält durch die Vielzahl frei verfügbarer Programme einen praktischen Bezug. Mit Hilfe des Programms ‚ExtractOnDemand for SAP' (EOD), welches ausschließlich lesende Zugriffe bereitstellt, wird dieses Bedrohungsszenario beispielhaft realistisch betrachtet. Dabei sollte der Zugriff stichprobenartig sowohl mit produktiven Berechtigungen als auch mit einem Testuser unter Laborbedingungen analysiert werden. Download-Authorisation o.ä. wird nicht benötigt, da das Tool eine eigene Preview- und Download-Funktion offeriert.

Nicht jeder Mitarbeiter im Unternehmen wird das Recht besitzen, Programminstallationen durchzuführen, ein Ausschluss solcher Rechte ist jedoch kaum sicherzustellen. Hinzu kommen temporär zugelassene Konfigurationen (aus Projekten o.ä.), die ebenfalls kaum abzusichern sind.

Des Weiteren werden nicht bei jeder Programminstallation lokale Administrationsrechte benötigt. Beispielsweise wird die Schnittstelle als Java-Connector (siehe bereitgestellte Klassen aus JCo) oder Access-Addon geliefert oder die Connection wird über server-basierte Skriptsprachen wie etwa PHP (siehe auch Open Source Projekt ‚SAPRFC' von Eduard Koucky) oder Perl (SAPRFC-Extension) bereitgestellt. EOD ist allerdings ein komplexes Programmpaket.

Zuletzt ist hier noch zu erwähnen, dass die Nutzung dieser Lücke auch über Systemgrenzen hinweg über die Verbindung von SAP-System zu SAP-System, je nach Berechtigungsausgestaltung z.B. von Entwicklung oder Test / Integration zu Produktion, möglich ist und somit ein fehlender Praxisbezug nicht unterstellt werden kann. Die Installation externer Programme stellt den schwierigeren Weg dar, insofern ist ein solches Szenarium durchaus als gegeben einzuschätzen.

Extract On Demand for SAP

EOD ist ein frei zugängliches Programmpaket, welches über die SOLONDE-Seite bezogen werden kann. Nach der Installation wird ein Licence-Key benötigt, dieser wird für eine befristete Testlizenz nach einer Registrierung bereitgestellt. Nach Vorliegen der Schlüsseldatei im Programmverzeichnis können alle SAP-Systeme angesteuert werden. EOD nutzt die SAP-Logon-Systemeinstellungen aus der SAPLOGON.INI oder eine manuelle Einstellung, die unter ‚Advanced' eingerichtet werden kann - das Zugangsprocedere ist mit dem des SAPGUI-Logon vergleichbar.

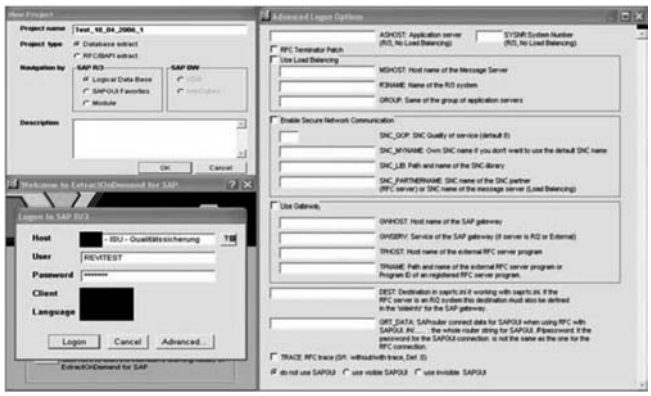


Abb. 2: Zugriff über EOD (Logon)

Nach erfolgreicher Anmeldung können aus den Tabellengruppen einzelne Tabellen- und View-Felder ausgewählt (Joins) und zu einer ‚Output-Fields'-Liste zusammengestellt werden. Ein Search-Modus ermöglicht die explizite Suche nach einzelnen Tabellen und Views, deren Daten über die Preview-Funktion angezeigt werden können. Grundsätzlich sind - vorbehaltlich entsprechender Berechtigungen - alle Daten eines SAP-Systems im Zugriff, die in Tabellen vorgehalten werden. Es gibt einige Bereiche, in denen die Daten in Binärform oder verschlüsselt vorliegen. Diese können nicht ohne weiteres aufgelöst werden, hierzu sind zusätzliche Bausteinaufrufe oder BAPI's zu nutzen (z.B. für Feldbeschreibungen DDIF_FIELDINFO_GET). Strukturen wie z.B. im HR die Infotypstruktur P0008 sind nicht notwendigerweise mit Tabellen verknüpft, sondern dienen meist der Aufbereitung von Daten aus verschiedenen Tabellen. Diese Strukturen werden nicht angezeigt - sehr wohl aber die zugehörigen Tabellen.

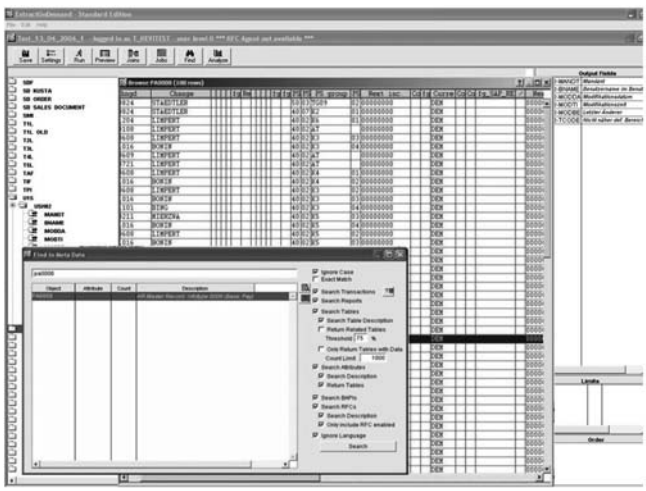


Abb. 3: Zugriff über EOD (HR PA0008)

Als besonders sensibel gelten beispielsweise die Payment-Daten. Auch diese sind über die Metadatensuche selektierbar, allerdings muss hier die BAPI-Technik (d.h. über Mitgabe eines BAPI's [HR-Cluster] - siehe u.a. BAPI_GET_PAYSLIP [Entgeltnachweis für Mitarbeiter]) einbezogen werden, um auf der Mitarbeiterebene, d.h. im detaillierten Einzelzugriff, Daten aufzubereiten.

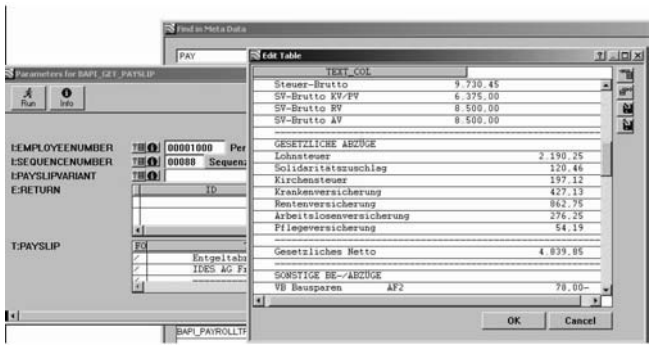


Abb. 4: Zugriff über EOD (Payment)

So lassen sich gewünschte Ergebnislisten per Preview und Download ohne Protokollierung im SAP beliebig auf dem Arbeitsplatzrechner zusammenstellen.

Fazit

Der hier beschriebene Zugriff auf SAP-Systeme demonstriert eine einfache Handhabung beim problemlosen Umgehen dokumentierter / gewünschter Sicherheitspolicies. Es zeigt sich deutlich, dass eine Beschränkung der Berechtigungsstrukturen in SAP nicht ausreicht, die umfangreichen betriebswirtschaftlichen Informationen, die im SAP - als die im Unternehmen zumeist maßgebliche Datenhaltung - abgelegt werden, abzusichern. Zum einen ist der Zugriff im SAP selbst, aber auch auf Betriebssystem- und Datenbankebene zu begrenzen, zum anderen besonders aber auch die Kanäle, die sich über die SAP-Schnittstellen und die Nutzung externer Connectoren ergeben. Dieser letzte Punkt kann nur unterbunden werden, wenn die Schnittstellen überwacht und eingeschränkt werden.

Häufig entscheidet das Unternehmen aus wirtschaftlichen Erwägungen heraus, die Administration in strukturellen Fragen zu entlasten und lediglich einen geringen Teil der Einschränkungsmöglichkeiten des SAP-Systems zu nutzen.

Folgende Maßnahmen sind hierzu u.a. erforderlich:

- Restriktiver Ansatz bei der Vergabe von RFC-Zugriffsberechtigungen
- Protokollierung gescheiterter, aber auch geglückter Zugriffsversuche über RFC und Dokumentationspflicht für die entsprechenden Benutzungen
- Auswertung der Protokollierung hinsichtlich dieser Ereignisse
- Reduzierung der Berechtigungen:
  - o Ausschluss von: S_ADMI_FCD: Funktion MEMO für alle Benutzerstammsätze; Ausnahme: Notfalluser, SAP-Hotline und Nicht-Dialog-User / Systemuser
  - o Ausschluss von: S_RFC: Funktionsgruppen BDCH, SYSE, SYST, SYSU, SRFC, SR1T, SRTT, SDTX und SUTL; Ausnahme wie zuvor
  - o Einschränkung von: S_TABU_DIS: dezidierte Einschränkung auf Ebene der Tabellengruppen auch für Anzeige der Tabellen bei allen Benutzern
  - o Einschränkung der Definitionsmöglichkeit von RFC-Destinationen (SM59 / NADM) => nur für SAP-Basisadministration und Notfalluser
- Analyse weiterer konkurrierender Zugangskanäle (auch RFC im Kundennamensraum u.a.) und möglicher Datencontainer und Eingrenzung dieser
- Positionierung des Unternehmens hinsichtlich des generell anzustrebenden Sicherheitsniveaus im Umfeld der SAP-Systeme und Risikoklassifizierung betriebswirtschaftlicher Informationen

Häufig entscheidet das Unternehmen aus wirtschaftlichen Erwägungen heraus, die Administration in strukturellen Fragen zu entlasten und lediglich einen geringen Teil der Einschränkungsmöglichkeiten des SAP-Systems zu nutzen. Es wird also auf der Ebene der Datenabsicherung in den SAP-Funktionen nicht in dem Maße eingegrenzt, wie dies sinnvoll ist ("Überversorgung" auf der Ebene der Berechtigungsobjekte) und überwiegend die Transaktionsebene als Schlüssel zur Funktionsbereitstellung genutzt. Tatsächlich substituiert ein wie hier dargestelltes Tool jedoch die bewusst entzogene Transaktionsberechtigung im Zielsystem (SE16, SQ01 usw.).

Es ist kaum zu verhindern, dass Schnittstellen durch externe Connectoren genutzt werden - es steht bereits eine Vielzahl von Tools zur Verfügung. Eine Reglementierung dieser von SAP bereitgestellten offenen, jedoch nicht jedem offensichtlichen Schnittstellen ist unausweichlich.

Ausgesuchte Literatur:

Beyer/Fischer/Jäck u.a.	SAP Berechtigungswesen - Design und Realisierung von Berechtigungskonzepten für SAP R/3 und SAP Enterprise Portal, SAP Press / Galileo Press, Bonn, 2003;
Thomas Tiede	SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP), 2. Auflage, Ottokar-Schreiber-Verlag, Hamburg, S. 282 - 304, www.osv-hamburg.de;
Christoph Wildensee	Ausgesuchte Berechtigungsobjekte des SAP R/3 - Systems als Prüfungsansatz für die IV-Revision - Eine Übersicht - Teil 1 bis 3 für Basis, FI & CO; Das SAP R/3 IS-U-Berechtigungskonzept - Versorgungswirtschaft - Ein Prüfungsansatz für die Interne Revision; Regelungsbedarf über die Berechtigungsdefinition und -vergabe hinaus, ReVision III/2001ff, Ottokar-Schreiber-Verlag, Hamburg, www.osv-hamburg.de;
OPAL	SAP Data Downloader www.opalsoft.com.au
SOLONDE	ExtractOnDemand for SAP®; www.solonde.com
TISCOM	RFCdirect; ww.tiscon.com
WINSHUTTLE	TablePro; www.winshuttle.com ✤

➲ SAP® Business Information Warehouse

Chancen und Risiken - Teil II: "Objekte der Begehrlichkeit!?"

Claus-Dieter Lillich
IBS Schreiber GmbH

Haben Sie eine Vorstellung von den möglichen Berechtigungsstrukturen für Ihr Unternehmen? Vertiefende Informationen zu BW-Berechtigungsobjekten schaffen Klarheit.

Was sie hier erwartet

Dieser Artikel erläutert das SAP BW-Berechtigungskonzept, welches auf der Nutzung von vordefinierten und selbst angelegten Berechtigungsobjekten basiert. Im folgenden sollen die wichtigsten Objekte in ihrer Funktionalität vorgestellt und an Beispielen verdeutlicht werden.

Ausblick

In weiteren Artikeln, die in den nächsten Ausgaben dieser Fachzeitschrift erscheinen, werden ihnen Schritt für Schritt vertiefende Kenntnisse des mit SAP BW zur Verfügung stehenden Instrumentariums vermittelt. Einen größerer Einblick in wichtige Teilaspekte verschafft ihnen die Möglichkeit, die Revisionsqualität ihres BW-Systems durch konkrete Prüfungsansätze maßgeblich zu erhöhen.

Berechtigungskonzeption von SAP BW

Das Berechtigungskonzept von R/3® stellt die elementarste Sicherheitsfunktion des Systems dar. Gleiches gilt für das Business-Information-Warehouse von SAP®. SAP® arbeitet transaktionsgesteuert. Das bedeutet, dass jede Anwendung innerhalb von SAP® durch eine Transaktion dargestellt wird. Das Berechtigungskonzept ist so aufgebaut, dass Benutzer Berechtigungen benötigen, um eine Funktion ausführen zu können. Diese werden bei SAP Transaktionen genannt.

Transaktionen

Transaktionen sind Programme, die einen Zugriff auf verschiedene Arten von Daten erlauben. Mit ihnen werden im Business-Warehouse Daten von anderen Systemen geholt, aufbereitet und verändert, gespeichert und für Auswertungen bereitgestellt. Das Berechtigungskonzept ist so aufgebaut, dass Benutzer Berechtigungen benötigen, um eine Transaktion ausführen zu dürfen. Für die meisten Transaktionen ist es notwendig, dass die Möglichkeiten, die diese Transaktion bietet, eingeschränkt werden. Es kann durchaus sinnvoll sein, einigen Benutzern die Anzeige von Tabellen zu gestatten, nicht allerdings die Änderung derselben. Realisiert werden diese notwendigen Einschränkungen über Berechtigungsobjekte.

Berechtigungsobjekte

Innerhalb des Berechtigungskonzeptes spielen spezielle Berechtigungsobjekte eine tragende Rolle. Für ein Objekt innerhalb des BW Systems gilt, dass es sich um einen vordefinierten <Datencontainer>

Es kann durchaus sinnvoll sein, einigen Benutzern die Anzeige von Tabellen zu gestatten, nicht allerdings die Änderung derselben.

handelt, der in Verbindung mit anderen <Datencontainern> des selben Benutzers bzw. der selben Benutzergruppe die Ausführung einer festgelegten Aktion erlaubt.

Liste aller Berechtigungsobjekte im SAP BW

Berechtigungsobjekte aus der Objektklasse RS (Business Information Warehouse)

RSCRMRTUPD	RSCRMRTUPD
R_AREA	Planungsgebiet
R_BUNDLE	Globale Planungssequenz
R_CT_SET	Währungsumrechnungseinstellungen
R_METHOD	Planungsmethode
R_PACKAGE	Planungspaket
R_PARAM	Parametergruppe
R_PLEVEL	Planungsebene
R_PM_NAME	Planungsmappe
R_PROFILE	Planungsprofile
R_STS_CUST	Ausführung des Customizing zum Status- und Tracking-System
R_STS_PT	Berechtigung für Planungsrunde und Teilplan
R_STS_ST	nicht mehr verwenden, bitte R_STS_PT verwenden!
R_STS_SUP	Berechtigung für Sonderzugriff Status und Tracking-System
R_UPX_EXEC	Vertriebsplanung ausführen
R_UPX_MNTN	Einstellungen zur Vertriebsplanung
R_WEBITF	Benutzung des Web Interface Builders
S_RS_ADMWB	Administrator Workbench - Objekte
S_RS_BCS	BEx Broadcasting Berechtigung zum Einplanen
S_RS_COMP	Business Explorer - Komponenten
S_RS_COMP1	Business Explorer - Komponenten: Erweiterung auf Owner
S_RS_FOLD	Business Explorer - Ordnersicht ein/aus
S_RS_HIER	Administrator Workbench - Hierarchie
S_RS_ICUBE	Administrator Workbench - InfoCube
S_RS_IOBC	Administrator Workbench - InfoObjectCatalog
S_RS_IOBJ	Administrator Workbench - InfoObject
S_RS_IOMAD	Administrator Workbench - Stammdaten pflegen
S_RS_ISET	Administrator Workbench - Infoset
S_RS_ISOUR	Administrator Workbench - InfoSource (flex. Fortschreibung)
S_RS_ISRCM	Administrator Workbench - InfoSource (direkte Fortschr.)
S_RS_MPRO	Administrator Workbench - Multiprovider
S_RS_ODSO	Administrator Workbench - ODS-Objekt
S_RS_TOOLS	Business Explorer - einzelne Werkzeuge

Zu Berichtszwecken stellt die SAP ferner die Objektklasse RSR (Business Information Warehouse - Reporting) zur Verfügung. In ihr und nur hier können eigendefinierte Berechtigungsobjekte gespeichert werden. Sie dienen den speziellen Anforderungen an das Reporting des einzelnen Unternehmens.

Anwendungsbereich und Aufgabe der wichtigsten Berechtigungsobjekte

Im Folgenden werden Berechtigungsobjekte im Zusammenhang mit ihrem Benutzerkreis dargestellt:

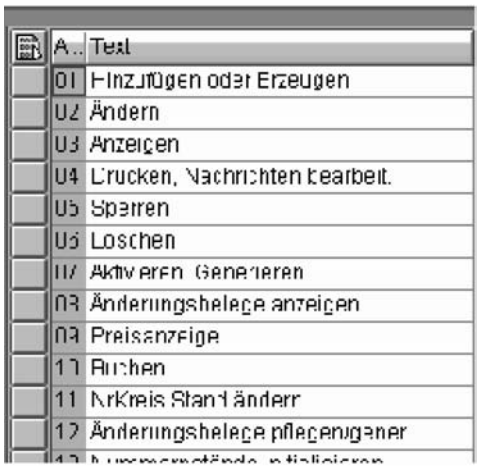
Objekte für wen	Bezeichnung	Beschreibung	Beispiel
Berichtswesen und Administration	**S_RS_ICUBE**	Berechtigungen zum Arbeiten mit InfoCubes und ihren Teilobjekten. Autorisierung der Anwender, die zur Definition des InfoCube, zur Anwendung von Fortschreibungsregeln und zur Anzeige der Daten im InfoCube berechtigt sind. Dieses Objekt schützt die Basis für das Arbeiten mit InfoCubes.	Ihr SAP BW-Administrator ist für das Anlegen von InfoCubes zuständig (Aktivität=01). Der Abteilungsleiter Verkauf benötigt Zugang zu den Daten in einem der neuen InfoCubes (Aktivität=03). Obwohl die Berechtigungswerte unterschiedlich sind, benötigen sowohl der Administrator als auch der Abteilungsleiter Verkauf Zugang zu diesem Objekt.
	S_RS_ODSO	Berechtigungen zum Arbeiten mit ODS-Objekten und ihren Teilobjekten	Zusätzlich zu den InfoCubes kann ein SAP-BW-Administrator ODS-Objekte zur Verarbeitung großer Mengen von Bewegungsdaten anlegen (Aktivität=01). Der Abteilungsleiter Verkauf benötigt auch Zugang zu Daten einiger ODS-Objekte, weil hier Detailinformationen zur Verfügung gestellt werden (Aktivität=03).
	S_RS_HIER	Berechtigungen zum Arbeiten mit Hierarchien. Durch dieses Objekt wird festgelegt, wer zum Anlegen von Hierarchien und wer zum Ausführen von Queries berechtigt ist, die Hierarchien verwenden.	Die Geschäftsleitung benötigt Informationen nach Kostenstelle. Der Abteilungsleiter Verkauf für die einzelnen Verkaufsgebiete (Europa, Amerika, Asien) und möchte diese auf Kostenstellenebene betrachten. Die Kostenstellen sind in einer Hierarchie definiert. Innerhalb der Hierarchie Verkaufsgebiet befinden sich die Kostenstellen für jede Region in diesem Bereich. Der BW-Administrator benötigt S_RS_HIER zum Anlegen der Hierarchien; der Abteilungsleiter Verkauf benötigt S_RS_HIER zum Ausführen der Queries, die Hierarchien nutzen.
Berichtswesen	**S_RS_COMP**	Berechtigung zur Verwendung verschiedener Komponenten für die Query-Definition. Dieses Berechtigungsobjekt ist sehr wichtig für das Reporting.	Im IKS ihres Unternehmens ist definiert, dass jeder Power-User Queries nur zu seiner eigenen Abteilung anlegen darf. Sie verwenden für jede Abteilung eine bestimmte Namenskonvention. S_RS_COMP kann zur Umsetzung dieser Strategie verwendet werden (in der Einkaufsabteilung müssen beispielsweise alle Queries mit EK beginnen). Möglichkeit 2 im IKS ihres Unternehmens ist definiert, dass jeder Power-User Queries nur zu seiner eigenen Abteilung anlegen darf. Sie haben die Abteilung mit einer bestimmten InfoArea und einem bestimmten InfoCube verknüpft. Alle Power-User können beliebige Queries mit einem beliebigen Namen erzeugen, solange sie nur Queries zu "ihrem" InfoCube erzeugen. S_RS_COMP kann ebenso zur Umsetzung dieser Strategie verwendet werden. Im ersten Beispiel ist die Berechtigung mit dem Query-Namen verknüpft, im zweiten Beispiel mit dem InfoCube.

Objekte für wen	Bezeichnung	Beschreibung	Beispiel
	S_RS_COMP1	Berechtigung für Queries von bestimmten Besitzern. Mit diesem Objekt kann nach Query-Besitzer eingeschränkt werden, welche Queries ein Anwender anzeigen kann.	Power-User A, B und C erzeugen Querys für verschiedene Arbeitsgebiete. Möchte ein Anwender im Bex Analyzer eine Query ausführen, enthält die Query-Liste nur die Queries, die von seinem Power-User erzeugt wurden.
	S_RS_FOLD	Berechtigung für Mappen anzeigen.	Der Reporting-Anwender kann nur seine Mappe Favoriten und die der zugewiesenen Rollen anzeigen. Es ist nicht möglich, andere InfoAreas anzuzeigen, zu denen kein Zugang erteilt wurde.
Administration	**S_RS_ADMWB**	Berechtigung zum Schutz der einzelnen Objekte der AdministratorWorkbench: Quellsystem, InfoObject, Monitor, Anwendungskomponenten, InfoArea, AdministratorWorkbench, Einstellungen, Metadaten, InfoPackages und InfoPackage-Gruppen.	U. a. wird dieses Objekt im Transaktionscode RSA1 verwendet und deckt zahlreiche Administrationsaufgaben ab. Hierzu zählt beispielsweise die Bearbeitung von Quellsystemen, InfoObjects, InfoPackages, Stammdaten und Bewegungsdaten.
	S_RS_IOBJ	Berechtigung zum Arbeiten mit einzelnen InfoObjekten und ihren Teilobjekten. Dieses Berechtigungsobjekt wird nur geprüft, wenn der Benutzer nicht zur Pflege oder Anzeige von InfoObjects berechtigt ist.	Muss ein Anwender nur Info-Objekte bearbeiten, kann ein Administrator mit der Berechtigung S_RS_ADMBW diesem Anwender S_RS_IOBJ zuweisen.
	S_RS_ISOUR	Berechtigung zum Arbeiten mit Bewegungsdaten, InfoSources und ihre Teilobjekte und Stammdaten InfoSources. Mit diesem Berechtigungsobjekt können Sie die Bearbeitung von InfoSources mit flexibler Fortschreibung und ihren Teilobjekten einschränken. Dieses Objekt schützt den Zugang zu den unterschiedlichen Quellsystemen und die Verwaltung der Übertragungsregeln.	Ein Administrator in Ihrem Unternehmen legt fest, welcher Administrator welche Daten (z.B. Bereich Einkauf) bzw. aus welchen Quellsystem(en) (z.B. Firma A oder Standort B) extrahieren darf, bzw. für die Batchverarbeitung, welche Daten extrahiert werden sollen.
	S_RS_ISRCM	Berechtigung zum Arbeiten mit Stammdaten-InfoSources und ihren Teilobjekten. Mit diesem Berechtigungsobjekt können Sie die Bearbeitung von InfoSources mit direkter Fortschreibung (für Stammdaten) oder mit ihren Teilobjekten einschränken.	Ein Administrator in Ihrem Unternehmen legt fest, welche Stammdaten auf welche Art und Weise (Verwaltung der Übertragungsregeln) aus welchen Quellsystemen extrahiert werden sollen.

Attribute von Berechtigungsobjekten

Ein Berechtigungsobjekt kann aus bis zu 10 unterschiedlichen Parametern bestehen, die Attribute genannt werden. Diese spezifizieren die Zugriffsmöglichkeiten.

Beispiel der möglichen Werte des Attributs: *Aktivität*



Nachfolgend werden die Attribute der aufgezeigten Berechtigungsobjekte vollständig dargestellt:

Bezeichnung	Beschreibung	Attribute	Wert
S_RS_ADMWB	Administrator Workbench Aktivität Administrator Workbench Objekt	ACTVT RSADMWBOBJ	* *
S_RS_COMP	Business Explorer - Komponenten Aktivität InfoArea InfoCube Name (ID) einer Reporting-Komponente Typ einer Reporting-Komponente	ACTVT RSINFOAREA RSINFOCUBE RSZCOMPID RSZCOMPTP	* * * * *
S_RS_COMP1	Business Explorer - Komponenten: Erweiterung auf Owner Aktivität Name (ID) einer Reporting-Komponente Typ einer Reporting-Komponente Besitzer (Verantwortlicher)	ACTVT RSZCOMPID RSZCOMPTP RSZOWNER	* * * *
S_RS_FOLD	Business Explorer - Ordnersicht ein/aus Druckknopf “Ordner” ausblenden	SUP_FOLDE	*
S_RS_HIER	Administrator Workbench - Hierarchie Aktivität Hierarchiename InfoObject Hierarchieversion	ACTVT RSHIENM RSIOBJNM RSVERSION	* * * *
S_RS_ICUBE	Administrator Workbench - InfoCube Aktivität InfoCube - Teilobjekt InfoArea InfoCube	ACTVT RSICUBEOBJ RSINFOAREA RSINFOCUBE	* * * *
S_RS_IOBJ	Administrator Workbench - InfoObject Aktivität InfoObject InfoObjectCatalog Teilobjekt zum InfoObject	ACTVT RSIOBJ RSIOBJCAT RSIOBJPAR	* * * *

Bezeichnung	Beschreibung	Attribute	Wert
S_RS_ISOUR	Administrator Workbench - InfoSource (flex. Fortschreibung) Aktivität Anwendungskomponente InfoSource InfoSource-Teilobjekt	ACTVT RSAPPLNM RSISOURCE RSISRCOBJ	* * * *
S_RS_ISRCM	Administrator Workbench - InfoSource (direkte Fortschreibung) Aktivität Anwendungskomponente InfoSource-Teilobjekt ObjectSource (Stammdaten, Texte und Hierachien)	ACTVT RSAPPLNM RSISRCOBJ RSOSOURCE	* * * *
S_RS_ODSO	Administrator Workbench - ODS-Objekt Aktivität InfoArea ODS-Objekt Teilobjekt zum ODS-Objekt	ACTVT RSINFOAREA RSODSOBJ RSODSPART	* * * *

Zuordnung zu Funktionen

Wie im SAP R/3-System, werden Profile für Benutzer mit gleicher Aufgabenstellung erstellt. Diese Profile bestehen aus Zuordnungen von Transaktionsberechtigungen und Berechtigungsobjekten. Grundsätzlich besteht der Wunsch nach der Attributsausprägung <*>, die den uneingeschränkten Zugriff auf die Funktionalitäten des Objekts beinhaltet.

Objekte der Begehrlichkeit

Aus der Erfahrung im Bereich Revision zeigt sich, dass der restriktiven Zuordnung von Berechtigungsobjekten zu wenig Beachtung geschenkt wird. Ohne feste Vorgaben und laufende Kontrolle, werden häufig - unabhängig von der tatsächlichen Notwendigkeit - ihre Mitarbeiten quasi unbemerkt zu <Superusern>. Dieses birgt neben gelegentlichen praktischen Vorteilen ein großes Risiko in Bezug auf den Schutz ihrer Geschäftsdaten vor unerwünschtem oder unberechtigtem Zugriff. Ein <Superuser> ist letztlich sogar in der Lage, aus dem BW-System heraus Daten zu verändern. Aus diesem Grunde sollte bei der Anlage von Profilen stets bedacht werden:

Berechtigungsobjekte sind ***"Objekte der Begehrlichkeit"****.*

✣

+++ Pressenotiz +++

Lohnsteuerrecht aktuell und die Auswirkungen für die Unternehmen Praxisrelevante Informationen zur Umsetzung der anstehenden Gesetzesänderungen auf dem 24. alga-Fachforum in Bad Neuenahr 12. Juni 2006 – Die Steueränderungen sind beschlossene Sache, doch welche Konsequenzen diese für die Unternehmen in der täglichen Praxis haben, ist noch unklar. Licht in den Dschungel der Neuerungen im Tagesgeschäft bringt das 24. alga-Fachforum vom 19.6. - 21.06.2006 in Bad Neuenahr. Namhafte Referenten erläutern die wichtigsten Auswirkungen sachgerecht und kompetent. In Diskussionsrunden können eingehend Fragen gestellt werden. „Da die Umsetzung der beschlossenen Steueränderungen in 2007 ansteht, haben wir gezielt nach Referenten gesucht, die Spezialisten auf diesem Gebiet sind. Es ist uns gelungen MR Richard Reinhart, Bundesfinanzministerium, Bonn, Michael-Ingo Thomas, Richter am Bundesfinanzhof, München sowie Roland Burau, Projektleiter ElsterLohn, Düsseldorf, zu gewinnen," erläutert Hans-Günter Böse, Geschäftsführer der datakontext-tagungen GmbH & Co.KG. Diskutiert werden in Bad Neuenahr auch weitere Gesetzesvorhaben 2007, wie der Arbeitgeber-Lohnsteuerjahresausgleich, die Vorsorgepauschale sowie die Festschreibung von Freibeträgen für Versorgungsbezüge. „Wir sind stolz darauf, dass es uns erneut gelungen ist, dieses spannende Thema Lohnsteuerrecht mit derart hochkarätigen Referenten zu besetzen, die im Tagesgeschäft mit den jeweiligen Fragestellungen der Praxis beschäftigt sind und somit Rede und Antwort stehen können", ergänzt Bernd Hentschel, Vorsitzender und Gesamtleiter des alga-Competence-Centers, Frechen. Hentschel kann durch seine langjährige Arbeit auf ein funktionierendes Netzwerk kompetenter Referenten zurückgreifen, die das Programm der alga-Fachforen interessant gestalten.

Ansprechpartner für Rückfragen:
Elke Peters
Tel. +49 (0)22 34 / 6 56 - 33
Fax +49 (0)22 34 / 6 56 - 35
E-Mail: mainz@datakontext.com

➲ IT-Revision

Liebe Leserinnen und Leser,

die Entwicklung von Applikationen und deren Einsatz in Unternehmen geht mit rasanter Geschwindigkeit voran. Immer mehr Funktionen, Prozesse und Datenbestände werden digitalisiert und miteinander verknüpft.

Für die interne Revision bleibt das Problem, dass für eine Prüfung dieser rasanten Entwicklung nur in den seltensten Fällen auch Tools bereitstehen, um diesen neuen Einsatz von Systemen und Prozessen prüfen zu können.

Daher bleibt oft nur der Weg, auf Standard-Tools für eine Auswertung und Analyse von Daten und deren Verknüpfungen zurückzugreifen.

Frau Katrin Fitz zeigt in einem Beitrag an praktischen Beispielen, wie man mit dem Einsatz von Microsoft-Office-Produkten Datenbestände aus Applikationen prüfen und auswerten kann, ohne dass diese dafür explizite Funktionen für einen Revisor bereitstellen müssen.

Anhand des Einsatzes von Excel und Access wird gezeigt, wie man nach bestimmten Kriterien in Grenzwerten Abweichungen ermitteln kann oder Inkonsistenzen zwischen verschiedenen Datenbeständen ermittelt.

Dass IT-Sicherheit heute nur Geld zusätzlich kostet, ist eine gängig verbreitete Meinung. Aber dass sich mit dem Einsatz von IT-Sicherheit auch Geld verdienen lässt, abgesehen von den sonstigen Steigerungen, die damit verbunden sind, ist nur für Wenige nachvollziehbar.

Hier kann auch die Empfehlung der Revision bei Prüfungen und deren Argumentation der wirtschaftlichen Vorteile bei der Umsetzung von Maßnahmen unterstützend wirken. Es gibt zwar keinen allgemeingültigen Kalkulator für ein "Return on Security Investment" (RoSI), aber in einem Beitrag finden Sie hier Ansätze , die auch einen wirtschaftlichen Aspekt darstellen lässt und kalkulieren lassen.

Ihr

Michael Foth

➲ Das MS Office Paket als Prüftool

Dipl.-Wirtschafts-Ing.
Katrin Fitz
IBS Schreiber GmbH

Speziell für die Prüfung von Massendaten gibt es zwei Produkte am Markt, die einen immensen Umfang an Programmfunktionen bieten. Sie sind speziell auf die Bedürfnisse des Revisors angepasst. Gemeint sind IDEA® und ACL®.

Die Stärken liegen eindeutig im Umgang mit Massendaten, in diversen Importfiltern für externe Daten und in den Analysefunktionen.

In welcher Weise grenzen sich diese Prüftools von den MS Office Produkten Excel® und Access® ab?

Der eindeutige Wettbewerbsvorteil der MS Office-Produkte ist, dass sie so vielfältig einsetzbar sind, dass sie in vielen Unternehmen bereits an jedem Arbeitsplatz vorhanden sind. Bei der Entscheidung zwischen IDEA® und MS Excel® bzw. MS Access® werden also meistenteils nicht die jeweiligen Kosten und Nutzen gegenüber gestellt. Es muss viel mehr geprüft werden, ob vorhandene Tools (hier also das MS Office Paket) den Bedarf abdecken können.

Welche Möglichkeiten bieten MS Excel® und MS Access® und wo liegen die Grenzen?

Der Spezifikation von MS Excel® 2003 ist zu entnehmen, dass ein Arbeitsblatt maximal 65.536 Zeilen und 256 Spalten haben kann. Jede Zelle kann 32.767 Zeichen aufnehmen. Die Anzahl der Arbeitblätter ist nur durch den verfügbaren Hauptspeicher begrenzt.

Auch in MS Access® kann eine Tabelle nicht mehr als 255 Spalten enthalten. Die Zeilenzahl ist nicht direkt beschränkt, die gesamte Tabelle darf jedoch nicht größer als 1GB werden. Die Anzahl der Objekte ist auf 32.768 beschränkt. Hierzu gehören Tabellen, Abfragen, Berichte, Formulare, Seiten und Module. Insgesamt darf die Datenbank nicht größer als 2GB werden.

Die Grenzen der zu bearbeitenden Datenmenge sind also klar definiert und für den größten Teil der Arbeit sicher ausreichend.

Der nächste Aspekt ist die Revisionsfestigkeit und die Protokollierung der ausgeführten Analysen. Diese sind bei IDEA® und ACL® vollständig gegeben, die MS Office Produkte bieten hier keine Möglichkeit. Die versehentliche Bearbeitung der Daten kann zwar begrenzt unterbunden werden, von Revisionsfestigkeit kann hier jedoch nicht gesprochen werden.

Von diesen Randbedingungen abgesehen bietet das Office-Paket mit Excel® und Access® zwei mächtige Werkzeuge zur Datenanalyse.

Nachfolgend möchte ich anhand von drei Beispielen aufzeigen, wie klassische Revisions-Fragen gelöst werden können.

Schichtung (Excel®)

Bei einer Menge von Auftragsdaten ist es zur Analyse sehr hilfreich, diese zunächst in verschiedene

Kategorien einzuteilen. Zum Beispiel gibt es ein sogenanntes *Vertrauensintervall*, in dem Aufträge nicht genauer geprüft werden. Die Mitarbeiter haben beispielsweise freien Handlungsspielraum bis 500 EUR. Hier würden die Grenzen von 400 EUR bis 500 EUR angesetzt.

Ein weiteres interessantes Intervall ist das der Ausschreibungsgrenzen. Evtl. gibt es Richtlinien die vorschreiben, dass ab einem Volumen von 5.000 EUR beschränkt ausgeschrieben werden muss und ab 10.000 EUR öffentlich. Hier sind die Bereiche kurz darunter interessant um Splittung aufzudecken. Für öffentliche Auftraggeber werden diese Grenzen durch das Vergaberecht geregelt.

In dem Beispiel teilen wir unsere Auftragsdaten also in folgende Schichten ein, die anschließend näher untersucht werden müssen:

400 EUR -	500 EUR	Vertrauensintervall
4.000 EUR -	5.000 EUR	bis beschränkte Vergabe
9.000 EUR -	10.000 EUR	bis Ausschreibung

Umsetzung in Excel®:

Zur Einteilung der Daten in die jeweiligen Schichten kann die Funktion `SVERWEIS()` verwendet werden.

Im ersten Schritt wird eine Matrix aufgestellt, die in der ersten Spalte die untere Grenze des Intervalls enthält. Als obere Grenze dient die untere Grenze des nächsten Intervalls. Aus diesem Grund müssen wir also auch die Intervalle, die nicht geprüft werden sollen, mit aufnehmen.

In der zweiten Spalte wird der Kategorie ein Name zugeordnet:

400 EUR	Vertrauensintervall
500 EUR	irrelevant
4.000 EUR	bis beschränkte Ausschreibung
5.000 EUR	irrelevant
9.000 EUR	bis Ausschreibung
10.000 EUR	irrelevant

Im zweiten Schritt wird an die Datenbasis (Auftragsdaten) eine berechnete Spalte angefügt. Als Formel dient hier der bereits erwähnte `SVERWEIS()`. Diese Funktion benötigt mindestens drei Argumente: `Suchkriterium`, `Matrix` und `Spaltenindex`.

`Suchkriterium` enthält den Wert, der in der Matrix gesucht wird.

In unserem Beispiel ist es das Auftragsvolumen, dass in eine der Schichten einsortiert werden soll.

`Matrix` enthält den Bereich in Excel®, in dem sich die Verweis-Matrix befindet. In unserem Beispiel kann es A1:B6 (Spalte A und B, Zeile 1 bis 6) sein.

`Spaltenindex` enthält den Index der Spalte, in dem der Name der Kategorie zu finden ist. Hierbei werden die Spalten der unter *Matrix* definierten Matrix mit 1 beginnend nummeriert.

In unserem Beispiel ist dies also der Wert 2.

In der berechneten Spalte steht nun je nach Auftragswert entweder ‚Vertrauensintervall', ‚bis beschränkte Ausschreibung', , bis Ausschreibung' oder ‚irrelevant'.

Im dritten Schritt kann nach diesen Begriffen nach Belieben gruppiert, sortiert und gefiltert werden. Interessante Stichworte hierzu sind die Funktionen *Teilergebnisse* und *Pivot-Tabelle* aus Excel®.

Für die Risiko-Bewertung ist ebenfalls interessant zu sehen, wie viele Aufträge den Hauptumsatz ausmachen. Werden z.B. 40% des Umsatzes mit 2% der Aufträge erwirtschaftet? Wie kann reagiert werden, wenn einer der Hauptkunden ausfällt?

Altersstrukturanalyse (Excel®)

Mit der Altersstukturanalyse können Datenbestände nach Bearbeitungszeiträumen gruppiert werden. So kann zum Beispiel das Zahlungsverhalten der Kunden überprüft werden. Fragestellungen wie "Wie viele Kunden zahlen innerhalb der ersten 30 Tage (Skonto)" oder "Wie verteilen sich die Offenen Posten im Bezug auf Rechnungsdatum?" können mit dieser Funktion leicht geprüft werden. Die Umsetzung in Excel® lässt sich ebenfalls durch die Funktion `SVERWEIS()` realisieren.

Im ersten Schritt wird ein berechnetes Feld angefügt, dass den Zeitraum zwischen zwei Daten angibt. Hierzu kann einfach das eine Datum vom zweiten abgezogen werden. Das Ergebnis ist die Anzahl der Tage als Zahl. Die Zelle muss also als Zahl formatiert sein um das Ergebnis korrekt angezeigt zu bekommen.

Das aktuelle Datum erhält man mit der Funktion `HEUTE()`

Die Formel für das Alter eines offenen Postens kann also folgendermaßen aussehen:
`=HEUTE() - RgDatum`

Wobei RgDatum für das Feld steht, in dem das Rechnungsdatum gespeichert ist.

Im zweiten Schritt muss eine Matrix aufgestellt werden. Sie kann folgendermaßen aussehen:

0 Tage	Skonto
10 Tage	Im Zahlungsziel
30 Tage	Zahlungsziel überschritten
40 Tage	erste Mahnung
50 Tage	zweite Mahnung

Hier gibt die erste Spalte die untere Grenze des Intervalls an, die zweite Spalte gibt den Namen für die Kategorie an.

Im dritten Schritt wird wie bei der Schichtung ein Feld für den `SVERWEIS()` angefügt. Als Suchkriterium dient bei der Altersstrukturanalyse das im Schritt Eins berechnete Feld.

Die Funktion könnte in dem angeführten Beispiel folgendermaßen aussehen:
`=SVERWEIS(RgAlter;A1:B5;2)`

Im vierten Schritt kann nach Belieben sortiert, gruppiert und gefiltert werden. Weitere Analysen können mit der Funktion *Teilergebnisse* oder über *Pivottabellen* berechnet werden

Inkonsistenzprüfung (Access®)

Diese Prüfung kann angewendet werden, wenn zwei verschiedene Tabellen mit einem gemeinsamen Schlüssel vorliegen. Es wird hierbei geprüft, ob in beiden Tabellen Daten zu jedem Schlüssel vorhanden sind. Dies können zum Beispiel Bestellkopfdaten und Bestelldetails sein. Die Kopfdaten-Tabelle enthält alle Daten zum Auftraggeber und die Tabelle Bestelldetails enthält alle Bestellpositionen. Die spezielle Prüffrage lautet hier: "Gibt es Bestellungen ohne Bestelldetails?"

Diese Fragestellung ist denkbar einfach zu lösen. Access® stellt hierzu einen Assistenten zur Inkonsistenz-Analyse zur Verfügung.

Über das Menü *Einfügen -> Abfrage* wird ein Fenster zur Auswahl des gewünschten Assistenten geöffnet. Nach der Wahl *Abfrage-Assistent zur Inkonsistenz-Suche* öffnet sich ein Auswahlfenster. Hier wählen Sie zunächst die Tabelle, die die ‚Master-Daten' enthält, aus. In unserem Beispiel ist dies die Tabelle *Kopfdaten*. Nach bestätigen der Auswahl mit Weiter werden sie gebeten, die Tabelle mit den Detail-Datensätzen anzugeben. In unserem Beispiel ist dies die Tabelle Bestellpositionen

Im nächsten Fenster geben Sie an, über welchen Schlüssel die Daten verknüpft werden sollen. In unserem Beispiel ist dies das Feld Bestellnummer.

Ein weiterer optionaler Schritt ermöglicht die Auswahl der Felder, die in der Ergebnismenge enthalten sein sollen. In unserem Beispiel können es also Daten zum Bearbeiter, die Bestellnummer und die Kundennummer sein. Es sollten hier alle Felder gewählt werden, die zur weiteren Analyse des Ergebnisses notwendig sind.

Nach der Wahl *Fertigstellen* erhalten Sie alle Master-Daten, denen keine Detail-Daten zugeordnet sind. In unserem Beispiel also die Bestellungen ohne Bestellposition.

Fazit

Excel® und Access® können zur Prüfungsunterstützung sehr gut eingesetzt werden. Welches Programm bevorzugt wird kann hauptsächlich von den Vorlieben des Prüfers abhängig gemacht werden. Die Funktionalität im Bezug auf die Datenanalyse ist sehr ähnlich. Lediglich die technische Umsetzung ist grundverschieden. ✤

IBS Prüfen mit Konzept

Jahresfachkonferenz

„Sicherheit und Prüfung im Gesundheitswesen“

16.10.-17.10.2006 in Hamburg

Liebe Interessenten,

zum ersten Mal findet in diesem Jahr auch eine branchenspezifische IBS-Fachkonferenz für den Bereich Revision statt. Mit dem Thema "Sicherheit und Prüfung im Gesundheitswesen" wollen wir den Anforderungen nach branchenspezifischen Themen gerecht werden und dieser Branche, die zur Zeit durch große Veränderungen geprägt ist, frühzeitig Hilfen und Hinweise für diese neuen Themen geben.

Das Gesundheitswesen ist zur Zeit durch das Gesundheits-Modernisierungs-Gesetz, Einführung der Gesundheitskarte, Telemedizinische Anwendungen, medizinische Netzwerke, Outsourcing und rechtssichere Archivierungsfragen geprägt.

Alle diese Themen sind für die Revision von hoher Bedeutung, da sie nicht unerhebliche Auswirkungen auf die Prozesse in Kliniken, bei Ärzten aber auch bei den Kostenträgern haben.

So werden wir am ersten Konferenztag durch den Bundesbeauftragten des Datenschutzes, Herrn Peter Schaar, und durch den Landesbeauftragten des Datenschutzes Schleswig-Holstein, Herrn Dr. jur. Thilo Weichert, etwas über die Anforderungen des Datenschutzes für Telemedizin und medizinische Netze erfahren, die auf einer Infrastruktur basieren, die technisch machbar ist, aber deren Anforderung unter Datenschutz- und Revisionsgesichtspunkten nur selten betrachtet wird.

Vor allem die rechtsverbindliche Archivierung von Patientenunterlagen, elektronische Signatur und die Einhaltung von Fristen, auch im Bereich medizinischer Netze, werden von Herrn Prof. Dr. Paul Schmücker vorgetragen und diskutiert.

Der zweite Konferenztag bietet in zwei Durchgängen die Möglichkeit, Themen zur Prüfung von SAP® durch Herrn Thomas Tiede oder die Anforderungen an Sicherheit der Gesundheitskarte für die Revision und den Datenschutz durch Herrn Marcel Weinand vom Bundesamt für Sicherheit in der Informationstechnik zu erörtern. Die Prüfbarkeit und Zertifizierung von Infrastrukturen und deren Aussagekraft durch Herrn Prof. Dr. Reinhard Vossbein wird parallel zum Thema Korruption und deren Verhinderung im Gesundheitswesen durch Herrn Prof. Dr. Joachim Tanski angeboten.

Ich freue mich auf spannende und aufschlussreiche Diskussionen zwischen Ihnen und unseren Referenten zur Beförderung Ihrer Prüfungsstrategie und -umsetzung in Ihrem Bereich und nicht zuletzt auf den gemeinsamen Hamburger Abend mit Ihnen.

Ihr Michael Foth

www.ibs-hamburg.com

Telematik im Gesundheitswesen

- Grundrecht auf informationelle Selbstbestimmung und Arztgeheimnis
- Datensouveränität der Patienten
- Technische und organisatorische Datenschutzprobleme
- Akzeptanz bei den Patienten

PETER SCHAAR, BUNDESBEAUFTRAGTER FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

Risiken und Prüfbarkeit der Infrastruktur

- Patientendaten im Netz
- Risiken der Mitlesbarkeit
- Neue Technologien, mobiler Einsatz und WLAN
- Möglichkeiten und Grenzen der Revision

MICHAEL FOTH, IBS SCHREIBER GMBH

Revision beim Outsourcing/Outtasking

- Externe Verarbeitung medizinischer Daten
- Outsourcing und Public-Private-Partnership
- Änderung der StPO § 97
- Auswahl eines Dienstleisters
- Anforderungen an Verträge und Möglichkeiten der Prüfbarkeit
- Verwendung Prüfungergebnisse Dritter

DIPL.-INF. HOLGER KLINDTWORTH, SUSAT & PARTNER OHG &
WP/STB DIPL.-KFM. (FH) OLAF MANGLIERS, SUSAT & PARTNER OHG

Elektronische Archivierung von Patientenunterlagen - Anforderungen an Datenschutz und Rechtssicherheit

- Anforderungen an Datenschutz und Rechtssicherheit
- Zugriffsberechtigungskonzepte für elektronische Patientenakten
- Prüfbarkeit von Fristen und Löschung
- Zulässigkeit, Ordnungsmäßigkeit und Revisionssicherheit digitaler Archivsysteme
- Grundsätze der beweiskräftigen elektronischen Archivierung
- Rechtssicherheit von digitalen Dokumenten mit Hilfe digitaler Signaturen
- Informationsaustausch in integrierten Versorgungsnetzen

PROF. DR. PAUL SCHMÜCKER - HOCHSCHULE MANNHEIM

Anschließend gemeinsames Abendprogramm “Hamburger Abend

www.ibs-hamburg.com

Workshops - Session 1

WS 1.1 - Zukünftige Anforderungen durch die Gesundheitskarte

- aktueller Sachstand zum Heilberufeausweis und zur Gesundheitskarte
- Anforderungen an die Sicherheit und Schutzprofile
- Vorgabe und Einbeziehung durch das BSI
- Wozu Schutzprofile - welcher Nutzen ist damit verbunden?
- Das Deutsche Sicherheitszertifikat und die EAL-Stufen

Dipl.-Ing. Marcel Weinand, Bundesamt für Sicherheit in der Informationstechnik

- Änderungen in Prozessen und Infrastruktur beim Leistungserbringer
- Risiken und Kontrollen der Lösungen
- Frühzeitige Einbindung von Datenschutz und Revision

Michael Foth, IBS Schreiber GmbH

WS 1.2 - Einsatz von SAP® Systemen in Krankenhäusern

- Datenschutz in SAP® Systemen mit Patientendaten
- Das Berechtigungskonzept in mySAP® Healthcare
- Möglichkeiten zum Zugriff auf Patientendaten
- Absicherung der Schnittstellen von mySAP® Healthcare zu mySAP® FI/MM

Thomas Tiede, IBS Schreiber GmbH

Workshops - Session 2

WS 2.1 - Prüfbarkeit und Zertifizierung der IT-Systeme/-Infrastruktur

- Welche Gütesiegel oder Zertifikate gibt es?
- Welche sind sinnvoll und aussagekräftig?
- Vorgehensweise bei der Durchführung von Audits
- Anforderungen an und Vorteile von Zertifizierungen
- Revisionsfähigkeit von Zertifizierungsergebnissen

Prof. Dr. Reinhard Vossbein, UIMCert

WS 2.2 -Korruption und Korruptionsverhinderung im Gesundheitswesen

- Korruptionsfälle und -ursachen
- Analyse von Korruptionsrisiken
- Maßnahmen zur Korruptionsverhinderung
- Aufgaben der internen Revision

Prof. Dr. Joachim Tanski, Fachhochschule Brandenburg

Prüfbarkeit und Anforderungen des Datenschutzes an medizinische Netze

- verfassungsrechtliche Grundlagen, Patientengeheimnis und Wahlfreiheit
- Verantwortlichkeit in verteilten Systemen
- gesetzliche Anforderungen, insbesondere im Hinblick auf die elektronische Gesundheitskarte
- regionale Praxisnetze, integrierte Versorgung, Telematik-Infrastruktur
- Anforderungen vernetzter elektronischer Strukturen nach §§ 63, 73a, 140 SGB V
- technische Sicherungen von Vertraulichkeit, Integrität und Revisionsfähigkeit
- Sicherung der Patientenrechte
- Kontroll-Szenarien der Datenschutz-Aufsicht und Best Practice, Gütesiegel, Audit

Dr. Thilo Weichert, Landesdatenschutzbeauftragter Schleswig-Holstein

Abschlußdiskussion und Verabschiedung

www.ibs-hamburg.com

...::::::: Anmeldung zur IBS-Jahresfachkonferenz "Gesundheitswesen" 2006 :::::::...

FON: +49 (0) 40 69 69 85-15 • Fax: +49 (0) 40 69 69 85-31 • E-Mail: seminare@ibs-hamburg.com

Vor-/Nachname:	Telefon:
Firma:	Telefax:
Abteilung:	E-Mail:
Straße/Postfach:	Ort, Datum:
PLZ/Ort:	Unterschrift:

Veranstaltungsort: Le Royal Méridien *****, An der Alster 52-56, 20099 Hamburg

Teilnahmegebühr: pro Person (2 Tage) 1.200,- € zzgl. MwSt.

(inkl. Abendveranstaltung, Fachkonferenzunterlagen als Ausdruck und auf CD, Mittagessen und Pausengetränke)

Jeder Teilnehmer erhält ein persönliches Exemplar „Interne Revision - Jahrbuch 2007".

Frühbucherrabatt: Bei Anmeldung bis zum **18.08.2006** bieten wir Ihnen die Teilnahme zu einem Preis von 950,- € (zzgl. MwSt.) an.

Die IBS Schreiber GmbH behält sich vor, inhaltliche und personelle Änderungen im Programm vorzunehmen, wenn die Gründe hierfür nicht vom Veranstalter zu vertreten sind.

Bitte tragen Sie hier Ihre Teilnahme für unser Abendprogramm („Hamburger Abend") am 16.10.2006 ein:

- ❒ Ja, ich nehme am Hamburger Abend teil.
- ❒ Ja, ich nehme am Hamburger Abend teil und bringe meine/n Partner/in mit.
- ❒ Nein, ich nehme nicht am Hamburger Abend teil.

Wie sind Sie auf unsere Fachkonferenz aufmerksam geworden? _____

Auf Wunsch nehmen wir gerne nachstehende Hotelreservierung für Sie vor:

Hotelreservierung von (Anreise): _____ bis (Abreise): _____

- ❒ Raucher
- ❒ Nichtraucher

Bei Buchung über die IBS Schreiber GmbH gewährt Ihnen unser Veranstaltungshotel (Le Royal Méridien) folgende Sonderkonditionen:

Zimmer: ❒ Einzelzimmer inkl. reichhaltigem Frühstücksbuffet 189,00 €

Wir bitten Sie um Ihre Hotelbuchung möglichst bis zum **15.09.2006**, da das Hotel nach diesem Datum keine freien Zimmer mehr garantieren kann.

Ort/Datum: _____ **Unterschrift**: _____

www.ibs-hamburg.com

➲ Mit IT-Sicherheit Gewinn erzielen

Dipl.-Ing.
Michael Foth
IBS Schreiber GmbH

Die Aufgabe der Revision ist es auch, die Sicherheitslösungen der IT-Infrastrukturen zu prüfen. Hier finden sich heute noch immer die größten Mängel und Lücken. Argumente, wie "es ist doch bisher nichts passiert" und "die Investitionen dafür sind zu hoch" klingen zunächst wie betriebswirtschaftliche Ausreden. Aber gerade aus Sicht der Revision lässt sich mit der Notwendigkeit von Mindest-Sicherheitsmaßnahmen für die IT-Infrastruktur sogar Gewinn erzielen. Dieses basiert nicht nur auf den Kriterien nach Basel II, um ein günstigeres Rating zu erreichen, was sich auf jeden Fall auch rechnen lässt, oder den Anforderungen nach KonTraG, was sich in der Bilanz gut darstellen lässt. Auch die nüchterne Betrachtung des Betriebes und der Systeme im täglichen Einsatz lässt eine Kosteneinsparung und für die Zukunft Gewinne aufzeigen. Hier kann die Revision die Chancen aufzeigen und beratend aus ihrer Rolle heraus als Initiator für ein "Return on Security-Investment" dienen. Dieser Beitrag soll Möglichkeiten für eine Herangehensweise aufzeigen, Investitionen in Security-Lösungen auch aus einer anderen Sicht zu betrachten. Die Prüfungen und Empfehlungen der Revision können hier die Basis bilden und sollten in den Empfehlungen auch diese Aspekte berücksichtigen, da Empfehlungen, die mit der Umsetzung von Sicherheits-Kriterien zusätzlich noch Kosteneinsparungen bringen, sich leichter durch alle Ebenen realisieren lassen.

Sicherheits-Gewinn

Investitionen in die Sicherheit der IT-Infrastruktur eines Unternehmens sind sicherlich keine zu vernachlässigende Größe und dürfen auch kein Selbstzweck sein. Angesichts deutlicher Zurückhaltung bei derartigen Investitionen erscheint jedoch eine erneute Besinnung auf die betriebswirtschaftlichen Überlegungen angebracht, die durchaus auch für Sicherheitsinvestitionen sprechen können.

Schäden durch Sicherheitsvorfälle sind zwar schwer zu beziffern, aber beileibe keine graue Theorie: Im Jahre 2004 legten Serverausfälle oder der Zusammenbruch ganzer Netzwerke zwei Drittel der Firmen zeitweise lahm. Wie Mummert Consulting in der Studie "IT-Security 2004" berichtet, fiel bei jedem elften registrierten Angriff das Unternehmensnetzwerk sogar länger als einen Arbeitstag aus. Die Folgen mangelhafter Sicherheitsmaßnahmen kosteten 44 der Firmen bis zu 10.000 €, jeder zehnte IT-Manager bezifferte den Schaden auf bis zu 100.000 € und l% beklagte sogar Verluste von mehr als einer halben Million.

Doch die wenigsten Unternehmen scheinen aus diesem Schaden klug zu werden. Mehr als die Hälfte der befragten Firmen haben ihr Engagement in puncto Datensicherheit gegenüber dem Vorjahr nicht aufgestockt - im Gegenteil: Fast jedes zwölfte Unternehmen will das entsprechende Budget sogar senken. Derzeit steht offensichtlich vor allem die Kostenseite der Investitionen im Fokus der Entscheidung. Die Folge: Zwei von fünf Sicherheitsinvestitionen scheitern, weil niemand das dafür nötige Geld in die Hand nehmen will. Bisweilen scheint es dabei an objektivierten finanziellen Argumenten zu mangeln.

Natürlich unterliegen Investitionen in die Sicherheit den gleichen Forderungen nach Wirtschaftlichkeit wie alle anderen Unternehmensausgaben auch. Die Besonderheit ist dabei, dass eine solche Investition der Senkung eines Risikos dient, das demnach erst einmal für die konkrete Umgebung korrekt einzuschätzen ist. Doch es gibt auch einige allgemeingültige Eckdaten, die das weltweite Ausmaß der Bedrohung kennzeichnen und die bei der Analyse bekannt sein sollten: Hier können Studien und Analysen aus Presse, von Consulting-Unternehmen sowie durch Anbieter, Computer Emergency Response Teams (CERTs) hilfreich sein.

Auch die Informationen sonstiger Organisationen wie des SANS Institute (www.sans.org) bilden eine gute Basis, um für einen bestimmten Zeitraum statistische Daten hinsichtlich der Art und des Aufkommens von Malware-Ausbrüchen und gezielten Attacken sowie über den verursachten wirtschaftlichen Schaden zu erhalten. Dieses kann zumindestens eine Basis für die Definition einer Eintrittswahrscheinlichkeit sein. Das ist nötig, um Investitionen in ein kalkulierbares Verhältnis für eine entsprechende Kalkulation setzen zu können.

Eine Schwachstelle alleine mag vielleicht noch kein ernstes Problem sein - trifft ein solcher wunder Punkt aber mit einem realistischen Bedrohungsszenario zusammen, so lässt sich anhand der angenommenen Eintrittswahrscheinlichkeit ein statistischer Wert für zu erwartende Schäden errechnen. Eine sinnvolle Kosten-Nutzen-Analyse für die IT-Sicherheit sollte das Risiko beziehungsweise die Auswirkungen eines Systemausfalls unter Annahme der Eintrittswahrscheinlichkeit im Verhältnis zum Aufwand für die Beseitigung des Risikos betrachten. Zu diesem Zweck sind zunächst die vorhandenen Risiken zu identifizieren und zu bewerten.

Risiko und Aufwand ermitteln

Der Risikowert eines Risikos lässt sich dabei als das Produkt aus seiner Eintrittswahrscheinlichkeit multipliziert mit der finanziellen Bewertung der damit verbundenen Auswirkungen ermitteln. Der Risikowert aller identifizierten Risiken ist dann die Summe der Risikowerte der Einzelrisiken. Eine Investition in die Risikoverminderung - also in die Sicherheit - lohnt sich dann, wenn im Betrachtungszeitraum der Risikowerte der Risiken die Investition in die Risikoverminderung zuzüglich des verbleibenden Risikos übersteigt.

Nach der Ermittlung des Risikowerts aller Risiken sowie der erforderlichen Investitionen zur Verminderung oder Vermeidung der Risiken kann der Return on Security-Investment (ROSI) kalkuliert werden: Er ergibt sich aus dem Wert, der durch die geplante Investition entsteht, dividiert durch die dafür notwendigen Ausgaben. Als Wert kann der Betrag angesehen werden, um den der Risikowert der Risiken reduziert wurde, also der Risikowert des Risikos vor der Investition abzüglich des Risikowertes des Restrisikos nach getätigter Investition.

Unternehmensprofil	
Angaben zur Paketberechnung	
Anzahl IP-Adressen in der Zentrale	200
Nebenstandorte: Anzahl im Inland	5
Anzahl im Ausland	2
Durchschnitt. Anzahl IP-Adressen pro Nebenstandort im Inland	25
pro Nebenstandort im Ausland	10
Mitarbeiter mit RLA-Zugriff: Anzahl im Inland	30
Anzahl im Ausland	25
Angaben zur RoSI-Berechnung	
Umsatz pro Jahr	50 Mio. €
Paketpreis / Return on Security Investment	
Paketpreis	134.010 €
Infrastrukturkosten	1.069 €
Amortisierungsdauer der Investition	17,2 Monate
Kostenersparnis pro Monat	7.832 €
Kostenersparnis durch reduziertes Schadenspotential und reduzierte Betriebskosten.	

Beispieldarstellung einer Return-on-Security-Investment Kalkulation für Arbeitsplatz und Kommunikationssicherheit.

Ermittlung des "Returns on Investment"

Ist beispielsweise in einem Unternehmen kein Virenschutz vorhanden, heißt das Bedrohungsszenario "Infektion des Netzwerks mit allen Folgen für die angeschlossenen Systeme und den Datenbestand". Die Wahrscheinlichkeit, dass ein solches Szenario heutzutage auftreten kann, beträgt realistische 40 % - allein der finanzielle Schaden durch zu erwartenden Datenverlust dürfte hier leicht 100.000 € und mehr erreichen. Lässt sich durch eine angenommene Investition in Höhe von 20.000 € die Eintrittswahrscheinlichkeit des identifizierten Risikos auf 5 senken, ergibt sich das folgende Bild (sofern der Schaden bei Eintritt unverändert mit 100.000 € angesetzt wird):

Risikowert des Risikos vor der Investition:
R(r) = 100.000 € x 0,40 = 40.000 €

Risikowert des Restrisikos nach getätigter Investition:
R(rr) = 100.000 € x 0,05 = 5.000 €

Bezogen auf einen Betrachtungszeitraum von einem Jahr beträgt die Amortisationsdauer der Investition damit 1:1,75 = 0,6 Jahre, also etwa sieben Monate.

Bei einer hierfür notwendigen Investition in die Informationssicherheit von 20.000 € folgt eine Verminderung des Riskowerts um den Faktor:

(40.000 € - 5.000 €): 20.000 € =1,75

Innerhalb des Betrachtungszeitraums ist die Verminderung des Riskowerts des Risikos also 1,75-mal größer als der investierte Betrag. Bezogen auf einen Betrachtungszeitraum von einem Jahr beträgt die Amortisationsdauer der Investition damit 1:1,75 = 0,6 Jahre, also etwa sieben Monate.

Kostenersparnisse pro Monat im Detail			
1 Abwehr von Hacker Angriffen			
Betriebskosten Paketfilter und Serversicherheit	2.100 €		
Potentieller Schaden Paketfilter ohne dedizierten Firewall-Schutz	619 €		
Betriebskosten Firewall		1.529 €	
Potentieller Schaden Firewall		41 €	
Gesamt	**2.719 €**	**1.570 €**	**1.149 €**
2 Virenschutz			
Betriebskosten ohne zentrale verwalteter Antivirus-SW	823 €		
Potentieller Schaden ohne zentrale verwalteter Antivirus-SW	1.327 €		
Betriebskosten mit zentral-verwalteten Antivirus-SW		893 €	
Potentieller Schaden mit zentral-verwalteten Antivirus-SW		195 €	
Gesamt	**2.150 €**	**1.088 €**	**1.062 €**
3 Sichere Kommunikation in Unternehmensnetzen			
Betriebs- und Kommunikationskosten ISDN-Verbindung	4.134 €		
Betriebs- und Kommunikationskosten IP-VPN-Verbindung		1.432 €	
Gesamt	**4.134 €**	**1.432 €**	**2.702 €**
4 Sicherer Remote LAN Zugriff auf Unternehmensressourcen			
Betriebs- und Kommunikationskosten ISDN-Verbindung	5.513 €		
Betriebs- und Kommunikationskosten sichere RLA-Verbindung		2.594 €	
Gesamt	**5.513 €**	**2.594 €**	**2.919 €**

Beispiel-Detaildarstellung der einzelnen Einsparungen für sichere Kommunikation.

Anwenderspezifische Größen

Der Return on Investment, also die Rentabilität von Investitionen in die Sicherheit, kann für jede Sicherheitslösung individuell errechnet werden. Allerdings lässt sich dieser Wert nicht einfach durch die Entwicklung eines allgemein gültigen Kalkulators etwa in Form einer Excel-Tabelle festmachen. Vielmehr ist eine flexible Betrachtung notwendig, die anwenderspezifische Größen berücksichtigt.

So ist auch eine Risikoanalyse zur Bestimmung und Bewertung der schutzbedürftigen Ressourcen notwendig, damit Anhaltspunkte über potenzielle Schäden sowie deren Eintrittswahrscheinlichkeiten transparent und nachvollziehbar sind.

Darüber hinaus sollten bei der Betrachtung unter anderem auch die Ausgaben für Organisation und Personal sowie für Service und Support in die Kostenberechnung einfließen. Außerdem sind Investitions- und Abschreibungszyklen kalkulatorisch zu berücksichtigen.

Vorfall: Hacker durchdringt Firewall		Paketfilter	Firewall
Hacker stiehlt Daten (Wirtschaftsspionage)			
Anzahl der (erfolgreichen) Vorfälle pro Jahr		0,015	0,001
Wenn ein Daten gestohlen werden, dann...			
Wirtschaftlicher Schaden in % vom sensiblen Daten	20%		
Wirtschaftlicher Schaden in Euro pro Vorfall	250.000 €		
Potentieller Schaden pro Jahr		3.750 €	250 €
Hacker ändert Daten (Web-Page ändern)			
Anzahl der (erfolgreichen) Vorfälle pro Jahr		0,150	0,010
Wenn ein Daten gestohlen werden, dann...			
Image Schaden in % vom Jahresmarketingbudget	2%		
Wiederherstellungsaufwand in Administratorstunden	2 h		
Wirtschaftlicher Schaden in Euro pro Vorfall	10.140 €		
Potentieller Schaden pro Jahr		1.521 €	101 €
Hacker benutzt Server als "Sprungbrett"			
Anzahl der (erfolgreichen) Vorfälle pro Jahr		0,150	0,010
Wenn ein Daten gestohlen werden, dann...			
entstehende Kommunikationskosten	1.000 €		
Wiederherstellungskosten (Server "bereinigen", Strafverfolgung...) in Administratorstunden	40 h		
Wirtschaftlicher Schaden in Euro pro Vorfall	3.800 €		
Potentieller Schaden pro Jahr		570 €	38 €
Potentielle Kosten der Schäden pro Jahr		7.425 €	494 €

Beispiel-Gegenüberstellung von Schutzmechanismen und Angriffszenarien.

Jedes Unternehmen sollte das Ausmaß verschiedener möglicher Gefahren abschätzen und seine Sicherheitsbedürfnisse priorisieren. Die zu schützenden Ziele und ihr wirtschaftlicher Wert können in einer Riskoanalyse ermittelt werden.

Im Rahmen der Analysen sind die Downtimes von IT-Services sowie die genannten allgemeinen Sicherheitsprobleme zu bewerten. Als Ergebnis wird die Risikosituation im Hinblick auf die Abhängigkeit von IT-Ressourcen und -Services (operationelles Risiko) und die Informations-Sicherheit dokumentiert.

Die Verantwortung für die Durchführung der Riskoanalyse liegt beim jeweiligen Geschäftsverantwortlichen. Initiatoren und daran aktiv Beteiligte sind daneben vor allem die Revision, die ClOs, die Informationssicherheitsverantwortlichen und gegebenenfalls Risikomanager der verschiedenen Unternehmensbereiche.

Abschließend lassen sich dann organisatorische und technische Konzepte für die notwendigen Sicher-

Für die meisten Unternehmen sind Sicherheitsgrundsätze (Policies) und -lösungen eine individuelle Angelegenheit, die an die spezifischen Gegebenheiten angepasst werden müssen.

Dazu gehört neben den benötigten Regeln und Sicherheitsmanagementprozessen auch die Abwägung des Risikos gegen die notwendigen Investitionen.

heitsmaßnahmen inklusive der erforderlichen Finanzpläne erstellen. Auf diese Weise werden alle notwendigen Daten erhoben, die auch für die Berechnung des Return on Investment benötigt werden.

Unternehmensprofil	
Angaben für die Paketberechnung	
Anzahl Mitarbeiter	1.000
Gebäudesicherheit	
Anzahl Türterminals (für Gebäude- und Raumzutritt)	12
Arbeitsplatzsicherheit	
Anzahl Mitarbeiter mit PC-Zugriffsschutz	1.000
Elektronische Geldbörse	
Anzahl automatische Aufladestationen	6
Anzahl manuell-bedienbare Aufladestationen	1
Anzahl Kantinenkassen	10
Anzahl Automatenkassen	0
Angaben zur RoSI-Berechnung	
Umsatz pro Jahr	40 Mio. €
Paketpreis / Return on Security Investment	
Paketpreis	281.171 €
Amortisierungsdauer der Investition	14,1 Monate
Kostenersparnis pro Monat	19.954 €

Beispieldarstellung einer Return-of-Security-Investment Kalkulation für den Einsatz von multifunktionalen Mitarbeiterausweisen.

Fazit

Für die meisten Unternehmen sind Sicherheitsgrundsätze (Policies) und -lösungen eine individuelle Angelegenheit, die an die spezifischen Gegebenheiten angepasst werden müssen. Um beim Wettlauf zwischen Sicherheitsbedrohungen und Vorbeugung schnell zu sein, benötigen Firmen eine vorausschauende, ganzheitliche Strategie.

Zu diesem Zweck sollte eine umfassende Sichtweise entwickelt werden, die Sicherheit als organisationsübergreifende Aufgabe definiert. Dafür sollten ausnahmslos alle potenziellen Bedrohungen identifiziert und Methoden zur Prävention vorgesehen werden.

Lücken in der Sicherheit erlauben keine Diskussion über "wer bezahlt das", und die Aussage "es ist doch bisher noch nichts passiert" basiert auf der Argumentation mit dem Faktor Glück.

Hierzu gehört auch das Bewusstsein, dass der Mensch immer das schwächste Glied in der Sicherheitskette darstellt. Hinzu kommen die sorgfältige Risikoanalyse und die Bestimmung der notwendigen Sicherheitsanforderungen. Auf dieser Basis können die bereits vorhandenen Sicherheitsvorkehrungen systematisch bewertet und eine robuste Sicherheitspolitik definiert werden. Dazu gehört neben den benötigten Regeln und Sicherheitsmanagementprozessen auch die Abwägung des Risikos gegen die notwendigen Investitionen.

Die Revision kann hier als Initiator mit einer verhältnismäßig neutralen Sichtweise dienen. Das Aufzeigen von Schwachstellen und die Empfehlung zu deren Beseitigung mit den Hinweisen auch auf betriebswirtschaftliche Vorteile lässt eine Umsetzung sicherlich schnell realisierbar machen.

Denn Lücken in der Sicherheit erlauben keine Diskussion über "wer bezahlt das", und die Aussage "es ist doch bisher noch nichts passiert" basiert auf der Argumentation mit dem Faktor Glück. Nur dieser Faktor ist eine nicht definierte mathematische Größe und somit ein unbekanntes Risiko. ✤

+++ Vorschau PRev III-2006 +++

Lesen Sie in der nächsten Ausgabe von PRev Artikel unter anderem zu folgenden Themen:

- Formelle und materlielle Brechtskritik
- Überblick über die SAP® IS-U-Funktions- und Berechtigungsanpassung durch IDEX-GE
- SAP® Business Information Warehouse Chancen und Risiken - Teil III
- Prüfen durch alle Schichten
- Prüfung einer WAN-Infrastruktur

Seminarcode: **R3GB**
31.08.-01.09.06

Revisionsführerschein für SAP® Systeme

Inhalte u.a.:

Einführung:
- SAP R/3® Architektur/Leistung
- Komponenten/Teilkomponenten

Die R/3®-Benutzeroberfläche
- Vergl. zum Windows-Standard
- Matchcode und Modi

Transaktionscodes
- Aufrufen von Anwendungen
- Historienliste

Individuelle Benutzereinstellungen
- Benutzerfestwerte
- Das Benutzermenü

Reports
- Standardreports in den Modulen
- Selektionskriterien

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**
07.09.-08.09.06

Prüfung des Berechtigungskonzeptes von SAP® 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: **R3SY**
11.09.-13.09.06

Systemprüfung von SAP®

Inhalte u.a.:

Basissicherheit:
- Schichten eines SAP-Systems und Gefahrenpunkte
- Systemparameter

Benutzerverwaltung:
- Grundkonzeption
- Lizensierungen

Protokollierungskomponenten
- Systemprotokollierung
- Anwendungslog

Verbuchungsprinzip:
- Gefahrenpunkte der asynchronen Verbuchung

Tabellensteuerung:
- Konzept der Tabellensteuerung
- 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: **R3FI**
14.09.-15.09.06

Revisionsworkshop „Finanzbuchhaltung“ von SAP® 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 Tabellenprotokollierung

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: **R3IS**
18.09.-19.09.06

Nutzung des AIS von SAP® für die Prüfung

Inhalte u.a.:

Einführung in das AIS:
- Struktur des AIS-Berichtsbaums
- Erstellung diverser Sichten auf das AIS
- Überwachung von Fortschrittshandlungen im Rahmen der Prüfungshandlungen größerer Prüfungsabteilungen

Funktionalität
- Einführung in das AIS basierte Kaufmännische Ausit

Auswertung
- Einführung in Auswertungsmöglichkeiten des SAP R/3® via Datentransport in EXCEL, WINIDEA, ACL usw.

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: **R3PF**
25.09.-27.09.06

Prüfungsworkshop zum Modul FI des SAP® Systems

Inhalte u.a.:

Einführung:
- Prüfungsansätze im Rahmen von PS 330/ISA 401
- Prüfleitfaden im Rahmen eines IKS

Workshopthema:
- Prüfung der Ordnungsmäßigkeit der Buchführung nach HGB in Anlehnung an PS 330/ISA 401

Prüfprozedur
- Erstellung eines Handlungsleitfadens
- Durchführung der Prüfungshandlungen
- Dokumentation 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: **R3HR**
09.10.-11.10.06

Revisionsworkshop Personalwesen - HR von SAP® Systemen

Inhalte u.a.:

Einführung in SAP®-HR:
- Projektabwicklung
- Projektmitarbeit der Revision

Grundlagen und Prüfung der Stammdaten

Grundlagen und Prüfung der Zeitwirtschaft

Grundlagen und Prüfung der Personalplanung

Auswertungsmöglichkeiten in SAP® HR

Revisionsaspekte SAP® HR
- Systemlandschaften
- Anforderungen an eine Systemdokumentation

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: **R3CB**
09.10.-10.10.06

Workshop zur Berechtigungsprüfung des Moduls CO von SAP®

Inhalte u.a.:

Spezifikation der Berechtigungskonzeption für das Controlling
- Berechtigungsobjekte des Controlling
- Komplexität und Quantitäten

Berechtigungsvergabe
- Einsatz von Funktionstrennungen
- Prüfen kritischer Berechtigungen und kritischer Kombinationen

Prüfung und Dokumentation
- Erstellung eines Prüfleitfadens zur Berechtigungskonzeption des Controlling
- Auswertungsmöglichkeiten mit SAP® Standardreports und Tabellen

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: **R3KT**
12.10.-13.10.06

Prüfung des Korrektur- und Transportwesens von SAP R/3® Landschaften

Inhalte u.a.:

R/3®-Systemlandschaften
- Mögliche R/3®-Systemlandschaften
- Test- und Freigabeverfahren

Transportwege
- Organisation und Schutz der Transportwege
- Automatische und manuelle Transporte

Rollentrennung beim Transportprozess
- Entwicklung, Qualitätssicherung, Administration
- Funktionstrennung

Das Transport Management System (TMS)

Kontrolle der Importvorgänge

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: **R3BW**
12.10.-13.10.06

Revisionsworkshop "Business Information Warehouse - BW" von SAP® Systemen

Inhalte u.a.:

Einführung
- Architektur von Data Warehouse Systemen
- Einordnung in das Gesamtkonzept
- Funktionalität SAP® BW

Datenbeschaffung prüfrelevanter Daten
- Stammdaten
- Bewegungsdaten

Datenmodellierung und Datenaufbereitung

Reporting und Analyse
- Erarbeitung von Musterlösungen

Sicherheitsrisiken BW
- Datenschutz
- Datensicherheit
- Berechtigungskonzeption

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: **R3HB**
16.10.-17.10.06

Workshop zur Berechtigungsprüfung des Moduls HR von SAP®

Inhalte u.a.:

Spezifikation der Berechtigungskonzeption für die Personalwirtschaft - HR
- Komplexität und Quantitäten
- Verwendungsnachweis
- Fehlerquellen - Fehleranalyse

Strukturelle Berechtigungen
- Konzeption - Einsatz
- Prüfen kritischer Berechtigungen und kritischer Kombinationen

Prüfung und Dokumentation
- Abbildung der Prüfungstätigkeit
- Auswertungsmöglichkeiten mit SAP R/3® Standardreports und Tabellen

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: **R3BD**
18.10.-20.10.06

Gesamtsicherheit durch alle Schichten von SAP® Systemen

Inhalte u.a.:

Die Client/Server-Umgebung unter SAP R/3®

Die Protokollierung von NT/UNIX, Oracle und SAP

Beeinflussung der Ebenen untereinander (Schnittstellen) in hierachischer Betrachtung
- WindowsNT/UNIX und SAP R/3®
- Sicherung der Client-Stationen

Risikomanagement und Sicherheitstrategien

Checklisten und ihre praktische Umsetzung

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: **DSDM**
04.09.-06.09.06

Ordnungsmäßigkeit und Prüfung von Dokumenten-management- und Archiv-Systemen

Inhalte u.a.:

Grundsätze der ordnungsmäßigen Archivierung originärer elektronischer Dokumente
- Datenzugriff der Finanzbehörde
- Steuerlich relevante Daten
- Maschinelle Auswertbarkeit

Theoretische Grundlagen
- Überblick und Einsatzmöglichkeiten
- DMS und digitale Signatur
- Prüfungsmethoden und -verfahren

Praktische Übungen/Workshops
- Erstellung von Prüfungsleitfäden und -checklisten

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: **GMPR**
06.09.-08.09.06

Praktische Projektrevision

Inhalte u.a.:

Einführung
- Projekte: Strategie-Backbone zur Realisierung von Unternehmens-visionen
- Definition und Zielsetzung von Projekten: Chance vs. Risiko
- Projektrevision: Notwendigkeit und Zielsetzung

Prozeß eines Projektes (Fallbeispiele)
- Initiierung und Begründung
- Das Projektteam
- Die Projektlenkung
- Fertigstellung und Abnahme
- Erfolgsmessung
- IT-gestütztes Projektmanagement

Projektrevision (Fallbeispiele)

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: **GMOS**
11.09.-12.09.06

IT-Revision und Outsourcing

Inhalte u.a.:

IT-Outsourcing
- Der Outsourcingprozess
- Generelle Risiken beim Outsourcing
- Kernkompetenzen im Wandel

Vertragsgestaltung

Prüfung des IT-Outsourcing
- Grundlagen der IT-Revision
- Die Revisionscheckliste

Der Revisionsbericht

Dokumentation

Revisionsgespräche mit Outsourcingpartnern

Prüfung des „Daheimgebliebenen“
- Prüfung verbliebener Systeme
- Prüfung von Schnittstellen
- Prüfung von IDV

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: **GMRI**
13.09.-15.09.06

Risikomanagement aus Revisionssicht

Inhalte u.a.:

Risiko und Chance

Kategorisierung von Betriebsrisiken aus Revisionssicht

Anforderungen an ein Risikomanagement-System aus diversen Sichtweisen - Sollvorgaben für die Revision?

Das Risiko-Kataster - Basis einer risiko-orientierten Prüfungsplanung? (Fallbeispiele?)

Aufbau und Prüfung von Frühwarnsystemen

Ordnungsmäßigkeit eines Risikomanagementsystems

IT-gestüztes RMS

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: **DSRF**
14.09.-15.09.06

RACF für Revisoren

Inhalte u.a.:

RACF-Begrifflichkeiten

Installation

Rollen und Rechte

Profile

Dateischutz

General Ressources

Protokollierung

Prüfhilfen

Prüfansätze

Diskussion

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: **DSIK**
18.09.-19.09.06

Prüfung interner Kontroll-systeme (IKS) in der IT auf Grundlage des Sarbanes-Oxley-Acts

Inhalte u.a.:

Das interne Kontrollsystem im Unternehmen

IKS und rechtliche Anforderungen/Normen
- GoBS
- KonTraG / RMS
- IDW PS 260 / PS 330
- SOX / SOA

Kontrollen der IT

Prozessbeschreibungen unter Kontrollgesichtspunkten

Wirksamkeitsprüfung / Testing

Dokumentation der Kontrollen

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: **BWGL**
25.09.-27.09.06

Baurevision - Grundlagen + Praxis mit Spezialproble-matiken

Inhalte u.a.:

Grundlagen Bau
- Kalkulation von Baupreisen
- Prüfsubjekte und -objekte

Praxis (Fallbeispiele)
- Bereich Ausschreibung
- Bereich Ausführung/Abrechnung

Baurevision als Projektrevision
- Projektleitung/-lenkung
- Abnahme-/Freigabeverfahren

Spezialproblematiken
- HOAI
- Nachträge

Grundlagen IT
- AVA-Programme

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: **BKEB**
12.10.-13.10.06

Electronic Banking aus Revisionssicht

Inhalte u.a.:

Techniken im eBanking

HBCI - eBanking

Kryptografische Verfahren beim Einsatz in Banken

Funktion und Qualität von Zertifizierungs-verkehr im Internet

Internet als Kapitalmarkt

Internet als Informationsmarkt

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: **CDXR**
23.10.-25.10.06

EXCEL für Revisoren

Inhalte u.a.:

Handling von Tabellen, Blättern und Mappen

Einlesen von Prüfdaten

Selektionen / Stichprobennahmen

Schichten von Datenbeständen (ABC-Analyse)

Funktionen zur Aufbereitung und Analyse von Daten

Formatierung und Darstellung

Verknüpfen von EXCEL-Tabellen und vergleichende Auswertungen

Automatisierungsmöglichkeiten von sich wiederholenden Prüfabfragen

Individuelle Anpassung

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: **GMSD**
25.10.-27.10.06

Prüfen des Vertriebs

Inhalte u.a.:

Einführung
- Definition und Strategie von Marketing und Vertrieb
- Gesetzliche Randbedingungen und Vertragsbedingungen

Risiken im Vertriebsprozess und Prüfung der Risikosteuerung
- Risikopotential und -ranking
- IT-Werkzeuge zur Prüfung von Umsätzen, Debitoren u.a.m.

Kommunikationsfluss
- Richtlinien/Ethik-Werk für den Vertrieb
- Die Kundenakte

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: **DSW2**
06.11.-08.11.06

Windows® 2000 für Revisoren

Inhalte u.a.:

Aufbau und Struktur des Betriebssystems:
- Leistungsmerkmale
- Eigenschaften der Serverversionen
- Kompatibilität

NTFS 5
- Verschlüsselung
- Prüfungsansätze

Security
- Anmeldesicherheit
- Restriktion für Benutzer

Berechtigungskonzept
- Einführung in ADS
- Gruppen und deren Verschachtelung
- Freigaberechte contra NTFS-Rechte

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: **CDAR**
06.11.-08.11.06

ACCESS für Revisoren

Inhalte u.a.:

Arbeit mit Tabellen/Datenbanken

Einlesen von Prüfdaten in ACCESS

Erstellen von Feldstatistiken

Schichten von Datenbeständen (ABC-Analyse)

Analyse der extrahierten Daten

Verknüpfen von ACCESS-Tabellen und ver-gleichbare Auswertungen

SQL-Abfragen

Zusammenfassung am Beispiel einer kom-pletten interaktiven Prüfung von Datenbeständen inkl. grafischer Auswertung

Automatisierungsmöglichkeiten von sich wiederholenden Prüfabfragen

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

Prof. Dr. Hanno Kirsch

Einführung in die internationale Rechnungslegung nach IFRS

Grundzüge der IFRS. Anwendung im Konzernabschluss. Folgerungen für den Einzelabschluss.

3. wesentlich überarbeitete und erweiterte Aufl. 2006.
Verlag Neue Wirtschafts-Briefe,
524 S., ISBN 3 482 52043 7
29,80 €

Vertiefte Kenntnisse der internationalen Rechnungslegung nach IAS/IFRS sind heute für jeden Studierenden der Betriebswirtschaftslehre sowie für Teilnehmer von Bilanzbuchhalter-Kursen und Kursen zum Bilanzbuchhalter International unabdingbar.

Diese Einführung in die internationale Rechnungslegung nach IAS/IFRS enthält eine systematische Gesamtübersicht über die internationalen Rechnungslegungsstandards. Das Buch schließt sowohl theoretische Grundlagen als auch praktische Umstellungsprobleme ein. Es bietet als Lern- und Nachschlagewerk eine strukturierte Orientierungshilfe auf dem Gebiet der internationalen Rechnungslegung.

Damit der Leser das erarbeitete Wissen sofort anwenden kann, wurden zahlreiche Beispiele und umfangreiche Fallstudien aufgenommen. Besonderer Wert wird auf eine übersichtliche und durch Abbildungen unterstützte Darstellung gelegt.

Die 3. Auflage berücksichtigt die zahlreichen Änderungen und wurde an den aktuellen Stand der IAS/IFRS angepasst. Sie enthält außerdem zwei zusätzliche Fallstudien zu Fertigungsaufträgen und zur Eigenkapitalveränderungsrechnung sowie viele neue Beispiele.

Investitionen sind notwendig, um den Bestand und die Weiterentwicklung der Unternehmen sicherzustellen. Aufgrund des sich anhaltend verstärkenden Kostendruckes und den sich dadurch entsprechend begrenzenden Kostenbudgets spielt die Wirtschaftlichkeit von Investitionen eine bedeutende Rolle.

Dipl.-Kaufmann Prof. Klaus Olfert

Investition

Reihe: Kompendium der praktischen Betriebswirtschaft

10. Auflage 2006.
Friedrich Kiehl Verlag,
522 S., ISBN 3 470 70470 8
24,00 €

Investitionen sind notwendig, um den Bestand und die Weiterentwicklung der Unternehmen sicherzustellen. Aufgrund des sich anhaltend verstärkenden Kostendruckes und den sich dadurch entsprechend begrenzenden Kostenbudgets spielt die Wirtschaftlichkeit von Investitionen eine bedeutende Rolle. Um den Nachweis zu erbringen, müssen sämtliche Investitionsvorhaben der Unternehmen auf den Prüfstand gestellt werden.

Die Aufgaben, die sich der Investition dadurch stellen, werden in diesem Band aus der Reihe "Kompendium der praktischen Betriebswirtschaft" umfassend behandelt. Der Inhalt ist übersichtlich, klar und verständlich aufgebaut. Investitionsmathematische Teile können einfach nachvollzogen werden. Zahlreiche Abbildungen und Beispiele veranschaulichen die thematische Beschreibung. Ergänzt wird die praxisnahe Darstellung durch die bewährten Elemente der Olfert-Kompendium-Reihe. Zur Lernkontrolle dienen insgesamt 500 Fragen sowie ein umfangreicher Übungsteil mit 80 Aufgaben und Lösungen.

Uwe Frank

Das Einmaleins der Entgeltabrechnung

70 Seiten Praxisteil mit Musterlösungen!

3. überarbeitete Auflage 2006,
Datakontext-Fachverlag,
476 S., ISBN 3-89577-407-3
39,00 €

Das Werk vermittelt in praxisbezogener und prozessorientierter Vorgehensweise das grundlegende

und vertiefende Wissen rund um die Lohn- und Gehaltsabrechnung. Viele Beispiele verdeutlichen die komplexe Materie. Ein 70-seitiger Praxisfall mit Musterlösungen gibt dem Leser die Möglichkeit das erlernte Wissen zu überprüfen. Dieser Ratgeber umfasst Grundlagenthemen wie

- Ablauf einer Lohn- und Gehaltsabrechnung, vom Brutto zum Netto
- Aufgaben und Pflichten der Lohnbuchhaltung
- Grundlagen des Lohnsteuer- und Sozialversicherungsrechtes
- Gesetzliche Abzüge und Arbeitspapiere
- Führen von Lohnkonten und Lohnjournalen
- Gesetzliche Aufzeichnungs- und Meldepflichten

bis hin zur ausführlichen Behandlung spezieller Sachverhalte wie z. B.

- alle Neuerungen im Lohnsteuer- und Sozialversicherungsrecht
- Einmalbezüge und Abfindungen
- Minijobs und Gleitzonenbeschäftigungen
- Firmen-Kfz und andere Sachbezüge
- Pauschalversteuerung
- Schüler, Studenten und Praktikanten
- Pfändung von Arbeitslohn

Das Einsteigerwerk von Frank hat sich mit der dritten Auflage mittlerweile in der Praxis etabliert und gehört zur Standardliteratur in der betrieblichen Ausbildung.

Zielgruppe:
Das Werk dient in idealer Weise Neulingen als Einstieg in das komplexe Thema, aber auch erfahreneren Praktikern zur Auffrischung bzw. Vertiefung Ihres Wissens.

Kai-Uwe Marten, Reiner Quick, Klaus Ruhnke

Lexikon der Wirtschaftsprüfung

Nach nationalen und internationalen Normen

Auflage 2006,
Schäffer-Poeschel Verlag,
929 S., ISBN 3-7910-2103-6
59,95 €

Das Lexikon erläutert in mehr als 500 Stichwörtern alle wichtigen Begriffe der Wirtschaftsprüfung im nationalen und internationalen Kontext. Behandelt werden neben der Abschlussprüfung auch andere gesetzliche und freiwillige Prüfungsleistungen sowie angrenzende Bereiche wie z.B. Berufsaufsicht, Balanced Scorecard, Beratung und Prüfung, Erwartungslücke, kontinuierliche Prüfung, Unternehmensbewertung oder die Prüfung von Börsenprospekten, Energieversorgungsunternehmen, Genossenschaften, Kreditinstituten und Versicherungsunternehmen.

Die Autoren stellen die Mehrzahl der Stichworte kompakt und knapp dar; einzelne Stichworte höherer Komplexität werden in abgeschlossenen Kurzbeiträgen behandelt. Ein Wesensmerkmal des Nachschlagewerkes ist die strukturierte Behandlung zentraler Abschlussposten nach einem festen Bearbeitungsschema, welches dem Leser zunächst die relevanten Rechnungslegungs- und Prüfungsnormen benennt, den zu behandelnden Bereich aus dem Blickwinkel der IFRS und des HGB kurz darstellt und anschließend die Prüfung insbesondere nach ISA und IDW PS erläutert. Eine umfassende Querverweistechnik sowie die Aufnahme von Schlagworten der aktuellen Diskussion machen dieses Lexikon zu einem wertvollen Nachschlagewerk für Praktiker und Studierende sowie für an Forschungsfragen interessierte Personen.

Dr. Matthias Heiden

Pro-forma-Berichterstattung

Reporting zwischen Informationen und Täuschung

Auflage 2006,
Erich Schmidt Verlag,
594 S., ISBN 3 503 09327 3
69,00 €

Im Sog der Bilanzskandale ist auch die Pro-forma-Berichterstattung ins Blickfeld der Öffentlichkeit geraten. An Stelle handelsrechtlicher Rechnungslegung rücken weltweit immer mehr Unternehmen, Medien und Analysten als "pro forma" bezeichnete Fantasiekennzahlen in den Vordergrund. Zwar kommt man damit Transparenzanforderungen und -bedürfnissen nach und beseitigt Unstetigkeiten. Zum anderen aber geht es oft schlicht darum, progressive Ergebnispolitik zu betreiben.

Die Pro-forma-Berichterstattung pendelt so zwischen wertvoller Information und Unglaubwürdigkeit, zwischen echtem Nutzen und bloßer Täuschung. Um nun aber Pro-forma-Informationen in all ihren Facetten zutreffend einzuordnen, stellen sich zahlreiche komplizierte Fragen:

- Was verbirgt sich hinter dem Begriff der Pro-forma-Berichterstattung?
- Welche Varianten der Pro-forma-Berichterstattung existieren?
- Welche Ziele verfolgen Unternehmen mit Pro-forma-Informationen?
- Welche Vorschriften sind für kapitalmarktorientierte deutsche Unternehmen zu beachten?
- Sind Informationsintermediäre und Anleger in der Lage, Pro-forma-Ergebnisinformationen sachgerecht zu interpretieren?

Das neue Buch von Matthias Heiden gibt auf die zentralen Fragen der Pro-forma-Berichterstattung fundierte und zielführende Antworten. Erstmalig wird grundlegend das komplexe Terrain der Pro-forma-Berichterstattung praxisgerecht erschlossen.

Die Vorschriften der für deutsche Unternehmen maßgeblichen Normensysteme, der IAS/IFRS und der US-GAAP werden analysiert und Ausgestaltungsmöglichkeiten aufgezeigt.

Prof. Dr. Michael Klotz, Dr. Dietrich-W. Dorn

Vertragsmanagement in der Informationsverarbeitung

Handbuch für Planung, Durchführung und Controlling von IT-Verträgen

Auflage 2006,
Erich Schmidt Verlag,
206 S., ISBN 3 503 09317 6
44,00 €

Anzahl und Verschiedenartigkeit von Verträgen in der betrieblichen Informationsverarbeitung (IV) nehmen ständig zu. Außer Beschaffungs- und Wartungsverträgen für Hard- und Software-Erstellungs- und Nutzungsverträgen gibt es zunehmend Systemverträge, Schulungs- und Beratungsverträge, IV-Infrastrukturverträge und weitere IV-Dienstleistungsverträge. Darüber hinaus verändert sich die Qualität von IT-Verträgen hinsichtlich Auftragshöhe, Langfristigkeit der Zusammenarbeit mit dem Vertragspartner, Internationalität und Umfang der Vertragsrisiken. Der Umgang mit IT-Verträgen ist also hochkomplex. Juristische Regelungen und Management-Perspektiven sind eng miteinander verzahnt. Oft kommt es gerade hier zu teuren und langwierigen Konflikten.

Vermeiden Sie schwierige oder sogar existenzielle Probleme und sorgen Sie lieber mit einem wirkungsvollen IV-Vertragsmanagement vor.

Vermeiden Sie schwierige oder sogar existenzielle Probleme und sorgen Sie lieber mit einem wirkungsvollen IV-Vertragsmanagement vor. Dieses umfasst nicht nur die Abmahnung, den Abschluss und die Verwaltung von IT-Verträgen, sondern vor allem auch planerische und steuernde Maßnahmen in der Vetragsdurchführung.

In ihrem neuen hochaktuellen Buch erläutern Ihnen Michael Klotz und Dietrich-W. Dorn verständlich und praktisch sofort umsetzbar alles Wichtige

- zu den Grundlagen des IV-Vertragsmanagements
- zu den verschiedenen Vertragsarten
- zur Vertragsplanung und -gestaltung
- zum Controlling der IT-Verträge oder
- zur Steuerung des Vertragsportfolios.

Viele Beispiele mit praktischen Bezügen und zahlreiche Checklisten mit über 700 Checkpoints erleichtern Ihnen die Einarbeitung in diese wichtige Materie. Zusätzlich werden Sie durch die dem Buch beiliegende CD-ROM bei Ihrer praktischen Arbeit unterstützt.

Raimund Weyand, Judith Diversy

Insolvenzdelikte

Unternehmenszusammenbruch und Strafrecht

7., überarbeitete Auflage 2006,
Erich Schmidt Verlag,
246 S., ISBN 3 503 09324 9
36,80 €

Im Zusammenhang mit fast allen Firmeninsolvenzen werden Straftaten begangen, welche die Staats-

anwaltschaft auf den Plan rufen. Langfristige und oft kostspielige Ermittlungsverfahren schließen sich fast immer an.

Nicht nur für die wirtschaftliche Existenz der betroffenen Unternehmer hat dies in den meisten Fällen gravierende Folgen. Haftungsansprüche von Geschäftspartnern, Kreditinstituten und der öffentlichen Hand stehen ebenso im Raum wie massive strafrechtliche Konsequenzen.

Haftungsansprüche von Geschäftspartnern, Kreditinstituten und der öffentlichen Hand stehen ebenso im Raum wie massive strafrechtliche Konsequenzen.

Dieses seit Jahren bewährte Standardwerk

- bietet einen umfassenden Überblick über den aktuellen Stand der Rechtsentwicklung,
- orientiert sich konsequent an der für die Praxis bedeutsamen Rechtsprechung,
- vermittelt gleichzeitig wichtige Einsichten in die Praxis der Ermittlungsbehörden,
- beschreibt detailliert die typischen Tatbestandsmerkmale von Insolvenzdelikten und
- verschafft durch Schaubilder einen schnellen Überblick über die komplexe Materie.

Raimund Weyand ist Oberstaatsanwalt und Stellvertretender Leiter der Staatsanwaltschaft Saarbrücken und befasst sich seit vielen Jahren mit dem Wirtschafts- und Steuerstrafrecht. Judith Diversy ist als Staatsanwältin für Steuer- und Wirtschaftsdelikte zuständig und war vorher Anwältin in einer großen wirtschafts-rechtlich ausgerichteten Kanzlei.

Peter Wolff

Die Macht der Blogs

Chancen und Risiken von Corporate Blogs und Podcasting in Unternehmen

1. Auflage 2006,
Datakontext-Fachverlag,
164 S., ISBN 3-89577-409-X
19,00 €

Seit Monaten ist das Phänomen der Blogs oder Weblogs in aller Munde. Mit diesem neuen Internettrend werden Ansätze diskutiert, das Bloggen auch innerhalb eines Unternehmens einzusetzen, um sowohl die Unternehmens- und Mitarbeiterkultur zu fördern, als auch nach außen glaubwürdig und regelmäßig mit seiner Unternehmensumwelt zu kommunizieren. Den sich ergebenden Chancen stehen eine ganze Reihe von Risiken gegenüber. (Ex)-Mitarbeiter z. B. könnten sich wenig schmeichelhaft bis sehr kritisch zum Unternehmen äußern oder geben Firmenwissen preis. Die Gefahren, die sich daraus für das Image und die Marktstellung ergeben, können fatal sein. Doch auch Unternehmen haben die Chance, aus den Beiträgen der Blogosphäre Markttrends und gesellschaftliche Entwicklungen heraus zu lesen und Wettbewerbs- und Umfeldbeobachtung zu betreiben.

Der Autor beschreibt, auf welche Fallstricke Unternehmen vorbereitet sein sollten, wenn sie das Kommunikationsinstrument Blog einsetzen und wie sich ein ehrlicher und persönlicher Dialog zu den Stakeholdern aufbauen lässt.

Der Autor beschreibt, auf welche Fallstricke Unternehmen vorbereitet sein sollten, wenn sie das Kommunikationsinstrument Blog einsetzen und wie sich ein ehrlicher und persönlicher Dialog zu den Stakeholdern aufbauen lässt. Da ein Weblog nur ein Instrument ist, werden die grundsätzlichen Fragen der Unternehmenskultur, Mitarbeiterführung, Wertekultur und Unternehmensethik angesprochen, die zur richtigen Imagepositionierung führen können.

Der Leser erfährt weiterhin, wie ein Weblog aufgebaut und gepflegt werden sollte, wie es sich von einer normalen Internetseite unterscheidet und welche Erfahrungen andere Unternehmen mit einem Corporate Blog gemacht haben. Es werden Monitoringtools vorgestellt, mit denen fremde Blogs analysiert werden, um jederzeit im Bilde zu sein, was "draußen" in der virtuellen Internetwelt über das eigene Unternehmen gesagt wird. Ebenfalls wird erklärt, wie der eigene Unternehmensblog in der Blogosphäre bekannt gemacht wird und wie sich ein Blog auf das Google-Ranking auswirken kann. Darüber hinaus wird der neue Trend des PodCastings vom Autor erläutert. ✤

ABO-Bestellung für PRev

Ein Abo von *Revisionspraxis* beinhaltet folgende Verlagsdienstleistungen:

- Zusendung von *PRev*
- IBS-Prüfmanual (Beilage)
- Zugriffsfreigabe auf umfassende Informationen unter **www.revision-hamburg.de** mit allen jeweils erschienenen 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 mindestens einen Monat vorher möglich.

PRev erscheint quartalsweise (jeweils 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 *Revisionspraxis* 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: _____