

Warum Revisionsberichte
nicht gelesen werden S. 5

Die Bedeutung von Arbeits-
papieren für die Interne
Revision S. 8

Überblick über die SAP®
IS-U-Funktions- und Berechti-
gungsparameter durch
IDEX-GE S. 13

SAP® Business Infor-
mation Warehouse S. 24

Prüfstandards für Datenschutz-
audits - Unterstützung der
Revisionsarbeit S. 29

Prüfung einer "Wide Area
Network"-Infrastruktur am
Beispiel einer ausgelagerten
Dienstleistung S. 34

Prüfung durch alle Schichten . . S. 40

Beilage: IBS-Prüfmanual "Windows® 2000/2003 - Teil III"

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

Rechtliche Hinweise

Der Inhalt dieser Zeitschrift inklusive aller Beiträge und Abbildungen ist urheberrechtlich geschützt. Jede Vervielfältigung oder Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen wird, bedarf der schriftlichen Zustimmung des OSV. Dies gilt auch für Bearbeitung, Übersetzung, Verfilmung, Digitalisierung und Verarbeitung bzw. Bereitstellung in Datenbanksystemen und elektronischen Medien einschließlich der Verbreitung über das Internet. Namentlich gekennzeichnete Artikel geben ausschließlich die persönlichen Ansichten der Autoren wieder. Die Verwendung von Markennamen und rechtlich geschützten Begriffen auch ohne Kennzeichnung berechtigt nicht zu der Annahme, dass diese Begriffe jedermann zur Verwendung oder Benutzung zur Verfügung stehen.

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
© Copyright 2006 by OTTOKAR SCHREIBER VERLAG GMBH, Hamburg
Alle Rechte vorbehalten.

Allgemein

Seminare S. 44

Buchhinweise S. 46

Abonnement S. 50

Impressum S. 3

Verlagshinweis

Nächste Ausgabe der
PREV

November 2006

Redaktions-/ Einsende-
schluss für diese Ausgabe:
31.10.2006

Beilagen dieser Ausgabe:

- Zugangscodes für den Abonnentenbereich auf www.revision-hamburg.de (nur für Abonnenten)
- IBS-Prüfmanual
- IBS Schreiber GmbH "Roadshow 2006"
- Datakontext Fachverlag "IKS-Management"



➔ Grundlagen und Ansätze der Internen Revision

Liebe Leserinnen und Leser,

in Fortsetzung unserer Betrachtungen zum Thema "Berichterstattung der Revision" stellen wir Ihnen nach Vorgabe der Sollvorgaben vom IIR, IDW und IAS in PRev II/06 in dieser Ausgabe PRev III/06 die Themen "Warum Revisionsberichte nicht gelesen werden" und "Die Bedeutung von Arbeitspapieren" zur Diskussion.

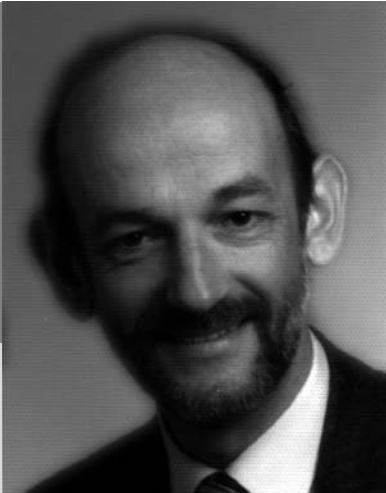
Im Revisionsbericht manifestieren sich das Arbeitsergebnis der Revision und ihre Arbeit an sich. Selbstverständliches Ziel des Berichts muss seine Effektivität sein, nämlich dass die Feststellungen in ihrem jeweiligen risikobezogenen Stellenwert ernst genommen und die daraus abgeleiteten Empfehlungen auch umgesetzt werden. Haub stellt in seinem Beitrag humorgewürzt vor, warum Revisionsberichte wegen Darstellungsmängeln und mangels Überzeugungskraft oft nicht gelesen werden geschweige wirksam sind.

Ernst genommen werden die Prüfergebnisse dann und nur dann, wenn sie "revisionsfest" sind. Deswegen stellen die Arbeitspapiere das maßgebliche "Rückgrat" für den Bericht dar, wie Sie dem Beitrag von Bosse entnehmen können.

Viel konstruktive Diskussion zu diesem "immerwährenden" Revisionsthema und viele Stellungnahmen von Ihnen wünscht sich wie immer

Ihr

Ottokar R. Schreiber



➔ Warum Revisionsberichte nicht gelesen werden

Frank Haub

In meinen Revisionsseminaren befrage ich die Teilnehmer, ob und welche Fehler sie denn schon einmal bei der Berichterstellung in der Revisionsabteilung gemacht haben. Verblüffend, was dabei herauskommt. Selbst Berufsanfänger, die noch keinen Bericht geschrieben haben, kommen auf die interessantesten Fehlermöglichkeiten.

Denken wir also schon an Fehler, bevor wir mit der Arbeit begonnen haben?

Nein? Um das Gegenteil zu beweisen, biete ich Ihnen einen kleinen Strauß an

Fehlermöglichkeiten aus meinen Seminaren an:

- subjektive Einschätzungen
- „Zahlenfriedhöfe“
- belehrender Berichtsstil („Oberlehrer“)
- kein Einsatz von Grafiken
- zu lange Sätze („Bandwurmsätze“)
- unstrukturierter Aufbau
- Summary fehlt
- Empfehlungen fehlen
- Rechtschreibfehler

Aus meiner langen Revisionserfahrung möchte ich auf die Frage „Warum werden Revisionsberichte nicht gelesen?“ Antworten gebündelt, in vier Blöcken geben.

Diätplan für Berichte

Ein leidiges Thema ist immer wieder: Wie lang und wie umfangreich darf ein Revisionsbericht sein?

Haben Sie schon einmal erlebt, dass sich Ihr Vorstand über einen zu kurzen Bericht beklagt hat? Das Gegenteil ist doch der Fall. Wir schreiben zu umfangreiche Berichte! Der Berichtsempfänger legt schon einmal den Bericht des Umfangs wegen beiseite und hebt ihn sich (vielleicht) für seinen nächsten Urlaub auf.

These 1:

Der Bericht ist kein Ablageplatz für die Arbeitspapiere. Das Fundament und die Mauern unseres Revisionshauses sind die Arbeitspapiere, der Bericht ist nur das Dach.

Der Satzbau in unseren Berichten ist viel zu lang. Sätze mit mehr als 25 Wörtern sind sehr schwer verständlich. Zählen Sie einmal Ihre Sätze nach Wörtern aus. Revisoren werden hinsichtlich Schachtel- und Bandwurmsätzen nur noch von Juristen übertroffen. In Gesetzestexten finden wir Sätze mit 50, 60 und mehr Wörtern. Die Absätze in Texten sind viel zu lang. Man beachte, dass die längsten Absätze zuletzt gelesen werden. Das kann aber auch heißen, sie werden nie gelesen. Denken Sie beispielsweise daran, dass niemand einen Brief im ersten Moment konsequent von oben bis unten liest. Im Brief sollte der erste Absatz der kürzeste sein, der letzte darf der längste sein.

These 2:

Je kürzer die Sätze, desto besser die Verständlichkeit. Füllwörter, Wiederholungen,

Überflüssiges streichen! Absätze sollten vier bis max. sieben Zeilen haben.

Redaktionelles Pech

Wir schreiben unseren Bericht aus unserer Sicht. Setzen Sie sich doch einmal die Brille ihres Berichtsempfängers auf. Plötzlich stellen Sie fest, dass Sie eine Revisionsprache vermitteln (Zunftjargon), die der Empfänger nicht versteht oder missinterpretiert. Wenn Sie schreiben „Es ergaben sich keine wesentlichen Beanstandungen“, meinen wir es als Lob, der Leser fasst es jedoch als Kritik auf.

These 3:

Erfolgreiche Berichtsverfasser verwenden Tatsachen, Ideen und Gefühle, die ihre Leser kennen oder anerkennen.

Der „eilige Revisor“ macht aus einer Auskunft eine Prüfungsfeststellung. Beispiel: „Wir stellten fest, dass die im Oktober vergangenen Jahres häufig aufgetretenen Arbeitsfehler auf eine schlechte Stimmung in der Abteilung zurückzuführen waren.“ Das stimmt natürlich formulierungsmäßig nicht. Es handelt sich stattdessen nur um eine Auskunft. Die richtige Formulierung müsste lauten: „Lt. Auskunft von Herrn/Frau... sollten die Arbeitsfehler auf von uns nicht mehr nachzuvollziehende Situationen zurückzuführen sein.“

Ich lese immer wieder in Berichten Ungenauigkeiten und Unpräzises. Kürzlich schrieb ein Revisor zum Schluss seiner Prüfungsaussagen: „Die Verluste bewegten sich im zweistelligen Millionenbereich“. Damit bietet er eine Bandbreite von 10 bis 99 Millionen an. Und welche Währung war gemeint? Dollar, Lire, Euro?

Wenn Menschen miteinander kommunizieren, tun sie es - jeder für sich - auf unterschiedliche Art, ausgeprägt auf den vier Ebenen.

These 4:

Zahlen, Daten, Fakten exakt und vollständig zu präsentieren heißt sauber recherchiert und professionell revidiert zu haben. Ungeprüfte Zahlen und Sachverhalte - sofern sie überhaupt zu erwähnen sind - müssen als solche dargestellt sein.

Kommunikation, die schöne Unbekannte

Haben Sie sich schon einmal mit den bekanntesten Kommunikationsmodellen beschäftigt? Schade! Ein spannendes Modell beschreibt Schulz von Thun in seinen Büchern "Miteinander reden: Störungen und Klärungen" Band I und II. Darin schildert er vier Kommunikationsebenen:

- Sachinhalt = Prüfungsfeststellungen
- Appell = Empfehlungen
- Beziehung = persönliche Einstellung zum Geprüften
- Selbstdarstellung = persönliche Darstellung des Revisors

Wenn Menschen miteinander kommunizieren, tun sie es - jeder für sich - auf unterschiedliche Art, ausgeprägt auf den vier Ebenen. Der eine ist sehr sachbezogen, er wird also den Sachinhalt besonders beachten, der nächste ist ein Appellmensch, der daran denkt, was er tun muss, der dritte ist auf der Beziehungsebene Zuhause und der vierte ist ein ausgesprochener Selbstdarsteller.

Analog dazu operieren wir als Berichtsschreiber auch unterschiedlich auf diesen vier Ebenen. Sind wir sehr sachbezogen, wird der Bericht vielleicht zu nüchtern sein. Haben wir ein übersteigertes Selbstdarstellungsbedürfnis, wird der Bericht wahrscheinlich zu subjektiv.

Zurückkommend auf unsere Frage „Warum werden Revisionsberichte nicht gelesen?“ wollen wir diese vier Ebenen aus der Sicht des Berichtsempfängers einmal analysieren:

- | | |
|------------|--|
| Ebene | Reaktion des Empfängers |
| Sachinhalt | „Das Prüfungsthema interessiert mich nicht“ |
| Appell | „Ich habe keine Zeit, Empfehlungen umzusetzen“ |

Wenn ein Revisionsbericht auf den Tisch des Geprüften kommt, hat er dann Vorteile oder Nachteile? Wenn nichts Positives vermerkt ist, hat er für ihn nur Nachteile. Also wird er nicht gelesen.

Beziehung	„Der Revisor hat mich während der Prüfung gestört“
Selbstdarstellung	„Wenn Herr/Frau XY diesen Bericht geschrieben hat, weiß ich schon vorher, welche Gemeinheiten er wieder verbreitet“

Dieses sind Negativbeispiele, wie Geprüfte auf den unterschiedlichen Ebenen reagieren könnten. Sie können in allen Fällen dazu führen, dass der Bericht nicht gelesen wird. Kürzlich berichtete mir einer meiner Referenten aus dem öffentlichen Dienst, dass der Geprüfte den Bericht nicht gelesen, ja, nicht akzeptiert hat aus folgendem Grund: Der Revisor hatte das SPD-Parteibuch in der Tasche und der Geprüfte war CDU-Mitglied.

Prof. Vögele, der bekannteste Trainer der Direktmarketing-Branche, stellt in seinem neuesten Buch „99 Erfolgsregeln für Direktmarketing“ u.a. die Frage: „Wie retten wir unsere Mailings vor dem Papierkorb?“ Seine Antwort: „Das Mailing muss mehrere Wegwerfwellen überleben!“

Analog zu unseren Prüfungsberichten wollen wir zwar nun nicht von Wegwerfwellen, aber doch von „Nichtlese-Wellen“ reden.

These 5:

Wir sollen empfängerorientierter denken und schreiben. Dabei sind auch die unterschiedlichen Ausprägungen und Wirkungsweisen der oben beschriebenen Kommunikationsebenen zu beachten!

Psychologisches Unglück

Seit Jahren diskutiere ich in meinen Seminaren mit den Teilnehmern kontrovers das Thema, ob im Bericht auch Positives aufgenommen und dargestellt wird. Die Teilnehmer bejahen es im allgemeinen, in den Unternehmen gibt es jedoch immer noch die gegenteilige Meinung. "Uns interessiert nur, wenn etwas nicht geklappt hat. Wenn alles in Ordnung ist, brauchen wir auch keinen Bericht". So ist von Kollegen, Vorgesetzten und Managern zu hören.

Ich zitiere nochmals Prof. Vögele. Sein Grundprinzip lautet:

"Wir lesen nur, wenn es mit Vorteilen verbunden ist." Dieses Prinzip bezieht sich zwar auf Direktmailings. Wenn ich also etwas nur lese, wenn es mit Vorteilen verbunden ist, heißt das für jeglichen Lesestoff, dass ich zumindest motiviert sein muss; also kaufe ich mir ein Buch, weil mich der Titel interessiert. Ich kaufe mir einen Roman, den ich als spannend einschätze oder ein anderes Buch verschafft mir beim Lesen Entspannung.

Wenn ein Revisionsbericht auf den Tisch des Geprüften kommt, hat er dann Vorteile oder Nachteile? Wenn nichts Positives vermerkt ist, hat er für ihn nur Nachteile. Also wird er nicht gelesen.

Aber halt, er wird ihn wohl doch lesen. Warum? Während der Prüfung wurde beim Geprüften so manches festgestellt. Neugierig, was und vor allem, wie der Revisor es beschrieben hat (siehe die vier Kommunikationsebenen), liest er doch den Text. Zum ersten Mal hat der Geprüfte jetzt die einmalige Chance, in die Rolle des Revisors zu schlüpfen. Er untersucht den Text nach Fehlern des Revisors und wird fündig. Es haben sich Rechtschreibfehler eingeschlichen, ungeprüfte Behauptungen sind aufgestellt, Auskünfte sind unglaubwürdig, er findet polemische Äußerungen und: Es steht nichts Positives im Bericht.

These 6:

Es ist notwendig, in einem Prüfungsbericht nicht nur gefundene Fehler aufzuzeigen, sondern neben Schwachstellen auch angemessen die Starkstellen herauszustellen. Berichte werden dann wieder gelesen, wenn sie auch mit Vorteilen verbunden sind! ❖



➔ Die Bedeutung von Arbeitspapieren für die Interne Revision

Richard Bosse
Techniker Krankenkasse

1 Vorbemerkungen

Als "Produkt" der Revision wird im Allgemeinen nur der Revisionsbericht wahrgenommen. Er gilt letztendlich auch als Visitenkarte der Revision. Daneben, bzw. als Grundlage für den Revisionsbericht, werden während der Prüfung jedoch laufend Arbeitspapiere erstellt. In der Außenwirkung führen sie ein stiefmütterliches Dasein, da in aller Regel nur in Beweis-situationen darauf zurückgegriffen werden muss. Für den Revisionsprozess haben sie jedoch eine eminent wichtige Funktion. Das vorliegende Papier stellt die Funktion und Bedeutung von Arbeitspapieren für die Revision dar. Es orientiert sich im Wesentlichen an dem Standard 2330 (Aufzeichnung von Informationen) des Institute of Internal Auditors (IIA) und den sich daraus ergebenden praktischen Ratschlägen

- 2330-1 (Aufzeichnung von Informationen)
- 2330.A1-1 (Kontrolle der Prüfungsunterlagen)
- 2330.A1-2 (Rechtliche Erwägungen bei der Gewährung des Zugangs zu den Prüfungsunterlagen)
- 2330.A2-1 (Aufbewahrung von Unterlagen)

2 Definition und Zielsetzung

Das Institute of Internal Auditors (IIA) hat in dem Standard 2330 festgelegt, dass die "Internen Revisoren alle relevanten Informationen zur Begründung der Schlussfolgerungen und Revisionsergebnisse aufzeichnen". Dies geschieht üblicherweise in den Arbeitspapieren. Auskonkretisiert kann man Arbeitspapiere definieren als:

Die übersichtlich und zweckmäßig geordnete Gesamtheit der Arbeits- und Fragebögen, auf denen der Revisor eigene Feststellungen und andere Angaben aufgeschrieben hat, einschließlich der schriftlichen Unterlagen, die er von anderen ergänzend zu seinen eigenen Aufzeichnungen erhalten hat. Die Arbeitspapiere sollen die im Einzelnen durchgeführten Prüfungsschritte (Prüfungshandlungen) und angewendeten Methoden, die dazu herangezogenen Unterlagen, durchgeführten Berechnungen und Prüfungsmaßnahmen enthalten, und zwar so systematisch geordnet, dass sie nicht nur als Grundlage der Berichterstattung, sondern auch zu ihrer Vertiefung dienlich sein und von Dritten nachvollzogen werden können.

Grundsätzlich gilt für Arbeitspapiere das gleiche wie in den GoBS definiert: Ein fachkundiger Dritter muss anhand der Arbeitspapiere die Prüfung und den Revisionsbericht in angemessener Zeit eindeutig und leicht nachvollziehen können.

Die Arbeitspapiere bieten i.d.R. einen höheren Detaillierungsgrad der Revisionskenntnisse als der Revisionsbericht. Sie unterstützen somit speziell im Schlussgespräch die Nachvollziehbarkeit und Akzeptanz der Revisionsergebnisse durch die geprüfte Organisationseinheit.

3 Funktion von Arbeitspapieren

Arbeitspapiere dienen im Allgemeinen als:

- Hauptgrundlage für die Berichterstattung über den Auftrag.

- Hilfe bei der Planung, Durchführung und dem Review von Aufträgen.
- Dokumentation, ob die Auftragsziele erreicht wurden.
- Basis für Überprüfungen durch Dritte.
- Basis für die Bewertung des Qualitätsprogramms der Internen Revision.
- Beleg in Situationen wie "geltend machen" von Versicherungsansprüchen, bei Betrugsfällen und im Rahmen von Gerichtsverfahren.
- Hilfsmittel für die Ausbildung der Internen Revisoren.
- Nachweis für das Einhalten der Internationalen Standards für die berufliche Praxis der Internen Revision durch die Interne Revision (Standards).

Im Detail stellen sich die wesentlichen Funktionen wie folgt dar:

a) Prüfungsvorbereitung

Die Arbeitspapiere dienen der Vorbereitung der Prüfung oder entstehen bei der Prüfung bzw. werden während der Prüfung übernommen. Ein nachträgliches "In Form bringen" ist reiner Selbstzweck und sollte tunlichst vermieden werden.

b) Detailangaben zum Revisionsbericht

Mit der nachvollziehbaren Führung von Arbeitspapieren wird vermieden, dass die Revisionsberichte selbst aufgebläht werden und umfangreiche Berechnungen und Sachverhaltsdarstellungen beinhalten. Diese Arbeitspapiere müssen die während eines Auftrags gewonnenen Informationen und durchgeführten Analysen enthalten. Zudem geben sie einen guten Überblick über die verwerteten Unterlagen und erhaltenen Auskünfte. Ebenso müssen sie als Basis die zu berichtenden Feststellungen und Empfehlungen untermauern.

c) Möglichkeiten der Vertretung

Bei Ausfall eines Revisors (z.B. durch Krankheit) ist der Einsatz eines anderen Revisors ohne Arbeitswiederholung möglich. Er setzt während der Prüfung dort auf, wo der ausgefallene Revisor seine Arbeit abgebrochen hat. Auf der Basis der Arbeitspapiere sollte es auch einem sachkundigen Revisor

möglich sein, den Revisionsbericht als Ergebnis der Prüfung zu fertigen.

d) Kontrollmöglichkeiten der Revisionsleitung

Arbeitspapiere ermöglichen der Revisionsleitung das Nachvollziehen der konkreten revisorischen Aktivitäten, sowohl in Bezug auf die Prüfungsvorbereitung als auch auf die -durchführung. Sie sind somit Grundlage der Führungsüberwachung durch den Vorgesetzten (siehe hier auch: Praktischer Ratschlag des IIA Nr. 2330.A1-1 - Kontrolle der Prüfungsunterlagen - und 2340-1, Ziff 5 - Beaufsichtigung der Auftragsdurchführung). Dies gilt umso mehr, als Revisoren von Hause aus in aller Regel ziemlich selbständig die ihnen übertragenen Prüfungsaufträge abwickeln. Die Revisionsleitung hat hiermit die Möglichkeit, sich im Zuge einer begleitenden Kontrolltätigkeit vom Stand der Prüfung zu überzeugen.

Mit der Kontrolle der Arbeitspapiere soll sichergestellt werden, dass alle erforderlichen Prüfverfahren angewendet wurden und eine ordnungsgemäße Grundlage für die Berichterstattung vorliegt. Sie ist ein Baustein der Internen Qualitätssicherung (siehe auch IIR-Revisionsstandard Nr. 3). Beispielhaft stehen hier folgende Aspekte im Vordergrund:

- Art und Umfang der Prüfhandlungen werden einheitlich, sachgerecht und ordnungsgemäß dokumentiert.
- die Prüfergebnisse sind aus den Arbeitspapieren eindeutig ableitbar und somit auch für sachkundige Dritte in angemessener Zeit nachvollziehbar.

Die Kontrolle erfolgt häufig mittels einer Review-Checkliste. Auf jeden Fall sollten schriftliche

Arbeitspapiere sind grundsätzlich Eigentum des Unternehmens. Es kann jedoch sinnvoll sein, den geprüften Stellen, der Managementebene oder weiteren betroffenen Organisationseinheiten die Arbeitspapiere zur Verfügung zu stellen, um Prüffeststellungen zu konkretisieren und zu erläutern.

Notizen über Art und Umfang sowie das Ergebnis des Reviews gefertigt werden. Schließlich ist das Review eine Hilfe für die berufliche Entwicklung von internen Revisoren.

e) *Information Dritter*

Arbeitspapiere sind grundsätzlich Eigentum des Unternehmens. Es kann jedoch sinnvoll sein, den geprüften Stellen, der Managementebene oder weiteren betroffenen Organisationseinheiten die Arbeitspapiere zur Verfügung zu stellen, um Prüffeststellungen zu konkretisieren und zu erläutern. Zudem ist es üblich, dass diese Unterlagen auch externen Prüfern, z.B. den WPs, zur Verfügung gestellt werden. Der Zugang zu den relevanten Unterlagen bedarf jedoch der Genehmigung des Revisionsleiters.

Zudem sind sie Beweismittel in schwierigen Fällen (z.B. bei Delikten) und dienen der Unterstützung bei Sachverhalten wie Durchsetzung von Versicherungsansprüchen.

4 Inhalt, Umfang und Struktur

Zur Gestaltung der Arbeitspapiere sollten folgende Grundsätze beherzigt werden:

- Einfach, übersichtlich, zuverlässig und lesbar
- Hinweise auf Ersteller und denjenigen, der die Arbeitspapiere prüft (z.B. Prüfungsleiter oder Führungskraft)
- Angabe der Informationsquelle
- Kennzeichnung in übernommene und erstellte Arbeitspapiere
- Redundanzfreiheit

Systematik, Layout und Inhalt der Arbeitspapiere hängen jeweils von der Art des Auftrags ab. Deshalb bietet es sich nicht an, Detailvorgaben über Aufbau und Inhalt unisono für jede Prüfung zu geben. In den Arbeitspapieren sind jedoch folgende Aspekte der Auftragsabwicklung zu dokumentieren:

- Planung.
- Risikobeurteilung.
- Prüfung und Bewertung der Angemessenheit und Wirksamkeit des Internen Kontrollsystems.
- Angewandte Prüfungsverfahren, gewonnene Informationen und entsprechende Schlussfolgerungen.

- Review.
- Entwurfsfassung(en) des Berichts.
- Follow-up.

Die Anfertigung, Indizierung und Sammlung von Arbeitspapieren hat ohne Zweifel erhebliche Vorteile. Welche Unterlagen konkret die Arbeitspapiere umfassen, ergibt sich beispielhaft aus Ziff. 3 des IIA-Standards 2330. Die Gliederung der Arbeitspapiere sollte sich hiernach in aller Regel an folgender Einteilung orientieren:

- Organisation (z.B. Inhaltsverzeichnis, Zwischenblätter)
- Allgemeiner Teil (Prüfungsauftrag, Revisionsfragebögen, Schriftwechsel)
- Prüfhandlungen (zum Soll-Zustand, Ist-Zustand, zu den Empfehlungen)
- Schlussbesprechung (Notizen und Protokolle, Terminübersichten zur Realisierung von Empfehlungen)

Arbeitspapiere müssen in sich stimmig und vollständig sein sowie Informationen zum Nachvollziehen und ggf. zur Belegführung gezogener Schlussfolgerungen enthalten. Dazu gehören beispielhaft unter anderem:

- Planungsunterlagen und Arbeitsprogramme.
- Fragebögen zu Kontrollen, Flussdiagramme, Checklisten und Erläuterungen.
- Notizen und Protokolle von Besprechungen.
- Informationen über die Organisation wie Organigramme und Stellenbeschreibungen.
- Kopien von wichtigen Verträgen und Vereinbarungen.
- Informationen über betriebliche und finanzwirtschaftliche Vorgehensweisen.
- Ergebnisse von Kontrollauswertungen.
- Bestätigungsschreiben und Vollständigkeits-erklärungen.
- Analyse und Prüfung von Transaktionen, betrieblichen Prozessen und Kontosalden.
- Ergebnisse aus analytischen Prüfungsverfahren.
- Der definitive Bericht und Stellungnahmen des Managements.
- Auftragskorrespondenz, falls diese im Rahmen des Auftrags getroffene Beurteilungen dokumentiert.

Arbeitspapiere können in Form von Papier, Bändern, Platten, Disketten, Filmen oder anderen Medien vorliegen. Falls die Arbeitspapiere in einer anderen

Form als auf Papier vorliegen, muss auf die Anfertigung von Sicherungskopien geachtet werden.

Wenn Interne Revisoren über Daten des Rechnungswesens berichten, muss aus den Arbeitspapieren hervorgehen, ob die Bücher mit diesen Daten übereinstimmen bzw. damit abgestimmt sind.

Im Folgenden werden einige typische Schritte für die Anfertigung von Arbeitspapieren dargestellt:

- Aus jedem Arbeitspapier sollten der durchgeführte Auftrag sowie Inhalt oder Zweck des Arbeitspapiers erkennbar sein.
- Jedes Arbeitspapier ist vom Ersteller zu unterschreiben (oder abzuzeichnen) und mit einem Datum zu versehen.
- Bearbeitungssymbole (Prüfzeichen) sind zu erklären.
- Informationsquellen müssen eindeutig erkennbar sein.

Standardisierte Arbeitspapiere wie Fragebögen und Prüfungsprogramme können die Effizienz der Auftragsabwicklung verbessern und das Delegieren erleichtern. Bestimmte Arbeitspapiere können als dauerhafte oder fortzuschreibende Revisionsakten genutzt werden. Diese Akten enthalten im Allgemeinen Informationen von fortdauernder Bedeutung.

Von allen prüfungsrelevanten Unterlagen sollten Fotokopien für die Arbeitspapiere angefertigt werden, damit

- die Prüfungsfeststellungen der Prüfungsberichte in den Arbeitspapieren dokumentiert sind und
- eine Rekapitulation von Sachzusammenhängen möglich ist.

Zu den Arbeitsunterlagen sind insbesondere zu nehmen

- alle Dokumente, die für die Prüfer von anderen Stellen erstellt wurden,
- von den Prüfern selbst angefertigt worden sind,
- alle Ablichtungen/Zweitschriften von Schriftstücken sowie Gesprächsnotizen, die Sachverhalte belegen, soweit sie für die Darstellung eines

Der Leiter einer internen Revision sollte Vorgaben entwickeln...

Sinnzusammenhangs oder des Umfangs der Schwachstellen relevant sind,

- Schriftstücke, die der Revisor zu seinen Akten nimmt und die von der geprüften Organisationseinheit oder Dritten stammen.

Vor jeder Prüfung hat der Prüfungsleiter Anspruch auf die notwendige Orientierung durch den Vorgesetzten zu Art, Umfang und Struktur der von ihm erwarteten Arbeitspapiere. Der Prüfungsleiter stimmt das Layout der Arbeitspapiere mit den beteiligten Prüfern ab. Bei einer mehrere Organisationseinheiten übergreifenden Themenprüfung hat sich z.B. eine tabellarische Darstellung nach einem vorgegebenen Fragenkatalog bewährt.

Die Erstellung des eigentlichen Revisionsberichts liegt in der Verantwortung des Prüfungsleiters. Er kann diese Arbeit jedoch nur effizient leisten, wenn alle beteiligten Revisoren ihm solide zuarbeiten. Aus diesem Grund erstellen sie während der jeweiligen Revision, spätestens nach Abschluss eines jeden Themenkomplexes, aussagefähige Arbeitspapiere. Die Arbeitspapiere sollen auch Querverweise und Schnittstellen zu anderen Prüfgebieten, die Bestandteil der Gesamtprüfung sind, aufzeigen. Die Arbeitspapiere übergeben die beteiligten Revisoren dem Prüfungsleiter. Kurz gesagt: Arbeitspapiere, die den Revisionsauftrag dokumentieren, werden vom Revisor erstellt und von den Führungskräften der Internen Revision überprüft.

Die Anforderungen an den Detaillierungsgrad von Arbeitspapieren ergeben sich in aller Regel aus der Unternehmenskultur, der Revisionsphilosophie, der Brisanz des Prüfthemas und der "Spitzfindigkeit" im Gegenargumentieren der geprüften Stelle.

5 Arbeitspraktische Schlussbemerkungen

Der Leiter einer internen Revision sollte Vorgaben entwickeln

- zu den Grundsätzen der Erstellung von Arbeitspapieren sowie
- zu den Regularien zur Aufbewahrung von Arbeitspapieren.

Diese Vorgaben stellen eine Orientierung für die Revisoren dar und sind zugleich Vorgabe für ein ziel- und qualitätsorientiertes Handeln. ❖



➔ Prüfen in SAP®

Liebe Leserinnen und Leser,

auch in Zukunft werden wir im SAP®-Teil der *Revisionspraxis* immer wieder SAP® Branchenlösungen behandeln. Aufgrund der unterschiedlichen Anforderungen werden vermehrt in allen Branchen spezifische Lösungen in die SAP® Systeme integriert. Sei dies z.B. für den öffentlichen Bereich das IS-PS (Public Sector), für Krankenkäuser das IS-H (Healthcare), für Banken das IS-B (Banking) oder für Energieversorger das IS-U (Utilities) und das IDEX-GE (Intercompany Data Exchange Extended - German Electricity). In dieser Ausgabe stehen die Energieversorger im Mittelpunkt. Herr Christoph Wildensee gibt in seinem Artikel einen Überblick über die Funktionalitäten des IDEX-GE. Insbesondere geht er hierbei auch auf das Thema der Zugriffsrechte zu IDEX-GE ein.

Der zweite Artikel ist die dritte Fortsetzung unserer SAP® BW-Reihe von Herrn Claus-Dieter Lillich, der sich diesmal mit dem Prüfen der Zugriffsrechte des SAP® BW auseinandersetzt. Dies hat eine besondere Relevanz, da in einem BW-System eine Vielzahl an Unternehmensdaten in aggregierter Form vorliegen und somit auch äußerst sensible Daten daraus extrahiert werden können. Aufgrund der Komplexität der Berechtigungen wird sich auch der vierte und letzte Teil unserer SAP® BW-Reihe, der in *Revisionspraxis* IV/2006 erscheint, noch eingehender mit diesem Thema befassen.

Ihr

Thomas Tiede



➔ Überblick über die SAP® IS-U-Funktions- und Berechtigungsparameter durch IDEX-GE

Dipl.-Betriebswirt
Christoph Wildensee,
CISM, CIFI, Hannover

Einführung

Der Begriff ‚Unbundling‘ ist gleichzusetzen mit Entflechtung oder Auftrennung und zielt auf die Pflicht zur Trennung eines betriebsnotwendigen Netzes von anderen Bereichen des Unternehmens wie der Erzeugung oder insbesondere dem Vertriebs- und Handelsbereich. Ein Netzmonopol ermöglicht es dem Netzzeiger, den öffentlich geforderten Wettbewerb zum Nachteil fremder Netznutzer im eingerahmten Gebiet zu stören, indem prohibitive Zugangsbedingungen wie hohe Netznutzungsentgelte und andere Beschränkungen durchgesetzt werden. Das Energiewirtschaftsgesetz (EnWG) verfolgt somit das Ziel, zum einen das natürliche Monopol ‚Netz‘ von anderen, dem Wettbewerb unterliegenden Unternehmensbereichen zu entflechten, und zum anderen, die Transparenz des Netzbereiches zu erhöhen und Quersubventionierungen aufzudecken und zukünftig zu verhindern. Das Energiewirtschaftsgesetz ist hier eindeutig:

§9 EnWG: Verwendung von Informationen

- (1): "Unbeschadet gesetzlicher Verpflichtungen zur Offenbarung von Informationen haben vertikal integrierte Energieversorgungsunternehmen und Netzbetreiber sicherzustellen, dass die Vertraulichkeit wirtschaftlich sensibler Informationen, von denen sie in Ausübung ihrer Geschäftstätigkeit als Netzbetreiber Kenntnis erlangen, gewahrt wird."
- (2): "Legen das vertikal integrierte Energieversorgungsunternehmen oder der Netzbetreiber [, der

im Sinne von §3 Nr. 38 mit ihm verbunden ist,] über die eigenen Tätigkeiten als Netzbetreiber Informationen offen, die wirtschaftliche Vorteile bringen können, so hat dies in nicht diskriminierender Weise zu erfolgen."

Die Deregulierung der Energiemärkte und die sukzessive offerierten Konkretisierungen der Bundesnetzagentur (BNetzA) führen bei den Energieversorgern zu Anpassungen der Geschäftsprozesse. Während in der Vergangenheit im Verhältnis zu anderen Netzmonopolisten nur geringer Aufwand z.B. zur Verwaltung von Wechselkunden entstand, werden zukünftig solche Vorgänge durch höhere Wechselquoten im eigenen Versorgungsgebiet zunehmen. Auch die Administration von "Großkunden- / Bündelkundenverträgen" ist hier als markanter Punkt zu nennen.

Wenn diese Prozesse zu Massenprozessen werden, muss auch die IT-Unterstützung entsprechende Funktionen bereitstellen und für Automatismen in der Abarbeitung der Datenströme sorgen. Hinzu kommt die Forderung, dass der eigene Vertriebsbereich gegenüber außenstehenden Mitbewerbern nicht bevorzugt werden darf. Dies führt unweigerlich zur Notwendigkeit eindeutiger Prozess- und Organisationsdefinitionen und zu Berechtigungstrennungen.

Unabhängig von der unternehmensrechtlichen Ausgestaltung des Unbundling erfordert die Verpflichtung des diskriminierungsfreien Zugangs zu wirtschaftlich sensiblen Informationen, also Vorkehrun-

gen gegen eine Weitergabe dieser an eigene, in Konkurrenz stehende Bereiche wie dem Vertriebs- und Handelsbereich. Entsprechend sind Datenverarbeitungssysteme im Rahmen des technisch, zeitlich, organisatorisch und wirtschaftlich Zumutbaren so auszugestalten, dass die Diskriminierungsfreiheit gewahrt wird.

Freiwillige Vereinbarungen der Verbände u.a. hinsichtlich des Netzzuganges, der Netznutzungsentgelte und der Mengenabrechnungen schienen ungeeignete Mittel, den geforderten diskriminierungsfreien Zugang von Fremdversorgern zu gewährleisten. Ausgehend vom Projekt VV2@SAP® arbeiteten neben SAP® selbst z.B. E.ON, RWE, EnBW, Vattenfall und ewmr als Impulsgeber an einer unterstützenden Lösung, die eine weitestgehende Automatisierung wesentlicher Prozesse / Workflows wie dem Lieferantenwechsel, die Mehr- / Mindermengenabrechnung und die Zahlungsbearbeitung / -abwicklung zwischen den Marktteilnehmern unterstützen sollte.

Das SAP® R/3 IS-U als Standardinstrumentarium deckt nicht die geforderten Funktionalitäten ab, so dass ohne weitere Unterstützung / Anpassung ein erheblicher Implementierungsaufwand im Unternehmen entsteht (EDM -Energiedatenmanagement / IDE - Unternehmensübergreifender Datenaustausch).

IDEX-GE (intercompany data exchange extended - german electricity) ist das Ergebnis dieser gemeinsamen Initiative zur (Weiter)Entwicklung einer SAP®-seitigen Abbildung standardisierter Prozesse im liberalisierten Energiemarkt. Durch die Bereitstellung neuer / geänderter Funktionen und Musterprozesse werden der Anpassungsaufwand verringert und bisherige Fehlerquellen ausgeglichen. Das vorrangige Ziel der Einführung im Unternehmen ist also, einen lauffähigen Prototypen mit vordefinierten Prozessanpassungen zu implementieren, der lediglich geringen, unternehmensspezifischen Anpassungsaufwand nach sich zieht und dabei über SAP®-Standard-Change-Modi unterstützt wird.

IDEX-GE basiert auf SAP® R/3 und ist eine Zusatzentwicklung zu den Modulen IS-U, EDM und IDE, wobei es auf Release 4.64 aufsetzt. Es ist in diese Module integriert und verändert alte Modul-

Funktionen, fügt aber auch neue Funktionen hinzu. Das Berechtigungskonzept wird modifiziert. Zum einen steht eine vorkonfigurierte Benutzerrolle ‚Kritischer Vertriebsmitarbeiter‘ zur Verfügung, die entsprechende Berechtigungsobjekteingrenzungen sowie ein CIC-Profil zur Begrenzung der Anwendungs- / Anzeigefunktionen enthält, zum anderen werden Änderungen der Verarbeitungslogik über BAPI's und BAdI's realisiert.

Über BAPI-Schnittstellen (Business Application Programming Interface) können in anderen Programmiersprachen oder Zugangsdefinitionen aufgebaute externe Funktionen mittels RFC (Remote Function Call) in jedem SAP®-System ohne SAPGUI-Nutzung aufgerufen werden. Rein technisch betrachtet sind BAPI's remotefähige Funktionsbausteine. Sie ermöglichen die Integration externer Systemkomponenten auf der betriebswirtschaftlichen Ebene. Nach Freigabe eines BAPI's durch SAP® bleiben seine Schnittstellendefinition und Aufruf-parameter bestehen - auf diese Weise ist sichergestellt, dass externe Zugriffe auf das SAP®-System dauerhaft stabil laufen.

Reichen die Customizing-Möglichkeiten von SAP®-Systemen / -Modulen nicht aus, stellen die Programme an vielen Stellen Erweiterungspunkte zur Verfügung, an denen kundenspezifische Programmmodifikationen in die Standardverarbeitung eingebettet werden können. Eine Möglichkeit besteht in der Nutzung von BAdI's (Business Add-Ins), die als "objektorientierte User-Exists" oder Einsprungpunkte in der Verarbeitungslogik gesehen werden können.

IDEX-GE-Funktionsumfang

Die folgende Übersicht gibt einen kurzen Einblick in den Funktionsumfang von IDEX-GE:

- Verbesserter Erfassungsdialog für den Wechselbeleg (kundenindividuelle Anpassungen über BAdI)
- Automatische Zählpunktidentifikation für eingehende Meldungen mit Möglichkeit der manuellen Nachidentifikation (der Zählpunkt ist kein Muss-Feld in der Wechselmeldung)
- Definition von Kündigungskonditionen zum Zweck der Prüfung einer Mindestvertragslaufzeit beim alten Lieferanten

- Erweiterungen bei der Mehr- / Mindermengenabrechnung, z.B. zählpunktbezogene Einzelnachweise
- Erweiterungen im Bereich Netznutzungsbearbeitung
- Rechnungsprüfung bei Eingang Netznutzungsrechnung beim Lieferanten
- Erweiterungen bei der Funktionalität zur Erzeugung elektronischer Netznutzungsrechnungen beim Netzbetreiber
- Erweiterte Funktionalitäten im Bereich Berechtigungen (Voraussetzung: Zwei-Vertragsmodell [2VM])
- Vorkonfiguration für den "kritischen Vertriebsmitarbeiter".

Hierzu stehen verschiedene Instrumente zur Verfügung wie z.B.

- Werkzeuge zur Datenübernahme (BC-Sets [Business-Configuration-Sets], CATT's)
- Geschäftsprozessorientierte Konfigurationsleitfäden: Exemplarische Beschreibung der Installation, sowohl manuelle Unterstützung als auch Werkzeugnutzung zur Automatisierung der Konfigurationsaktivitäten
- Detaillierte Ablaufbeschreibungen von Muster-Geschäftsprozessen
- Muster zur Abrechnung von Mehr- / Mindermengen.

Die erweiterten Funktionen beziehen sich vorwiegend auf den Lieferantenwechsel, die Netznutzungsbearbeitung und die Mehr- / Mindermengenabrechnung. Die Erweiterungen ermöglichen insbesondere

- das manuelle Nachidentifizieren von Zählpunkten: Optimierte Identifikation für eingehende Meldungen im automatischen Datenaustausch integrierbar mit der Möglichkeit der manuellen Nachidentifizierung im Workflow für Lieferantenwechsel und Kündigungsbearbeitung, Identifizierung während Dialogerfassung, über Adressdaten- oder über Zählpunkteingabe, keine Eindeutigkeit = Auswahlliste
- die Prüfung der Mindestvertragslaufzeit: Definition von Kündigungskonditionen, optimierte Bearbeitung bei der Berechnung des nächstmöglichen Kündigungstermins
- eine prozessabhängige Ermittlung relevanter Feldbelegungen bei Mussfeldprüfungen im Erfassungsdialog des Wechselbeleges

- und dabei die effiziente Erfassung von Wechselbelegen: Anzeige der Felder in Abhängigkeit von ‚Wechselsicht‘ und ‚Wechselart‘, Vorbelegung von Feldern
- Datenaustausch innerhalb eines Mandanten (Voraussetzung: Netzbetreiber und eigener Lieferant werden im selben Mandanten geführt und für die Abbildung von All-Inclusiv-Kunden wird wie oben erwähnt ein 2VM verwendet)
- Netznutzungsbearbeitung innerhalb eines Mandanten wie direkte Netznutzungsrechnungsbuchung zum Rechnungseingang des Lieferanten (INVOIC), Überführung der Rechnungen in das FI-CA des Lieferanten, Zahlung der Rechnungen und Erstellung von Zahlungsavisen (REMAADV) über den Zahlungslauf des Lieferanten
- Optimierter Rechnungseingang durch Feldvorbelegungen, Erfassungsvarianten, Identifikation von Zählpunkten im Dialog, verbesserte Rechnungseingangsprüfungen, Prüfparameter, die in Prüfbausteinen der optimierten Rechnungseingangsprüfung verwendet werden können
- Kundengruppenspezifische Ermittlung und Abrechnung von Mehr- / Mindermengen, getrennte Abrechnungen der Mehr- / Mindermengen nach Kundengruppen: **Bilanzierungsreport**: REEDMSETTLPROC_VV2_SYNTH_GRP (synthetisches Bilanzierungsverfahren nach VV2 - kundengruppenspezifisch) - **Bilanzierungsschritt**: SUMRES08SU; **Bilanzierungsreport**: REEDMSETTLPROC_FINSETTL_GRP (Mehr- / Mindermengenermittlung nach VV2 - kundengruppenspezifisch) - **Bilanzierungsschritt**: DIFFGRPSU; Mehr- / Mindermengenabrechnung erfolgt über RTP-Schnittstelle
- Zählpunktbezogener Einzelnachweis für die jeweiligen Lieferanten, u.a. Aufschlüsselung von Differenzmenge je Zählpunkt, Report: /ISIDEX/RESETTLPODLIST; ALV-Grid-Control oder Filetransfer, Zählpunktselektion über Belegnummer
- Verbessertes Bilanzierungsreporting: Zählpunkt ↔ Bilanzierungsbelege
Transaktion EEDMSETTLANALYSE / EEDMSETTLANALYSEPOD.

Eine exemplarische Kurzübersicht über ausgesuchte Basis-Einstellungen aus den SAP®-Building-Block-Konfigurationsleitfäden, die gleichzeitig zu analysie-

renden Revisionsaspekten entsprechen, gibt einen wichtigen Ausblick auf die Implementationsaktivitäten:

Geschäftsprozess Lieferant und Lieferantenwechsel (Verteilnetzbetreiber)	
<p>Zugehörige Rollen: IDEX LW LIEFERANT BLOCK und IDEX LW VERTEILNETZBETREIBER BLOCK</p>	
<p><u>Fristen-Framework</u> Der Lieferantenwechselprozess benötigt für die Wechselarten Lieferantenwechsel, Lieferbeginn und Lieferende eine Reihe von Fristen. Zu diesen zählen z.B. bilaterale Fristen zwischen Marktpartnern, Fristen nach Marktregeln, Fristen für unterschiedliche Zählpunktgruppen usw. Mit dem Fristen-Framework werden diese definiert und überwacht.</p>	<p>View-Cluster: VC_EIDESWTTIME</p> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Fristenarten definieren</p>
<p><u>Prüf-Framework-Grundeinstellungen</u> Die Infrastruktur für Prüfungen im Lieferantenwechselprozess wird über das Prüf-Framework bereitgestellt. Hierbei können die Exception-Behandlung, die Protokollierung und das Ignorieren von Zuständen (Übersteuerung: Definition, ob der Prozess / die Aktion übergangen werden kann, es wird dann mit dem nächsten Prozess / der nächsten Aktion fortgefahren) eingestellt werden.</p>	<p>View-Cluster: VC_EIDESWTCHECK V_EIDESWTCHECKEV</p> <p>Customizing über: Werkzeuge → Systemanpassung → Kundeneigene Funktionserweiterung für IDE → Lieferantenwechsel → Prüfungen definieren und Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Ausnahmebehandlung für Prüfungen definieren (POD_MISSING)</p>
<p><u>Wechselbeleg-Nummernkreis</u> Die Protokollierung der Wechselprozesseinzel-schritte erfolgt über die Wechselbelege.</p>	<p>Customizing über: Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Nummernkreise für Wechselbelegnummer definieren</p>
<p><u>Art der Serviceanbietervereinbarung</u> Die Serviceanbietervereinbarung dient zur Steuerung der Folgeprozesse abhängig von den Servicearten. Hieran sind der Marktpartner und der prozessausführende Serviceanbieter beteiligt.</p>	<p>View-Cluster: V_EDRGSPAGRTYPE (DeregProzess: GRIDUSAGE)</p> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Serviceanbietervereinbarungen → Arten der Serviceanbietervereinbarungen festlegen</p>
<p><u>Workflows zu Wechselsichten</u> Der entsprechende Prozess-Workflow wird in Abhängigkeit des Serviceanbieters gestartet.</p>	<p>View-Cluster: V_EIDESWTVIEWTAS</p> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Workflow pro Wechselsicht definieren</p>

Geschäftsprozess Lieferant und Lieferantenwechsel (Verteilnetzbetreiber)

<p><u>Datenaustauschprozesse</u> Der Datenaustauschprozess zwischen Serviceanbietern ist eine zentrale Aufgabe. Er basiert auf den implementierten DA-Basismethoden. Ein DA-Prozess zwischen zwei Serviceanbietern wird über eine Datenaustauschdefinition veranschaulicht, entsprechend der DA-Aufgaben können DA-Definitionen gesteuert und überwacht werden.</p>	<p>Customizing über: Unternehmensübergreifender Datenaustausch → Datenaustauschprozesse → Datenaustauschprozesse definieren</p>
<p><u>Wechselbeleg-Erfassungsdialo</u> Der Wechselbeleg-Erfassungsdialo wurde durch stichtags(un)abhängige Vorbelegungen, spezifische Feldeigenschaften und Mussfelddefinitionen erweitert (VDEW-Vorgabenrichtwerte für Kann-, Soll- und Mussfelder einer Systemnachricht).</p>	<p>Customizing Erfassungsdialo über: (SE19) Werkzeuge → ABAP Workbench → Hilfsmittel → Business-Add-Ins → Implementierung</p> <p>BAdI-Aktivierung: /SIDEX/IDE_SWITCHD</p> <p>Mussfelddefinitionen: View-Cluster: VC_EIDESWTMSGFIELD /SIDEX/V_EMDCHK</p> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Feldprüfung festlegen und Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Verwendung der Mussfeldprüfungen festlegen</p> <p>(Neue Prüfmethode /SIDEX/CL_ISU_IDE_SWITCH_CHECK → Methode Check_Msgdata_Ext() kann kundenindividuell integriert werden.)</p>
<p><u>Zählpunktidentifikation</u> Die Abweisung der UTILMD-Anfrage bei der automatischen Zählpunktidentifikation kann über eine manuelle Nachidentifikation des Zählpunktes ausgeglichen werden. Hierzu sind projektspezifische Anpassungen des Muster-Workflows notwendig.</p>	<p>View-Cluster: /SIDEX/V_EIDPRD</p> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Verwendung der Prozessvarianten für Identifikation der Zählpunkte festlegen</p> <p>Die manuelle Zählpunktidentifikation kann nur durch eine Ausprägung des BAdI ISU_IDE_COMM_SWT ? Methode Inbound_Determine_POD() eingebunden werden. Damit das System die UTILMD-Anfrage nicht automatisch ablehnt, ist die Workflow-Exception POD_MISSING für die Wechselsicht ‚Netzbetreiber‘ und ‚Alter Lieferant‘ mit 09 (kein Fehler nach Sachbearbeiterentscheidung fortsetzen) überzudefinieren.</p>

Geschäftsprozess Lieferant und Lieferantenwechsel (Verteilnetzbetreiber)	
<p><u>Mindestvertragslaufzeit</u></p> <p>Bei der Kündigung eines Stromlieferungsvertrages zu einem gewünschten Zeitpunkt muss entschieden werden können, ob der Beendigungswunsch aufgrund von Mindestvertragslaufzeiten, Verlängerungsregelungen und einzuhaltenden Kündigungsfristen korrekt ist. Das System prüft die Eingaben auf zeitliche Konsistenz.</p>	<p>View-Cluster: /ISIDEX/V_CANCON</p> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Prozessbearbeitung → Lieferantenwechsel → Kündigungskonditionen für Prüfungen der Mindestvertragslaufzeit definieren Erweiterung durch Subscreen-Einbindung, Feldprüfungsdefinition, DDIC-Strukturanlage (CI_EVER → Hinzufügen der Komponente CANC_COND_ID vom Komponententyp /ISIDEX/E_CANC_COND_ID), Kopieren und Aktivieren neuer Dynpros vom Programm /ISIDEX/SAPLXES20 in das Programm SAPLXES20, Include-Erweiterung in der Funktionsgruppe XES20 und Erweiterung des Workflow ‚Alter Lieferant‘ um die Prüfung NOTICE-PERIOD.</p>
<p><u>Ereignistypkoppelung</u></p> <p>Wird das Ereignis ‚Wechselbeleg angelegt‘ ausgelöst, startet die Typkoppelung. Zur differenzierten Betrachtung im Workflow wird eine Check-Funktion benötigt.</p>	<p>Customizing über: (SWETYPV) Werkzeuge → Business Workflow → Entwicklung → Hilfsmittel → Ereignisse → Typkoppelung</p> <p>Checkfunktion: ISU_IDE_CHECK_SWT_WF_START</p>
<p><u>Lieferantenwechsel - Sicht Neuer Lieferant (LN); Lieferbeginn - Sicht Neuer Lieferant (LN); Lieferantenwechsel - Sicht Alter Lieferant (LA); Lieferende - Sicht Alter Lieferant (LA)</u></p>	<p>Customizing über: (EWBC) Kundenservice → Front-Office → Front-Office-Prozesse definieren</p>
<p><u>Serviceanbieter</u></p> <p>Serviceanbieter können nur angelegt werden bei Vorliegen korrespondierender Geschäftspartner (GP). Das GP-Feld ist bei der Serviceanbieterpflege ein Muss.</p> <p>Ein Serviceanbieter (Marktteilnehmer, der Dienstleistungen anbietet) kann sowohl ein fremdes Unternehmen (Marktpartner) als auch eine Organisation im eigenen Konzern (prozessausführender Serviceanbieter) sein.</p> <p>Eine Bilanzierungseinheit (BE) beinhaltet relevante Zählpunkte (ZP) für eine Bilanzierung. Das System ordnet jeder BE einen virtuellen technischen ZE zu, um Profile direkt einer BE zuordnen zu können. (? Bilanzierungsergebnisse).</p> <p>Zu einer BE ermittelt das System Deregulierungszählpunkte, die zu den Servicetypen einen Zählpunktservice zum jeweiligen Serviceanbieter besitzen. Bei der BE-Generierung vergleicht dann das System die Serviceanbieter der BE und der ZP und ordnet entsprechend die ZP den BE zu.</p> <p>Ein Netz ist ein ganzes oder ein Teilnetz eines Versorgungsgebietes eines Verteilnetzbetreibers. Es bildet die Hierarchie von Verteil- und Übertragungsnetzen und ggf. auch physikalisch getrennte Regelzonen ab.</p>	<p>Geschäftspartner Verteilnetzbetreiber und Lieferant aus Sicht des Verteilnetzbetreibers:</p> <p>Customizing über: (FPP1) Stammdaten kaufmännisch → Geschäftspartner → Vertragspartner → Anlegen</p> <p>Für GP ‚Fremder Verteilnetzbetreiber‘, ‚Eigener Lieferant‘ und ‚Fremder Lieferant‘ und ‚Bilanzkreiskoordinator‘</p> <p>Serviceanbieter aus Sicht des Lieferanten:</p> <p>Customizing über: (EEDMIDESERVPROV01) Unternehmensübergreifender Datenaustausch → Serviceanbieter → Anlegen</p> <p>Bilanzierungseinheiten für die Sicht Lieferant:</p> <p>Customizing über: (EEDMSETTLUNIT01) Energiedaten-Management → Bilanzierung → Stammdaten → Bilanzierungseinheit anlegen (Gen.-Report: EEDM_SETTLUNIT_GEN)</p> <p>und (EEDM09) Stammdaten technisch → Zählpunkt → Anlegen</p> <p>Netzanlage aus Sicht des Lieferanten: (EEDMIDE_GRID01) Unternehmensübergreifender Datenaustausch → Netz → Anlegen</p> <p>Nutzung der Stammdatenvorlagen über: SPRO (Zahlungsklasse), CAA1 (aggregiertes Vertragskonto) und EEDMIDESERVPROV02 (Serviceanbieterergänzung)</p>

Geschäftsprozess Lieferant und Lieferantenwechsel (Verteilnetzbetreiber)

<p>Customer Interaction Center (CIC) Unter Verwendung des CIC werden die Prozesse des Lieferantenwechsels ausgelöst (Anpassungen über CIC-Profil (Z)ISU_DRG).</p>	<p>Customizing über: (PPOME) Personal → Organisationsmanagement → Aufbauorganisation → Organisation und Besetzung → Ändern (EWFC0) Kundenservice → Customer Interaction Center → Komponenten Konfiguration → Einstellungen zur Action Box → Konfigurationsprofile für Actionbox festlegen Kundenservice → Customer Interaction Center → CIC-Profile → CIC-Profile pflegen mit View-Cluster: V_CICPROF</p>
---	---

Deregulierungs-Basiseinstellungen Verteilnetzbetreiber und Deregulierungs-Basiseinstellungen Lieferant

<p>Zugehörige Rollen: IDEX Dereg VERTEILNETZBETREIBER BLOCK und IDEX Dereg LIEFERANTEN BLOCK</p>			
<p>Deregulierungseinstellungen Unterscheidung zwischen Dialog- und Prozess-Steuerung. <u>Dialogsteuerung:</u> Serviceanbietervereinbarung und Versorgungsszenario; <u>Prozess-Steuerung:</u> Zahlungsabwicklung und Servicefindung.</p>	<table border="1"> <tr> <td data-bbox="767 943 938 1055"> <p>View-Cluster: VC_EDRGSWITCH</p> </td> <td data-bbox="938 943 1489 1238"> <p>Customizing über: Grundeinstellungen/Unternehmensstruktur → Deregulierungseinstellungen festlegen</p> </td> </tr> </table>	<p>View-Cluster: VC_EDRGSWITCH</p>	<p>Customizing über: Grundeinstellungen/Unternehmensstruktur → Deregulierungseinstellungen festlegen</p>
<p>View-Cluster: VC_EDRGSWITCH</p>	<p>Customizing über: Grundeinstellungen/Unternehmensstruktur → Deregulierungseinstellungen festlegen</p>		
<p>Servicearten</p>	<p>Customizing über: Unternehmensübergreifender Datenaustausch → Services → Servicearten definieren</p>		
<p>Versorgungsszenarien Es werden Datenmodelle für unterschiedliche Versorgungsszenarien festgelegt.</p>	<table border="1"> <tr> <td data-bbox="767 1417 938 1529"> <p>View-Cluster: VC_EDRGSCENARIO</p> </td> <td data-bbox="938 1417 1489 1713"> <p>Customizing über: Unternehmensübergreifender Datenaustausch → Versorgungsszenarien → Versorgungsszenarien definieren</p> </td> </tr> </table>	<p>View-Cluster: VC_EDRGSCENARIO</p>	<p>Customizing über: Unternehmensübergreifender Datenaustausch → Versorgungsszenarien → Versorgungsszenarien definieren</p>
<p>View-Cluster: VC_EDRGSCENARIO</p>	<p>Customizing über: Unternehmensübergreifender Datenaustausch → Versorgungsszenarien → Versorgungsszenarien definieren</p>		
<p>Workflow: Customizing verifizieren und Stammdatenvorlage</p>	<p>Customizing über: (SWU3) Werkzeuge → Business Workflow → Entwicklung → Hilfsmittel → Customizing verifizieren Stammdatenvorlage: /ISIDEX/VNB (Verteilnetzbetreiber) bzw. /ISIDEX/LIEF (Lieferant)</p>		

IS-U-EDM Basis Block - Einstellungen	
	<p>Zugehörige Rolle: IDEX EDM BASIS BLOCK</p>
	<p><u>Grundeinstellung Customizing EDM - Energie-Daten-Management</u></p> <p>1. Grundeinstellung Kalender und Nummernkreise Customizing über: <u>Kalender</u>: Allgemeine Einstellungen → Kalender pflegen <u>Nummernkreise</u>: Energiedaten-Management → Profilverwaltung → Nummernkreise für Profile definieren <u>Profilarten</u>: Energiedaten-Management → Grundeinstellungen → Profilart → Profilarten definieren <u>Intervallzulässigkeit</u>: Energie-Datenmanagement → Grundeinstellungen → Profilart → Zulässigkeit der Intervalllänge je Profilart definieren</p>
	<p>2. Saisonblock / Tagesblock / Tageszeitblock Customizing über: <u>Saisonarten</u>: Energiedaten-Management → Grundeinstellungen → Saisonblock → Saisonarten definieren <u>Saisonblöcke</u>: Energiedaten-Management → Grundeinstellungen → Saisonblock → Saisonblöcke definieren <u>Tagesarten</u>: Energiedaten-Management → Grundeinstellungen → Tagesarten definieren <u>Tagesblöcke</u>: Energiedaten-Management → Grundeinstellungen → Tagesblöcke definieren <u>Tageszeitarten</u>: Energiedaten-Management → Grundeinstellungen → Tageszeitblock → Tageszeitarten definieren <u>Tageszeitblöcke</u>: Energiedaten-Management → Grundeinstellungen → Tageszeitblock → Tageszeitblöcke definieren</p>
	<p>3. Profilverwaltung Customizing über: <u>Nummernkreise für Profile</u>: Energiedaten-Management → Profilverwaltung → Nummernkreise für Profile definieren <u>Nummernkreise für Herkunftssystem</u>: Energiedaten-Management → Grundeinstellungen → Nummernkreise für Herkunftssystem definieren <u>Rollen für Profilzuordnung</u>: Energiedaten-Management → Profilverwaltung → Rollen für Profilzuordnung definieren <u>Anzeige von Profilwerten</u>: Energiedaten-Management → Profilverwaltung → Anzeigefunktion → Anzeige des Status von Profilwerten definieren</p>
	<p>4. Synthetische Profile Customizing über: <u>Tagesprofil</u>: Energiedaten-Management → Profilverwaltung → Profilkopf anlegen (EEDM06) CATT: /ISIDEX/EEDM06_C001_U01 Prog. REEDMPROFILEIMP01 <u>Dynamisierungsprofil</u>: wie zuvor; Dynamisierungsfaktoren über Transaktion EEDMFACTORCALC <u>Synthetisches Profil</u>: wie zuvor; CATT: /ISIDEX/EEDM06_C002_U01 Profile beziehen sich auf definierte Profilarten</p>

Tab. 1: Kurzdarstellung ausgesuchter SAP®-Building-Block-Konfigurationsleitfäden

Neue Berechtigungen

Mit IDEX-GE können sensible Daten aufgrund eines erweiterten Berechtigungskonzeptes geschützt werden (siehe auch Tabelle AUTHX). Es setzt allerdings hierbei die Abbildung des Zwei-Vertrags-Modells (2VM) im IS-U voraus. Das erweiterte Berechtigungskonzept basiert auf zusätzlichen Berechtigungsprüfungen innerhalb der Funktionsaufrufe und auf Begrenzungen in der Navigation. Es bezieht sich w.o.e. insbesondere auf Mitarbeiter, die kritische Vertriebsaufgaben wahrnehmen und dabei durch die Kenntnisnahme sensibler Daten ggf. einen Wettbewerbsvorteil erlangen. Hierzu wird die Berechtigungsrolle SAP®_ISU_IDEX_VERTRIEB ausgeliefert. In dieser Berechtigungsrolle werden neue und alte Berechtigungsobjekte adäquat zusammengefasst.

Berechtigung-Objekt	Bezeichnung	Steuerungsfeld	Feldbezeichnung	Referenz-domäne/-tabelle
E_EDM_PRF2	Berechtigungsobjekt für die Bearbeitung von EDM-Profilen - IDEX	ISU_PRFACT	Aktionen, die auf EDM-Profile ausgeführt werden	D:E_EDMPROF ACTION_ID
		ISU_PRFTYP	Profilart	D:PROFATYPE [EPROFATYPE]
E_NBSERVIC	Berechtigungsobjekt für Zählpunktservice	ISU_ACTIVT	Aktivität bezüglich Berechtigungen in IS-U	D:E_ACTIVITY / D:E_MODE
		BEGRU	Berechtigungsgruppe	D:BEGRU
E_NBSERVI2	Berechtigungsobjekt für Zählpunktservice - IDEX	ISU_ACTIVT	Aktivität bezüglich Berechtigungen in IS-U	D:E_ACTIVITY / D:E_MODE
		ISU_SERVIC	Serviceart	D:SERVCAT [TECDE]
		ISU_SERVID	Serviceanbieter	SERVICE_PROV [ESERVPROV]
E_INV_ETHI	Berechtigungsobjekt Aggregierte Buchung Vkto. Serv.anb. - IDEX	ACTVT	Aktivität	D:ACTIV_AUTH TACT
E_INSTLN2	Berechtigungsobjekt zur Versorgungsanlage	ISU_ACTIVT	Aktivität bezüglich Berechtigungen in IS-U	D:E_ACTIVITY / D:E_MODE
		ISU_SERVIC	Serviceart	D:SERVCAT [TECDE]
E_MR_DOC2	Ber.objekt zu Ablesebelege und Ableseaufträgen bez. Buchung	ISU_MR_ACT	Aktivitäten bezüglich Ablesung	D:ACTIONMR
		BUKRS	Buchungskreis	T001
E_POD2	Berechtigungsobjekt für die Zählpunkttransaktion	ISU_POD_TB	Tabreiter Zählpunkt	D:E_POD_TAB

Berechtigung-Objekt	Bezeichnung	Steuerungs-feld	Feldbezeichnung	Referenz-domäne /-tabelle
E_SERVPROF	Berechtigungsobjekt zum Serviceanbieter	ISU_ACTIVT	Aktivität bezüglich Berechtigungen in IS-U	D:E_ACTIVITY / D:E_MODE
		BEGRU	Berechtigungsgruppe	D:BEGRU
E_SWTDOC	Berechtigungsobjekt zum Wechselbeleg	ISU_ACTIVT	Aktivität bezüglich Berechtigungen in IS-U	D:E_ACTIVITY / D:E_MODE
		BEGRU	Berechtigungsgruppe	D:BEGRU
		SWTVIEW	Wechselsicht	D:EIDSWTVIEW [EIDSWTVIEWS]

Tab. 2: Beispiele wichtiger Berechtigungsobjekte im Bereich IDEX-GE

Folgende beispielhafte Anpassungen wurden in den Berechtigungsprüfungen vorgenommen:

- **E_INSTLN2:** Es werden nur die Anlagen angezeigt, für die eine Berechtigung für die Serviceart ‚Lieferung‘ existiert.
- **E_POD2:** Es werden nur die Zählpunktdaten angezeigt, für die eine Berechtigung existiert.
- **E_NBSERV12:** Es werden nur die nicht-abrechenbaren Services angezeigt, für die eine Berechtigung für die Serviceart und für den Serviceanbieter existiert.
- **E_MR_DOC2:** Es werden nur Ableseergebnisse angezeigt, für die eine Berechtigung existiert.
- **E_EDM_PRF2:** Es werden nur Profilwerte angezeigt, für die eine Berechtigung existiert oder für die gültige Anlagen, Verträge, Vertragskonten und Geschäftspartner gefunden werden können.
- **Datenumfeldanzeige:** Es werden nur die Daten in der Umfeldanzeige angezeigt, für die eine Berechtigung existiert. Dies gilt für das Datenumfeld aller relevanter IS-U-Stammdaten.
- **Kundenübersicht:** Es werden nur die Verträge und Druckbelege angezeigt, für die eine Berechtigungseingrenzung existiert.
- **Anschlussobjektübersicht:** Es werden nur die Verträge angezeigt, für die eine Berechtigungseingrenzung existiert.
- **Tree-Anzeige verschiedener Transaktionen:** Es werden nur die Daten in der Hierarchie angezeigt, für die eine Berechtigung vorliegt (dies gilt u.a. für das CIC [Navigation] und für die Transaktionen zur Anzeige von Zählpunkten und Abrechnungsbelegen).

- **Anzeige von Ableseergebnissen:** Es werden nur die Ableseaufträge / -ergebnisse für die Zeiträume angezeigt, in denen die Zählpunkte vom eigenen Lieferanten versorgt werden oder wurden.
- **Anzeige von Druck- und Fakturierungsbelegen:** Es gelten die Berechtigungsprüfungen des Vertragskontos. Zusätzlich werden Berechtigungsprüfungen für die Anzeige von Belegpositionen durchgeführt.

Trotz des Reduzierens auf den "Kritischen Vertriebsmitarbeiter", der typische Vertriebs- und Handelsaktivitäten wahrnimmt, stellen die IDEX-GE-Implementationsaktivitäten einen nicht unerheblichen Arbeitsaufwand dar, der nicht nur das Customizing betrifft, sondern auch das IS-U-Change-management tangiert. Mit den weiteren IDEX-GE-Releases steuern Implementationen auf die Administration zu, die kaum über eigene / kundenspezifische Individualanpassungen aufzubauen sind.

Fazit

Mitarbeiter mit allgemeinen Aufgaben wie Call Center- und Backoffice-Aktivitäten o.ä. sind aus der Betrachtung ausgenommen, da sie lt. SAP® keinen explizit betriebswirtschaftlichen Vorteil aus der Einsicht in potentiell diskriminierende Daten erreichen können. Entsprechend ist der als kritisch einzustufende Datencluster von SAP® definiert. Trotzdem kann diese Eingrenzung auf ausschließlich vertriebliche Aktivitäten ein Problem darstellen. "Shared Services" müssen mit organisatorischen

Eine SAP®-Lösung, die organisatorische Vorgänge homogenisiert und so zu einem standardisierten und stringenten Arbeitsablauf zwischen den Marktteilnehmern sorgt, ist mehr als sinnvoll...

Regelungen erfasst werden, da sie z.T. als Nahtstelle zwischen Erzeugung, Netz, Handel und Vertrieb z.B. über Reporting-Strukturen Informationen bündeln und übergreifend zur Verfügung stellen (siehe auch CRM und BI / BW). Daher ist diese Begrenzung wahrscheinlich auch der stärkste Kritikpunkt am IDEX-GE, da sie doch zu einseitig Einschnitte in Organisations- und Informationsflüsse fordert und so dem Unternehmen zu viel Freiheit im Unterlassen von Informationsflussregelungen und entsprechenden Systemanpassungen lässt.

Eine SAP®-Lösung, die organisatorische Vorgänge homogenisiert und so zu einem standardisierten und stringenten Arbeitsablauf zwischen den Marktteilnehmern sorgt, ist mehr als sinnvoll, meines Erachtens erhält die Berechtigungsseite jedoch nicht genügend Aufmerksamkeit. Die Beschränkung auf den "Kritischen Vertriebsmitarbeiter" kommt doch einem Ignorieren der Unternehmensorganisation und dort vorhandener Abläufe gleich.

Jedoch ist es die Aufgabe des eigenen Unternehmens, für angemessene Informationszugangssicherheit zu sorgen. So ist die SAP®-Lösung IDEX-GE auch nicht als "Rundum-Sorglos-Paket" zu werten, sondern vielmehr als aufwandreduzierende Ergänzung der eigenen Bemühungen um eine gesetzeskonforme Umsetzung der Unbundling-Forderungen, einer prozessoptimierten Abarbeitung von Kundenaktionen und der damit verbundenen Datenaustauschprozesse.

Ausgesuchte Literatur:

Beyer/Fischer/Jäck u.a. SAP® Berechtigungsweisen - Design und Realisierung von Berechtigungskonzepten für SAP® R/3 und SAP® Enterprise Portal, SAP® Press / Galileo Press, Bonn, 2003;

Hans-Christian Gerig IDEX-GE Erweiterungen Netznutzungsbearbeitung, SAP® AG, DSAG 12/2004;

Hans-Christian Gerig IDEX-GE Vorkonfiguration, SAP® AG, DSAG 12/2004;

Ingo Haug IDEX-GE Unbundling, SAP® AG, DSAG 12/2004;

Christian Orłowski IDEX-GE Erweiterungen Mehr- und Mindermengenabrechnung, SAP® AG, DSAG 12/2004;

Christian Orłowski IDEX-GE Erweiterungen Lieferantenwechsel, SAP® AG, DSAG 12/2004;

Thomas Tiede SAP® R/3 Ordnungsmäßigkeit und Prüfung des SAP®-Systems (OPSAP), Ottokar-Schreiber-Verlag, Hamburg, www.osv-hamburg.de;

SAP® AG Building-Block-Konfigurationsleitfäden IS-U/IDEX;

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/2001 ff, Ottokar-Schreiber-Verlag, Hamburg, www.osv-hamburg.de; ❖



➔ SAP® Business Information Warehouse

Chancen und Risiken - Teil III:
"Berechtigungen - Ein weites Feld"

Claus-Dieter Lillich
IBS Schreiber GmbH

Haben Sie Ihre Felder gut bestellt? BW-Berechtigungsobjekte auf Feldebene als Schlüssel zum detaillierten Sicherheitskonzept.

Was Sie hier erwartet

Dieser Artikel erläutert das SAP® BW-Berechtigungskonzept auf Feldebene und zeigt erste Schritte zur Realisierung auf. Im Folgenden wird diese Art der Berechtigung in ihrer Grundfunktionalität vorgestellt und an einem Beispiel verdeutlicht.

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. Größeren Einblick in wichtige Teilaspekte verschafft ihnen die Möglichkeit, die Revisionsqualität ihres BW-Systems durch konkrete Prüfungsansätze maßgeblich zu erhöhen.

Berechtigungskonzeption von SAP® BW auf Feldebene

Das Berechtigungskonzept auf Feldebene stellt die unterste Berechtigungsebene und damit die höchste Selektionsstufe des Systems dar. Dieses bedeutet, dass jeder Anwender innerhalb von SAP® in seiner Zugriffsberechtigung individuell beschränkt werden kann.

Feldebene

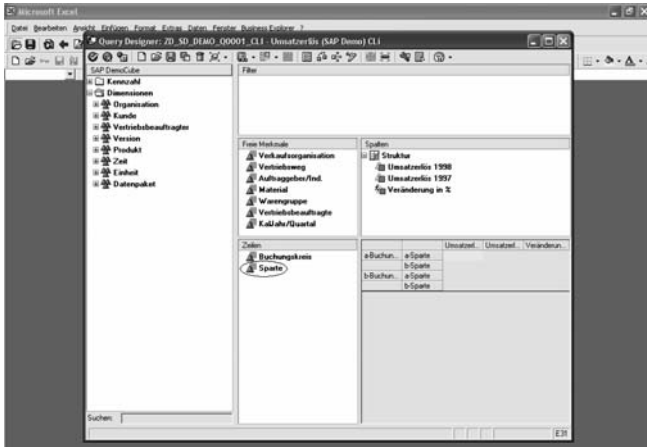
Die Feldebene ist der Ort, an dem sich die zur Datenaufnahme fähigen Kopien einzelner Datenfelder (InfoObjects) befinden, die die kleinste Einheit des jeweiligen Datenspeichers (InfoCube bzw. ODS-Object) darstellen. Hier entscheidet sich die Frage, welches InfoObject geschützt werden soll bzw. wird.

Berechtigungsvergabe

Wird ein InfoObject auf der Feldebene als berechtigungsrelevant definiert, so kann in der Berechtigungsverwaltung einzelnen Mitarbeitern bzw. Gruppen eine Zugriffsberechtigung auf ausgewählte Informationen zugeordnet werden.

Praktische Umsetzung

Bisher können auf der Grundlage der vorherigen Artikel in PRev Daten nur bis zur InfoCube-Ebene geschützt werden. Wird ein weitergehender Schutz vor Einsichtnahme als notwendig erkannt, kommt eine weitergehende Berechtigungsvergabe zum Einsatz. Anhand des folgenden Beispiels wird die Zugriffsbeschränkung über das InfoObject <<Sparte>> (0D_DIV) des IDES-Systems aus dem Bereich *SAP® Demo → Vertrieb* dargestellt. Der Test erfolgt mit der abgeänderten Kopie der Query 0D_SD_DEMO_Q0001 in der InfoArea *SAP® Demo → SAP® Demo Vertrieb → SAP® DemoCube → Umsatzerlös (SAP® Demo)*.



Abgeänderte Kopie

	Sparte	Internal	Umsatzerlös 1998	Umsatzerlös 1997	Veränderung in %
15	IDES	7	50.164,00 DM		
16	IDES	7	High Tech	3.228.416,00 DM	
17	IDES	8	Service	66.036,00 DM	
18	IDES	8	Ergebnis	3.345.416,00 DM	
19	Century Inc.	7	High Tech	1.245.704,00	
20	Century Inc.	8	Service	1.17.342,00	
21	Century Inc.	8	Ergebnis	1.263.046,00	
22	ACE Technology	7	High Tech	3.906.469,00 FRF	
23	ACE Technology	7	Ergebnis	3.906.469,00 FRF	
24	Hallec Enterprise	7	High Tech	4.563.706,00	
25	Hallec Enterprise	7	Ergebnis	4.563.706,00	
26	Cannon Electronics	7	High Tech	2.093.656,00 CAD	
27	Cannon Electronics	7	Ergebnis	2.093.656,00 CAD	
28	Gesamtergebnis			11.132.352,00 MD	

Ergebnisliste der Uneingeschränkten Query

Beispiel:

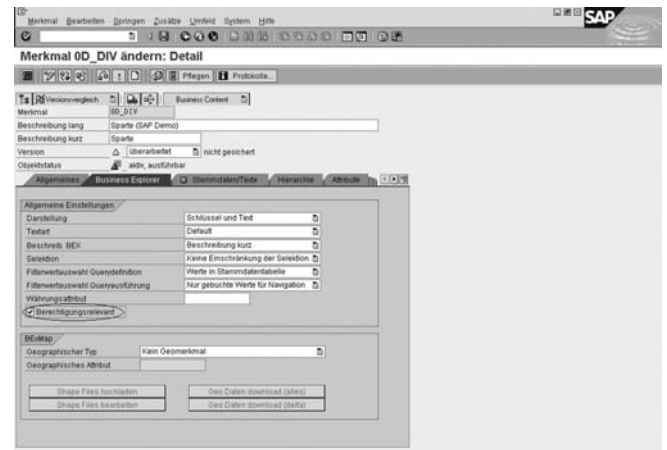
Ein Vertriebsleiter, der eine Query ausführt, soll nur die Ergebnisse der Sparten sehen, für die er verantwortlich ist.

Die folgende Darstellung zeigt auf, welche Schritte bei der Definition der Zugriffsberechtigung auf ein InfoObject zu befolgen sind:

1. Sicherheitsdefinition für ein InfoObject (Sicherheit auf Feldebene)

Die spezifischen Anforderungen des Unternehmens entscheiden darüber, welche InfoObjects für die Sicherheit relevant sind. Die Festlegung "berechtigungsrelevant" für ein InfoObject wird im Register Business Explorer in der InfoObject-Definition vorgenommen. Kennzeichnen Sie das InfoObject

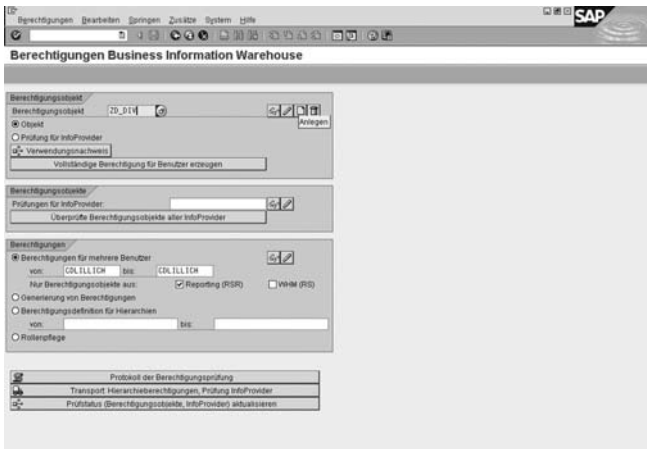
<<Sparte>> als berechtigungsrelevant. Dies geschieht mit Hilfe der *Administrator Workbench (Transaktion RSA1)*, indem Sie *Modellierung* → *InfoObjects* wählen und das entsprechende Objekt ändern. Beachten Sie hierbei, dass die Anwender innerhalb von SAP® BW u.a. Queries ausführen, um die Grundlage für strategische Entscheidungen zu liefern. Demgemäß ist zu beachten, dass diese Mitarbeiter in der Regel Zugang zu mehr Daten benötigen, als dieses in SAP® R/3 der Fall wäre. Eine zu starke Einschränkung würde evtl. nicht brauchbare bzw. in ihrer Aussage unzutreffende Daten zur Folge haben.



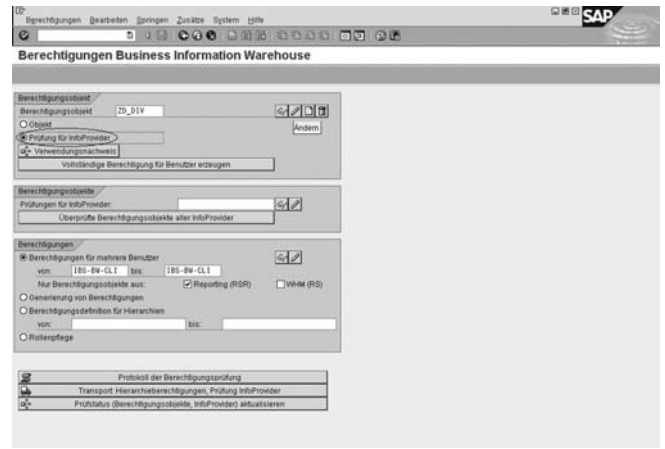
InfoObject ändern

2. Anlage eines spezifischen Reporting-Berechtigungsobjektes

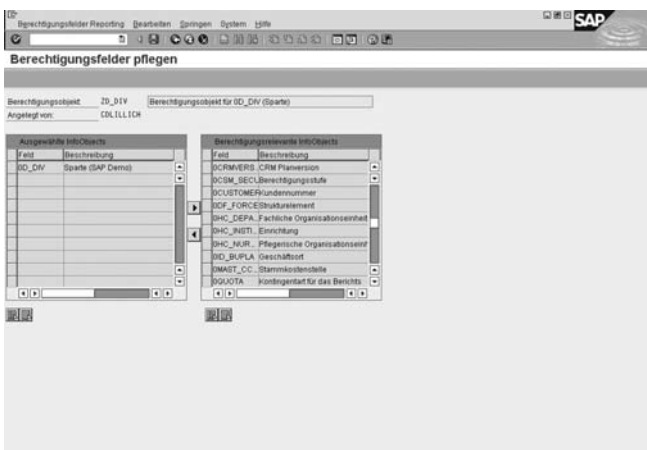
Da seitens der SAP® keine entsprechenden Objekte angeboten werden, müssen Sie für zu schützende InfoObjects eigene Reporting-Berechtigungsobjekte anlegen. Dies geschieht über den Menübaum *SAP® Business Information Warehouse* → *Business Explorer* → *Berechtigungen* → *Reporting-Berechtigungsobjekte* wählen bzw. den Transaktionscode *RSSM* aufrufen. Für die Anlage eines Reporting-Berechtigungsobjektes <<ZD_DIV>> wählen Sie aus einer Liste der berechtigungsrelevanten InfoObjects diejenigen aus, die für dieses spezielle Berechtigungsobjekt relevant sein sollen. Diese erstellten Berechtigungsobjekte werden in der Objektklasse *RSR* (Business Information Warehouse-Reporting) abgelegt. Eine schnelle Übersicht, welche Berechtigungsobjekte welche InfoObjects enthalten können Sie über die Transaktion *SE16* in der Tabelle *TOBJ* mit der Einschränkung "RSR" im Feld *OCLSS* bekommen.



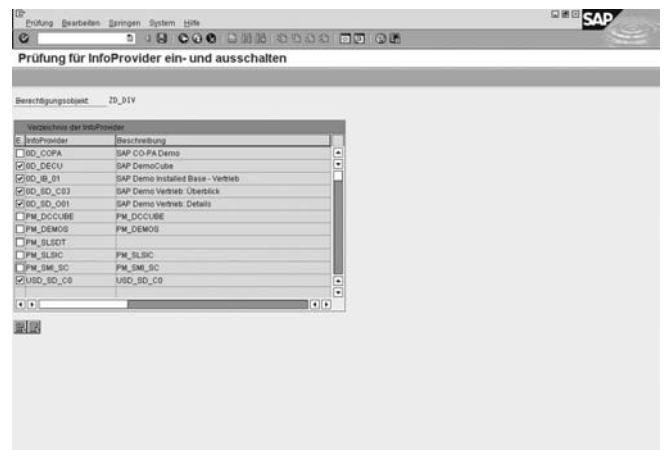
Berechtigungsobjekt anlegen



Prüfung für InfoProvider → Ändern



Berechtigungsrelevante(s) Feld(er) auswählen (max. 10)



Übersicht und Zuordnung (Spalte 1) der berechtigungsrelevanten InfoProvider

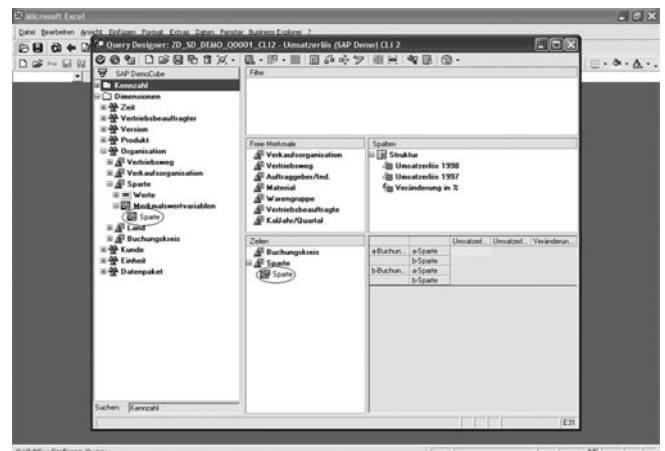
3. Verknüpfung des Reporting-Berechtigungsobjektes mit einem InfoProvider

InfoProvider ist ein Begriff für alle Arten von SAP® Datenspeichern (physische und logische Speicher). Wählen Sie *Prüfung für InfoProvider → Ändern*. Sie erhalten eine Liste der InfoCubes, welche die in dem Berechtigungsobjekt zuvor ausgewählten InfoObjects enthält. Sie haben nun im Änderungsmodus die Möglichkeit, einzelne InfoCubes aus der Berechtigungsprüfung herauszunehmen, indem Sie die Markierung entfernen.

Die Verknüpfung Ihres Reporting-Berechtigungsobjektes mit einem InfoProvider hat zur Folge, dass Anwender, die zuvor Queries auf den InfoProvider ausführen konnten, dieses nach der Verknüpfung ohne eine entsprechende Berechtigung nicht mehr können. Durch die Verknüpfung wird eine Prüfung seitens des Reporting-Berechtigungsobjektes initiiert, sobald eine Query angefordert wird.

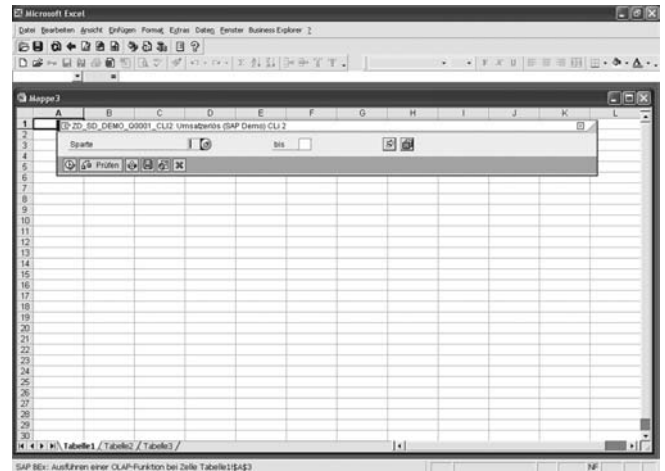
4. Zuordnung des neuen Berechtigungsobjektes zu einer Rolle

Nachdem Sie ein neues Reporting-Berechtigungsobjekt angelegt und mit den entsprechenden InfoProvidern verknüpft haben, benötigen die Anwender ihrer Funktion entsprechend Zugang zu dem neu geschaffenen Reporting-Berechtigungsobjekt. Fügen Sie Ihr Objekt mit den entsprechenden Parametern manuell in eine Rolle ein bzw. erfassen Sie eine neue Rolle.

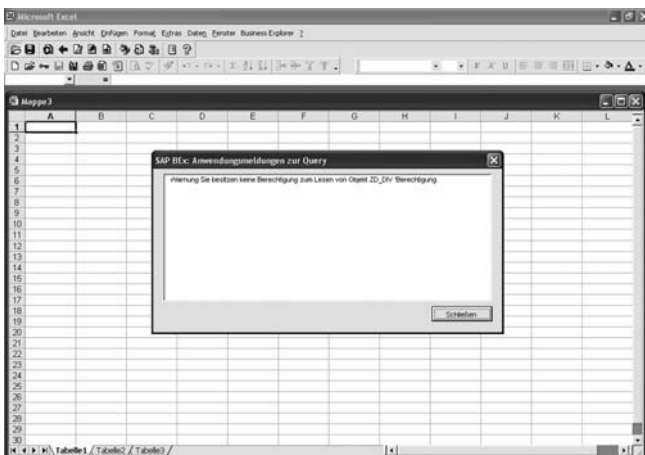


5. Anpassung der Queries

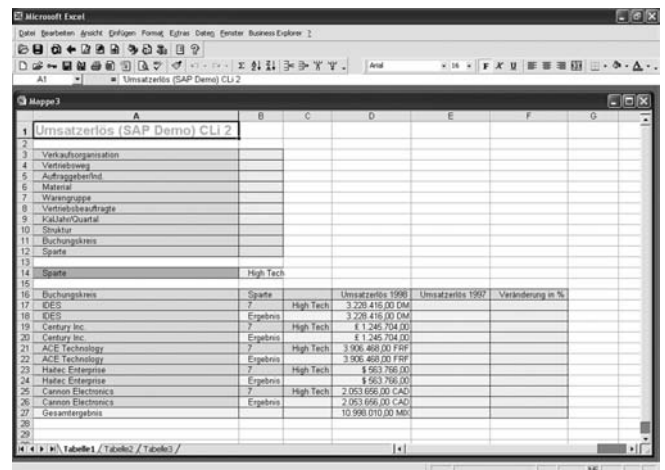
Fügen Sie den durch die vorgenommene Änderung betroffenen Queries eine neue Variable hinzu, indem Sie die Variable <<Sparte>> aus der Liste der Merkmale in die Query-Definition übernehmen. Verwenden Sie die veränderte Version des Queries 0D_SD_DEMO_Q0001, indem Sie über den Pfad der InfoArea *SAP® Demo* → *SAP® Demo Vertrieb* → *SAP® DemoCube* gehen. Über die Hinzufügung von Variablen wird die Filterfunktion einer Query gesteuert. So erhält jeder Mitarbeiter nur die ihm zugeordneten Informationen.



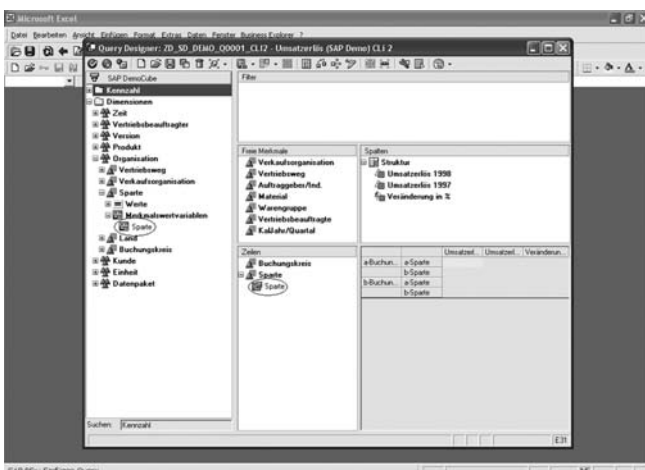
Eingabeaufforderung der Variable Sparte



Berechtigungsmeldung bei nicht geänderter Query bzw. fehlender Berechtigung



Ergebnis bei korrekter Eingabe der berechtigten Werte



Queryanpassung

So erhält jeder Mitarbeiter nur die ihm zugeordneten Informationen.

Wer sein Feld gut bestellt...

kann durch die Einführung einer auf Feldebene basierenden Berechtigungshierarchie eine sehr komplexe und der Situation angepasste Sicherheitsarchitektur aufbauen, in der nur Daten zu den Anwendern gelangen, die die entsprechenden Informationen im Rahmen ihrer Tätigkeit auch benötigen. Im Nebeneffekt erhält das Unternehmen eine übersichtliche Anzahl von InfoProvidern, da Datenspeicher für einzelne Anwender bzw. Gruppen nicht mehr erstellt und gewartet werden müssen. Dieses bedeutet einen Gewinn an Ressourcen durch Optimierung der Prozesse. Wer sich der Mühe unterzieht

...erhält reiche Ernte.



➔ IT-Revision



Liebe Leserinnen und Leser,

die Qualitätsanforderungen an Datenschutz und Sicherheit steigen immer weiter an. Die fortschreitende Vernetzung und Automatisierung von Prozessen ist noch lange nicht am Ende. Immer schneller werden immer mehr Daten und vor allem auch personenbezogene Informationen verarbeitet.

Zwar machen BDSG und andere relevanten Datenschutzgesetze, wie z. B. das TKG oder TDDSG (wobei die letzteren beiden durch das neue Telemediengesetz ab März 2007 abgelöst werden, aber dazu lesen Sie in der nächsten Ausgabe mehr), klare Vorgaben, die jedoch für Auditzwecke nicht geeignet sind.

Möglichkeiten für Audits im Datenschutzbereich diesbezüglich, Standards und deren Anwendbarkeit und Unterstützung für die Revision werden von Prof. Dr. Reinhard Voßbein erläutert.

An einem Beispiel der Prüfung einer "Wide Area Network-Infrastruktur" als ausgelagerte Dienstleistung zeigt Dipl.-Betriebswirt Axel Hirsch auf, welche Probleme und Besonderheiten eine solche Prüfung mit sich bringt und wie eine strukturierte Vorgehensweise für eine solche Prüfung aussehen kann.

Dass Prüfungen und Prüfobjekte nicht immer eine eindeutige Aussage über die Sicherheit oder Qualität bringen, wird Ihnen im Beitrag "Prüfen durch alle Schichten" aufgezeigt, der ein wenig das Blickfeld für das "Drumherum" weiten soll, damit viele, oft unberücksichtigte Aspekte und Punkte, zumindest erwähnt werden und ggf. als Restrisiko definiert werden können.

Ihr

A handwritten signature in black ink, appearing to read "Michael" followed by a stylized flourish.

Michael Foth



➔ Prüfstandards für Datenschutzaudits - Unterstützung der Revisionsarbeit

Prof. Dr. Reinhard Vossbein
UIMCert

1 Datenschutzaudits als Revisionsaufgabe

Datenschutzaudits sind als Kernaufgabe der internen Revision mittlerweile zum Tagesgeschäft geworden. Viele Unternehmen haben dem Umstand, dass der Datenschutzbeauftragte eine Vielzahl von Revisionsaufgaben in seinem spezifischen Bereich wahrzunehmen hat, dadurch Rechnung getragen, dass der Datenschutzbeauftragte in seiner Hauptfunktion Mitglied der Revisionsabteilung ist. Diese Form der Institutionalisierung des Datenschutzes bei einer gleichzeitigen Verbindung zum Bereich Revision hat sich offensichtlich in einem so starken Maß bewährt, dass oft sogar der Leiter der Revision zum Datenschutzbeauftragten berufen wurde.

Auch wenn der Datenschutzbeauftragte nicht Mitglied der internen Revision ist, hat es sich bewährt, Revisionsprojekte im Rahmen des Datenschutzes Mitarbeitern der Revision zu übertragen. Wenn Datenschutz und Revision in Personalunion wahrgenommen werden, stellt sich die Frage der Kompetenz des Revisors im Hinblick auf sein Datenschutzwissen nicht. Wenn jedoch eine Funktionstrennung vorliegt, ist es denkbar, dass der Revisor ein Defizit im Datenschutzwissen aufweist, was dann bei der Wahrnehmung einer Revisionsaufgabe im Datenschutz das Problem des Findens einer geeigneten Vorgabe für die Prüfung im Sinne einer "Messlatte" entstehen lässt. Zwar bietet das Gesetz (BDSG und andere relevante Datenschutzgesetze, wie z. B. das TKG oder TDDSG) eine klare Vorgabe, an der die Ordnungsmäßigkeit der Umsetzung der Datenschutzgesetze im Unternehmen gemessen werden

kann. Andererseits zeichnet sich das Gesetz jedoch speziell für Auditzwecke durch eine zu geringe Präzisierung aus, um ohne weiteres als Prüfgrundlage übernommen werden zu können.

Auf dieses Problem wurde bereits im Rahmen der REVISION unter dem Aspekt eingegangen, dass die Gesetzesformulierungen zur Erstellung von Prüflisten genutzt werden könnten.

2 Das BDSG und das (nicht erlassene) Auditgesetz

Das BDSG unterstützt im Prinzip die professionelle Auditierung des Datenschutzes bei Datenverarbeitungssystemen und Daten verarbeitenden Stellen. Es sagt hierzu:

Datenschutzaudit § 9 a BDSG²

"Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt."

Insbesondere der zweite Satz des zitierten Paragraphen stellt fest, dass noch ein besonderes Gesetz, ein so

genanntes Auditgesetz, erlassen werden soll. Dieses Gesetz ist bisher in seiner Erarbeitung und Verabschiedung politisch variierenden Konstellationen mit unterschiedlichen Interessen am Datenschutz zum Opfer gefallen. Dies ist zumindest für die Revisoren bedauerlich, da sie durch ein hinreichend präzises Auditgesetz deutliche Vorgaben für die Durchführung von Prüfvorhaben erhalten hätten. Wann die unterschiedlichen politischen Interessenlagen es möglich machen werden, das Projekt "Datenschutzauditgesetz" wieder in Angriff zu nehmen, ist noch unklar. Aus diesem Grund scheint es sinnvoll, sich mit dem Gedanken an eine hinreichend präzise Prüfgrundlage zu beschäftigen. Da es sich beim Datenschutz um eine gesetzliche Verpflichtung der Unternehmen handelt, die ebenso zu erfüllen ist wie andere gesetzliche Verpflichtungen aus dem Bereich des Rechnungswesens, erscheint es sinnvoll, eine gedankliche Anleihe in diesem Sektor zu machen, um das Prüfproblem für die Revisoren operational und effizient zu lösen.

3 Auditobjekte und ihre Grundlagen

Das Gesetz stellt im Prinzip fest, welche Auditobjekte Gegenstand einer Prüfung zumindest nach dem Willen des Gesetzgebers sein sollten. Es handelt sich hierbei um

- Datenverarbeitungssysteme und -programme sowie
- Daten verarbeitende Stellen.

Aus Gründen der Klarheit und der präziseren Vorgabemöglichkeiten für Revisoren - unter anderem auch unter Berücksichtigung der in der Zwischenzeit veröffentlichten Prüfungsstandards des IDW für andere Gebiete - sollen die oben genannten zwei Punkte noch ergänzt werden um

- einfache und komplexe Verfahren der Datenverarbeitung personenbezogener Daten.

Diese Auditobjekte sollen im Folgenden genauer definiert werden.

Auditierungsobjekte (Definition und begriffliche Abgrenzung)

- Verantwortliche/Daten verarbeitende Stellen
Daten verarbeitende Stellen sind öffentliche oder nicht öffentliche Stellen/Institutionen, die personenbezogene Daten unter Einsatz von Daten-

verarbeitungsanlagen verarbeiten. Um das Auditierungsproblem besser behandeln zu können, sei darauf hingewiesen, dass Institutionen über eine oder mehrere Daten verarbeitende Stellen verfügen können. Faktisch bedeutet das, dass innerhalb einer Institution komplexe Prozesse sowie einzelne Stellen durch Bestimmung ihrer Schnittstellen mit anderen Prozessen und/oder Stellen abgegrenzt werden können, um so einem Audit unterzogen zu werden, das nicht die gesamte Institution mit sämtlichen in ihr enthaltenen hochkomplexen Prozessen und/oder Stellen umfasst, sondern sogenannte Scopes definiert.

- Produkte
Produkte sollen definiert werden als Erzeugnisse auf dem Softwaresektor, die geeignet sind, eine automatisierte Abwicklung von Abläufen oder Teilabläufen vorzunehmen oder zu unterstützen. Sie sind daher nahezu generell gleichzusetzen mit Programmen, die die gleiche Funktion haben. Typische Produkte sind z. B. elektronische Archivierungssysteme, Personaldatenverarbeitungssysteme, Lohn- und Gehaltsabrechnungssysteme, Kundendatenverarbeitungssysteme oder ähnliche.
- Verfahren/Prozesse
Der Begriff des Verfahrens ist nicht hinreichend klar determiniert. Es soll daher von folgender Definition ausgegangen werden: Als Verfahren gelten minimal solche Prozesse, die ohne automatisierte Teilprozesse, also ohne den Einsatz von Produkten/Programmen ablaufen. Im Regelfall wird aber ein komplexes Verfahren (s. u.) unter Einsatz von Produkten/Programmen ablaufen und hierbei in Kombination mit Organisationsregeln Prozesse oder Teilprozesse beinhalten, die in einer Institution entsprechend den Aufgaben dieser Institution abzuwickeln sind. Als typisch "reine" Verfahren auf dem Datenschutzsektor können z. B. solche der Vernichtung von Datenträgern genannt werden. Bei Verfahren dieser Art kann im Regelfall der Anteil der EDV-Stützung als vernachlässigungswürdig angesehen werden.
- Komplexe Verfahren/Prozesse unter Einschluss von Produkten
Produkte in Kombination mit Verfahren hingegen sind gering-, mittel- oder hochkomplexe Prozesse, die zwangsläufig eine Kombination

von Produkten/Programmen und organisatorischen Abläufen beinhalten, und die nicht sinnvoll zu trennen sind.

Die Einsatzumgebung muss bei der Auditierung mit Gegenstand der Betrachtung sein. Die Rechtfertigung hierzu ergibt sich aus dem BDSG durch die Präambel des Anhangs zum § 9. Hier wird gefordert, dass die Institution die entsprechenden organisatorischen Maßnahmen zu treffen hat, um die in der Anlage nachfolgend aufgeführten Kontrollmaßnahmen sicherzustellen. Eine weitere Rechtfertigung ergibt sich aus den in verschiedenen Landesdatenschutzgesetzen enthaltenen Vorschriften zu einer sog. Vorabkontrolle.

4 Vorhandene Standards

Es gibt mittlerweile eine Anzahl von Standards auf dem Datenschutzsektor, die eine unterschiedliche Ausrichtung haben. Abgesehen von technischen Standards - hier sind die Common Criteria von besonderer Bedeutung und weltweiter Geltung - sind die Standards

- quid
- GoodPrivacy sowie
- Audit-Verordnung des Landes Schleswig-Holstein DSAVO SH

als bedeutungsvoll zu nennen.

Quid ist ein Standard, der insbesondere auf die Auditierung "Daten verarbeitender Stellen" ausgerichtet ist. Seine Eignung für Verfahren ist nur begrenzt, für Produkte im Wesentlichen nicht gegeben. Obwohl quid eine hohe Qualität aufweist, konnte eine Marktdurchdringung und Marktgeltung bisher nicht erreicht werden.

Das schweizerische Gütesiegel GoodPrivacy basiert auf dem BS 7799 und ist von seiner Konzeption ebenfalls auf Daten verarbeitende Stellen ausgerichtet. Insbesondere ist es darüber hinaus möglich, durch Abwandlungen und eine stärkere Anlehnung an den BS 7799 auch eine Prüfung von Softwareentwicklungsumgebungen wahrnehmen/durchführen zu können. Hingegen sind Produktaudits auch mit diesem Standard im Prinzip nicht durchführbar. Inwieweit inzwischen eine Anpassung an den BS 7799 ablösenden Standard ISO 27001 vorgenommen wurde, ist nicht bekannt.

Die Audit-Verordnung des Landes Schleswig-Holstein DSAVO SH ist von ihrer Konzeption her schwerpunktmäßig auf Produkte ausgerichtet. Nähere Informationen hierzu können von der Homepage des ULD gewonnen werden. Dieser Standard ist sehr präzise, wobei eine Übertragung der in dem Standard festgelegten Prüfmodalitäten auf andere Anwendungen als die eigentlich vorgesehenen - Prüfung von Produkten mit dem Einsatz in den Behördeninstitutionen des Landes Schleswig-Holstein - durchaus möglich ist. Hier würde dann dieser Standard als Prüfgrundlage dienen, ohne dass notwendigerweise eine Gütesiegelung durch das ULD erfolgen muss. Im Prinzip hat das ULD auch Prüfgrundlagen für die Auditierung "Daten verarbeitender Stellen" entwickelt, die jedoch von der Konzeption her auf Behörden ausgerichtet sind und daher in ihrer Übertragungsfähigkeit auf andere Institutionen möglicherweise nicht voll gegeben sind.

5 UIMCert Prüfstandards

Aus den Erkenntnissen zu den oben genannten Prüfstandards lässt sich ableiten, dass die unterschiedlichen genannten Auditobjekte differierende Standards erfordern. Dies ist auch in den IDW Prüfstandards in ähnlicher Form vorzufinden, die - wenn auch auf einem anderen Gebiet - ebenfalls eine Ausrichtung unterschiedlicher Art im Hinblick auf die Prüfobjekte aufweisen. Es liegt daher nahe, Prüfstandards für die Datenschutzauditierung so zu entwickeln, dass sie in ihrer Zielrichtung auf die oben genannten Prüfobjekte ausgerichtet sind. Eine solche Ausrichtung weist die Prüfstandard-Reihe der UIMCert auf, wobei die Prüfstandards auf folgende Prüfobjekte ausgelegt sind:

- Prüfstandard PS 101: Standard für die Auditierung von Daten verarbeitenden/verantwortlichen Stellen
- Prüfstandard PS 102: Standard für die Auditierung von Produkten (Programme, Anwendungssysteme)
- Prüfstandard PS 103: Standard für die Auditierung von Verfahren (einfache bis komplexe)

Die UIMCert Prüfstandards stellen sog. proprietäre Prüfstandards dar. Dieser Typ von Standards ist im Prinzip durchaus verbreitet und soll sicherstellen, dass Wertungen und/oder Gütesiegel nur nach ein-

deutig nachvollziehbaren und objektiven Prinzipien vergeben werden.

Die UIMCert Prüfstandards sind in ihrem Aufbau und der Form der Darstellung an der Methode der IDW Standards ausgerichtet und geben der internen Revision die Möglichkeit, sich bei Datenschutzauditorierungen in einem "gewohnten Umfeld" zu bewegen. Im Folgenden sollen anhand von Beispielen diese Standards ausführlicher dargestellt werden, um es dem Revisor zu ermöglichen zu prüfen, inwieweit sie ihm bei seiner Arbeit eine Hilfe sein können.

Die folgenden drei Beispiele sollen einen Überblick über die Struktur, die inhaltlichen Aussagen und über die Gesamtheit der Standardreihe geben.

Prüfungsstandardreihe UIMCert PS 101 - 103	
PS 101 Standard für die Prüfung der Datenschutzordnungsmäßigkeit von verarbeitenden/verantwortlichen Stellen	Der Prüfungsstandard UIMCert PS 101: „Standard für die Prüfung der Datenschutzordnungsmäßigkeit von verarbeitenden/verantwortlichen Stellen“ zeigt die Anforderungen auf, die das Bundesdatenschutzgesetz (BDSG) und andere Datenschutzgesetze zur Wahrung des Ordnungsmäßigkeitsprinzips an jede verantwortliche Stelle richten.
PS 102 Standard für die Prüfung der Datenschutzordnungsmäßigkeit von Produkten/Systemen für die Verarbeitung von personenbezogenen Daten	Der Prüfungsstandard UIMCert PS 102: „Standard für die Prüfung der Datenschutzordnungsmäßigkeit von Produkten/Systemen für die Verarbeitung von personenbezogenen Daten“ zeigt die Anforderungen auf, die bei der Prüfung von Produkten/Systemen zu erfüllen sind, um eine Datenschutzordnungsmäßigkeit zu erreichen.
PS 103 Standard für die Prüfung der Datenschutzordnungsmäßigkeit von Verfahren (mit und ohne DV gestützte Systeme) für die Verarbeitung von personenbezogenen Daten	Der Prüfungsstandard UIMCert PS 103: „Standard für die Prüfung der Datenschutzordnungsmäßigkeit von Verfahren (mit und ohne DV-gestützte Systeme)“ zeigt die Anforderungen auf, die bei der Prüfung von Verfahren unter Einschluss der Einsatzumgebung zu erfüllen sind, um eine Datenschutzordnungsmäßigkeit in betrieblichen Prozessen zu erreichen.

Die Abb. 1 gibt einen Überblick über die Konzeption der Reihe.

Die Abbildung zeigt, dass zwischen den einzelnen Standards Beziehungen bestehen, die Prüfobjekte jedoch deutlich differieren.

Die Abb. 2 gibt einen kompletten Überblick über den Aufbau des Prüfstandards PS 103 und vermittelt, welche Gebiete in ihm abgearbeitet werden und welche Tiefe hierbei vorgegeben wird.

Prüfungsstandard UIMCert PS 103 zur Prüfung von Verfahren	
1. EINLEITUNG	1.1 PRÄAMBEL 1.2 ANWENDUNGSBEREICH 1.3 NORMATIVE VERWEISUNGEN 1.4 BEGRIFFE UND DEFINITIONEN
2. DIE ORDNUNGSMÄßIGKEIT DES VERFAHRENS (OHNE EINSATZUMGEBUNG)	2.1 DATENVERMEIDUNG UND DATENSPPARSAMKEIT 2.2 GESETZESKONFORMITÄT 2.3 ZULÄSSIGKEIT DER ÜBERMITTLUNG UND NUTZUNG 2.4 RECHTE DES BETROFFENEN 2.5 DOKUMENTATIONEN DES VERFAHRENS 2.6 WARTUNG DES VERFAHRENS
3. DIE ORDNUNGSMÄßIGKEIT UNTERSTÜTZENDE MAßNAHMEN DURCH DIE VERANTWORTLICHE STELLE	3.1 ERLASS UND BEFOLGUNG VON ORGANISATIONSANWEISUNGEN 3.2 DATENVERMEIDUNG UND DATENSPPARSAMKEIT 3.3 GESETZESKONFORMITÄT 3.4 RECHTE DES BETROFFENEN 3.5 ZULÄSSIGKEIT DER ÜBERMITTLUNG UND NUTZUNG 3.6 DATENGEHEIMNIS/FERNMELDEGEHEIMNIS 3.7 VERFAHRENSVERZEICHNIS 3.8 VERARBEITUNG IM AUFTRAG 3.9 PRÜFUNG UND FREIGABE 3.10 WARTUNG
4. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN NACH BDSG	4.1 ZUTRIITTSKONTROLLE 4.2 ZUGANGSKONTROLLE 4.3 ZUGRIFFSKONTROLLE 4.4 WEITERGABEKONTROLLE 4.5 EINGABEKONTROLLE 4.6 AUFTRAGSKONTROLLE 4.7 VERFÜGBARKEITSKONTROLLE 4.8 TRENNUNGSGEBOT
5. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN NACH TDDSG	
6. BERICHTERSTATTUNG UND QUALITÄTSSIEGEL	

Der folgende Auszug ist ein Beispiel für die Formulierungen der Standards dieser Reihe

"Datenschutzkonzept (Kapitel 2.1.2 des Standards PS 101)
Alle grundlegenden Datenschutzziele und davon abgeleiteten Richtlinien, Regelungen und Maßnahmen sind in einem organisationsweit gültigen und verbindlichen Datenschutzkonzept schriftlich zu fixieren. Dieses Dokument sollte sowohl Angaben zur definierten DS-Policy als auch die konkrete Beschreibung des Datenschutz-Managementsystems enthalten. Zu letzterem gehören insbesondere aufbau- und ablauforganisatorische Parameter der Datenschutzorganisation. Die Festlegung der relevanten Datenschutzmaßnahmen ist zur Umsetzung der DS-Policy und der Datenschutzziele von den Fachverantwortlichen zu erarbeiten und von der Geschäftsleitung zu verabschieden. Damit einher geht eine Anweisung

zur Umsetzung an die verantwortlichen Mitarbeiter. Arbeitsanweisungen sind von diesen Maßnahmen abzuleiten, zu dokumentieren und den Mitarbeitern zu kommunizieren. Dabei sind auch Zielvereinbarungen festzulegen, die die Vorgaben für die Mitarbeiter konkretisieren, um eine Sensibilisierung und datenschutzkonforme Verhaltensweise und Geschäftstätigkeit sicherzustellen. Kontrollen des Datenschutzkonzepts sind sowohl in regelmäßig definierten Abständen gemäß eines definierten Kontrollverfahrens durchzuführen als auch fallweise bei bedarfsmäßigen Modifikationen vorzunehmen zur Wahrung der Aktualität und Angemessenheit. Der Verantwortliche für den Datenschutz in der Organisation ist zuständig für die Berichterstattung datenschutzrelevanter Fragestellungen und den Fortschritt der Implementierung des DSMS an die Geschäftsleitung zwecks Information und Sensibilisierung. Diese Berichte können dem Datenschutzkonzept als Anlage beigefügt werden, zumindest sind jedoch Verweise auf die entsprechenden Dokumente, inkl. ihres Ablageortes in das Datenschutzkonzept einzubringen. Der Prüfer muss die Berücksichtigung aller Aspekte bezüglich der Dokumentation und Umsetzung untersuchen und seine Ergebnisse nachvollziehbar dokumentieren. Nicht umgesetzte Inhalte sind zu hinterfragen und begründend zu erläutern (z. B. ob eine Umsetzung aufgrund fehlender Relevanz nicht gegeben ist)."

Die Abb. 3 gibt einen auszugsweisen Überblick über den Aufbau des Prüfstandards PS 101 und vermittelt, welche Gebiete in ihm abgearbeitet werden, und welche Tiefe hierbei vorgegeben wird.

Prüfungsstandard UIMCert PS 101 Zur Prüfung von verantwortlichen Stellen (Auszug aus der Struktur)	
1.	Einleitung
2.	Datenschutzstrategie und Datenschutzpolitik - Strategische Ausrichtung des Datenschutzes - Festlegung des Angemessenheitsniveaus - Transparenz der Datenverwendung - Datenschutzrelevante Werte - Rechtskonformität
3.	Datenschutz-Kooperationen
4.	Datenschutzrechtliche Forderungen und Rechte der Betroffenen
5.	Telekommunikationsgesetze und Teledienstschutzgesetz
6.	Sonderformen der Datenverarbeitung
7.	Technische und organisatorische Maßnahmen (TOM) - Zutrittskontrolle - Zugangskontrolle - Zugriffskontrolle - Weitergabekontrolle - Eingabekontrolle - Auftragskontrolle - Verfügbarkeitskontrolle - Trennungsgebot - Informationsausgabe - Allgemeine Informationsverarbeitung - Dokumentationsrichtlinien
8.	Datenschutzschulungen
9.	Berichterstattung und Qualitätssiegel

Der Text des Standards gibt klare Vorgaben für das, was in der Institution vorhanden sein muss und auf

Grund dieses Vorhandenseins Gegenstand der Prüfung ist. Hierbei wurde in einigen Punkten aus stilistischen Gründen und im Hinblick auf die zu leistende Arbeit der Institution selbst darauf verzichtet, jede der dargestellten Anforderungen mit einem expliziten Prüfhinweis zu versehen. Dieser, dann am Ende des betreffenden Absatzes vorzufindende Prüfhinweis, bezieht sich logischerweise auf den gesamten vorstehenden Text.

6 Prüfstandards und Tooleinsatz

Es ist plausibel, dass ein Tooleinsatz umso effizienter ist, je stärker ein Prüfgebiet standardisiert ist. Somit ist die Nutzung eines Standards bei der Prüfung nicht nur eine Voraussetzung für eine effiziente und klar strukturierte Prüfung durch Vorgaben des Standards an sich, sondern auch eine wichtige Bedingung einer Möglichkeit, die Revisionsaufgabe toolgestützt zu lösen. Jedes Tool setzt voraus, dass eine klar formulierte Norm oder Vorgabe die Möglichkeit bietet, durch Abstraktion eine strukturierte Prüfgrundlage zu schaffen. Prüflisten sind als Vorstufe zu Tools anzusehen. Aus dem obigen Text können durch Umformulierung der Aussagen leicht entsprechende Checklisten gewonnen werden. Die primitive Form einer Checkliste kann dann in ein Tool eingebracht werden, das Analyse, Berichterstattung und Bewertung der Feststellungen unterstützt. Im Regelfalle wird ein Prüftool die gleiche Struktur aufweisen wie der ihm zu Grunde liegende Standard. Hiermit würden die in Abb. 2 und 3 genannten Inhalte des Standards Strukturkomponenten eines auf ihm aufbauenden Prüftools bilden.

7 Fazit

Um Prüfungen effizient, nachvollziehbar und in ihren Feststellungen unangreifbar durchführen zu können, sollte die interne Revision sich - sofern nur eben vorhanden - an Normen und/oder Standards orientieren. Diese dienen insbesondere der Rechtfertigung der Prüfobjekte und ihrer Komponenten insofern, als unter Umständen vor Inangriffnahme des betreffenden Prüfprozesses die Vorgaben des Standards in der Institution diskutiert werden können, um im Vorfeld eine Einigung über die der Prüfung zu Grunde liegenden Bewertungsmaßstäbe zu erreichen. Diese Möglichkeit sollte jeder Revisor nutzen, der sich mit Datenschutz-Ordnungsmässigkeitsprüfungen auseinander zusetzen hat. ✚



➔ Prüfung einer "Wide Area Network"-Infrastruktur am Beispiel einer ausgelagerten Dienstleistung

Dipl.-Betriebswirt Axel Hirsch, CISA
Deutsche WertpapierService Bank

Die Deutsche WertpapierService Bank (dwpbank) bietet in ihrer Funktion als führende Transaktionsbank System- und Prozessdienstleistungen rund um Wertpapiere (inkl. Fonds und Derivate) im Wholesale- und Retailgeschäft an. Ihre Idee ist es, sich ausschließlich auf die professionelle und standardisierte Abwicklung von auslagerungsfähigen Prozessen zu konzentrieren.

Betriebswirtschaftlich ausgerichtet folgt sie dabei konsequent dem Industriegedanken einer "modernen Bankfabrik" mit geringer Fertigungstiefe und Konzentration auf das Kerngeschäft. In Folge dessen hat sie, neben anderen Dienstleistungen, den Betrieb ihres Wide Area Network (WAN) ausgelagert. Er ist Teil eines mit einem IT-Dienstleister abgeschlossenen Leistungspaketes und beinhaltet die Bereitstellung und den Betrieb einer standortübergreifenden Netzinfrastruktur.

Aufsichtsrechtliche Regelungen verlangen, dass (hier verkürzt wiedergegeben) die Auslagerung von wesentlichen Bereichen des Bankgeschäftes weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen noch die Steuerungs- oder Kontrollmöglichkeiten der Geschäftsleitung beeinträchtigen darf. Vor diesem Hintergrund und der Gegebenheit, dass der beauftragte IT-Dienstleister nach deutschem Aufsichtsrecht nicht über eine operativ angemessene IT-Revision verfügt, nimmt die dwpbank eigene Prüfungen beim Dienstleister vor. Der nachfolgende Artikel beschreibt die dabei gemachten

Erfahrungen und gibt dem Prüfer in einer Art Checkliste Prüfungsschwerpunkte an die Hand.

1 Gesetzliche Grundlagen

Die im Rahmen einer Auslagerung zu beachtenden wichtigsten gesetzlichen Vorgaben seien hier der Vollständigkeit halber nochmals erwähnt:

1.1 § 25a Abs. 2 KWG

Die Auslagerung von Bereichen auf ein anderes Unternehmen, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, darf weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen noch die Steuerungs- oder Kontrollmöglichkeiten der Geschäftsleitung noch die Prüfungsrechte und Kontrollmöglichkeiten der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) beeinträchtigen. Das auslagernde Institut hat sich insbesondere die erforderlichen Weisungsbefugnisse vertraglich zu sichern und die ausgelagerten Bereiche in seine internen Kontrollverfahren einzubeziehen. Das Institut hat die Absicht der Auslagerung sowie ihren Vollzug der BaFin und der Deutschen Bundesbank unverzüglich anzuzeigen.

1.2 MaRisk AT 9

Die teilweise oder vollständige Auslagerung von Aktivitäten und Prozessen darf nur unter der

Maßgabe der im § 25a Abs. 2 KWG niedergelegten Grundsätze sowie der Einhaltung diesbezüglich erlassener Regelungen erfolgen.

1.3 Rundschreiben 11/2001 des BaFin zur Auslagerung von Bereichen auf ein anderes Unternehmen gemäß § 25a Abs. 2 KWG.

Kapitel V Nr. 3 "Anforderungen an zulässige Auslagerungen" verlangt hier u.a. folgendes:

"Das Institut hat das Auslagerungsunternehmen mit der erforderlichen Sorgfalt auszuwählen, es angemessen in seine Aufgabe einzuweisen und zu überwachen" sowie "Die Leistungserbringung des Auslagerungsunternehmens ist laufend zu überwachen und zu beurteilen, so dass notwendige Korrekturmaßnahmen sofort ergriffen werden können.

Es ist institutsintern für jede Auslagerung eine verantwortliche Stelle zu definieren, die für die Überwachung und Steuerung der jeweiligen Auslagerungsmaßnahme zuständig ist."

Da unser Dienstleister über keine nach deutschem Aufsichtsrecht operativ angemessene IT-Revision verfügt, wurde vertraglich vereinbart, dass die IT-Revision der dwpbank diese Funktion wahrnimmt und die Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit der ausgelagerten Dienstleistungen prüft.

Hierfür wurde durch uns ein mehrjähriger Prüfungsplan entwickelt, der am Anfang eines jeden Jahres spezifiziert wird. Ebenfalls zu Beginn eines jeden Jahres werden die Prüfungsthemen und die Zeiträume der stattfindenden Prüfungen dem Dienstleister kommuniziert mit dem Ziel, die benötigten Ressourcen rechtzeitig für die Prüfungen disponieren zu können.

Im Rahmen des Auslagerungs-Vertragsverhältnisses wurden mit dem Dienstleister außerdem verfahrenstechnische Fragestellungen wie zeitlicher Vorlauf der Prüfungsankündigung, Eröffnungsgespräch, Fragen zum Ablauf der Prüfung, Feststellungen und deren Einstufungskriterien, Berichtsentwurf, Berichtsbesprechung, Schlussbesprechung sowie die Nachverfolgung und Ausräumung von Mängeln festgelegt.

2 Prüfungsschwerpunkte

Die von der dwpbank eingekaufte Dienstleistung "WAN-Services" umfasst die Bereitstellung und den Betrieb der standortübergreifenden Netzinfrastruktur. Das Prüfungsvorgehen, sozusagen der "rote Faden", orientierte sich an den vereinbarten Service Level Agreements und umfasste folgende Schwerpunkte:

- Ordnungsmäßigkeit der Dokumentation des WAN
- Administration und Betrieb des WAN
- Change- und Störungsmanagement
- Physische und logische Sicherheit

Der Prüfungsplanung lag übergeordnet die Systematik des COBIT-Frameworks zugrunde. Die Prüfungsschwerpunkte orientierten sich in ihrer Struktur an den mit dem IT-Dienstleister gelebten Prozessen. Die relevanten COBIT-Kontrollziele wurden durch weitere, in der Regel technisch orientierte, Prüfungsfragen ergänzt.

Im nachfolgenden Text werden neben der Beschreibung von Sachverhalten dem Prüfer Checklisten für die Praxis an die Hand gegeben.

3 Ordnungsmäßigkeit der Dokumentation des Wide Area Network

Zur Wertpapierabwicklung kommen in der dwpbank komplexe und weitgehend integrierte Informations- und Kommunikationssysteme zum Einsatz.

Die rechtlichen Grundlagen für das Erstellen einer Dokumentation der für die Wertpapierabwicklung sowie Rechnungslegung angewandten Verfahren ergeben sich z. B. aus den §§ 238 ff. des Handelsgesetzbuches (HGB), in denen u. a. Grundsätze für die Führung von Handelsbüchern definiert sind.

Die inhaltlichen Vorgaben für die Verfahrensdokumentation wurden zuletzt 1995 in den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) festgelegt. In Folge dessen müssen aus der Verfahrensdokumentation für einen sachverständigen Dritten in angemessener Zeit und ohne Kenntnis der Programmiersprache der Inhalt sowie Aufbau und Ablauf des Verfahrens vollständig ersichtlich und nachvollziehbar sein. Die GoBS ver-

lassen jedoch nicht einen bestimmten, relativ hoch angesiedelten, Abstraktionsgrad, wodurch man als Prüfer nicht selten in eine Diskussion kommt, was noch als ausreichende Qualität anzusehen ist.

Neben den formalen Aspekten besteht jedoch ein unabdingbares materielles Interesse an einer guten Dokumentation, denn:

- Die Systeme werden immer komplexer.
- Die Innovationsabstände werden immer kürzer.
- Die Personalfuktuation nimmt in einigen Bereichen ständig zu.
- Die Abhängigkeit von Kopfmonopolen sollte reduziert werden.
- Der Trend zur Auslagerung nimmt zu und damit die Pflicht zur Kontrolle und Steuerung des Dienstleisters.
- Die Basis für Planung, Steuerung und Kontrolle des IT-Einsatzes sowie für die Notfallvorsorge liefert eine aktuelle Dokumentation der vorhandenen IT-Systeme.

Durch den vermehrten Einsatz von gekaufter Software ist ein großer Teil der Dokumentation von dem Systemlieferanten bzw. -hersteller zur Verfügung zu stellen. Dabei sind die Standardhandbücher allerdings oft nicht ausreichend, so dass die Lieferung einer im Sinne der GoBS vollständigen Verfahrensbeschreibung bereits mit Abschluß des Kaufvertrages vom Hersteller unbedingt vertraglich zu vereinbaren bzw. vom Dienstleister zu erstellen ist.

4 Dokumentation der WAN-Netzstruktur

Die dwpbank praktiziert eine Multi-Provider-Strategie. Dies erfordert eine klare Festlegung, Abgrenzung und Dokumentation der Verantwortlichkeiten.

Bezüglich einer zu prüfenden WAN-Netzstruktur muß somit explizit erkennbar sein, welche aktiven und passiven Netzkomponenten in die Verantwortung des IT-Dienstleisters fallen. Sind an dem Prozess mehrere Dienstleister beteiligt, müssen die Übergabepunkte der Verantwortung eindeutig definiert sein.

Häufig, jedoch auf den ersten Blick nicht zu erkennen, bedient sich der Dienstleister weiterer Subunternehmer. Hier ist darauf zu achten, dass der

Dienstleister vertraglich verpflichtet wird, zwischen ihm und dem Subunternehmer die gleichen Verpflichtungen wie zwischen der dwpbank und dem Dienstleister zu vereinbaren. Eine Weiterverlagerung ist außerdem gegenüber dem auslagernden Unternehmen anzuzeigen. Gleichzeitig sind ausreichende Informationen über den Subunternehmer zur Verfügung zu stellen, damit eine umfassende Beurteilung dessen Leistungsfähigkeit möglich ist.

Eine ordnungsgemäße Netzdokumentation muss folgende Fragen beantworten können:

- Welche Bandbreiten kommen zum Einsatz?
- Welche Protokolle "gehen" über die Leitungen?
- Sind die Verantwortungsbereiche des IT-Dienstleisters klar abgegrenzt?
- Sind die Übergabepunkte zu anderen IT-Dienstleistern eindeutig ersichtlich?
- Sind angemessene Backup-Leitungen vorhanden?
- Sind die Netzübergänge dokumentiert?
- Sind die Netzübergänge (durch Firewallsysteme) abgesichert?
- Sind die Positionen der Router und Switches erkennbar?

5 Administration und Betrieb des WAN

In unserem Haus bedient sich der IT-Dienstleister für die Bereitstellung und den Betrieb der passiven Netzkomponenten (Leitungen) eines weiteren Dienstleisters (= Subunternehmer). Die aktiven Netzwerkkomponenten jedoch administriert er selbst.

Nachfolgende Fragen sollten hier beantwortet werden:

- Sind für den Betrieb der WAN-Strecken Service Level Agreements (SLA's) vereinbart?
- Sind die SLA's angemessen (z.B. im Hinblick auf Dauer des überwachten Betriebes oder der Reaktionszeiten im Falle einer Störung)?
- Sind für die Administration und den Betrieb der aktiven und passiven Netzkomponenten aktuelle und dokumentierte Anweisungen vorhanden?
- Sind diese Anweisungen umgesetzt?
- Wie erfolgt die Überwachung der aktiven und passiven Netzkomponenten?
- Mit welchem Tool erfolgt die Überwachung?

- Ist die personelle und technische Ausstattung für die Überwachung ausreichend?

6 Change- und Störungsmanagement

Das Ziel der hier zu etablierenden Prozesse sollte sein, strukturierte und wiederholbare Prozesse zu entwickeln, die genutzt werden können, um Änderungen in der IT-Umgebung zu verwalten, damit die damit verbundenen Services nur minimalen Störungen ausgesetzt werden.

Der Prüfer muß sich hier ein Bild machen, inwieweit angemessene Prozesse definiert sind, damit mit dem IT-Dienstleister Änderungen initiiert, dokumentiert, genehmigt, durchgeführt und nachgehalten werden können.

In der dwpbank ist hierfür ein sogenanntes "Lagezentrum" geschaffen worden. Dies dient als zentraler Ansprechpartner, zentrale Meldestelle sowie zentraler Verteiler von Informationen zum Status aller in der dwpbank produktiv eingesetzten DV-Systeme. Ein aktives Eingreifen des Lagezentrums erfolgt dann, wenn das aufgetretene Problem nicht in einem kurzfristigen Zeitraum lösbar ist. Das Lagezentrum sorgt bei Bedarf für die Bildung eines Expertenteams mit Beteiligung der betroffenen Leiter der Organisationseinheiten, Providern sowie Vertretern aus der Anwendungsentwicklung und den Fachbereichen.

Der Prüfer sollte klären, ob nachfolgende Prozesse geregelt sind:

- Wie wird kontrolliert, dass die zugesicherten Leistungen und Standards eingehalten werden?
Zum Beispiel:
 - Wartungszustand der Systeme u. Anwendungen
 - Performance
 - Verfügbarkeit
 - Qualitätsniveau
 - Vereinbarte Sicherheitsstandards
 - Proaktives Kapazitätsmanagement
- Wie wird auf Systemausfälle reagiert?
- Existiert ein Problemmanagementprozess zwischen den Providern und der dwpbank?
- Werden Fehler u. Störfälle in Kategorien nach Art, Schwere und Dringlichkeit eingeteilt?
- Welche Tools kommen zum Einsatz?

- Sind Reaktionszeiten und Eskalationsstufen festgelegt?
- Erfolgt ein geregelter Kommunikationsprozess zwischen den Providern und der dwpbank?
- Über welche Medien erfolgt die Kommunikation?
- Werden alle offenen und geschlossenen Probleme dokumentiert?

7 Physische und logische Sicherheit

Ein Netz besteht aus aktiver und passiver Netztechnik. Als passive Netztechnik wird in erster Linie die strukturierte Verkabelung verstanden. Hierzu gehören Patch-Felder (über Steckfelder konfigurierbare Kabelverteiler), Schutzschränke, Anschlussdosen am Arbeitsplatz sowie die Leitungsverbindungen.

Zur aktiven Netztechnik gehören beispielsweise Hubs, Bridges, Switches und Router, wobei in modernen Netzen fast nur noch Switches zum Einsatz kommen.

Der Schwerpunkt der Prüfung liegt hier auf der Sicherheit der zum Einsatz kommenden Router und Switches sowie der Leitungen.

7.1 Prüfungsschwerpunkt "aktive Netzwerkkomponenten"

Router und Switches bilden die Basis und das Rückgrat der IT-Infrastruktur. Sie müssen deshalb vor unerlaubten Zugriffen und Manipulationen geschützt werden.

Der Prüfer sollte nachfolgende Fragen klären:

- Gibt es eine mit dem IT-Dienstleister abgestimmte Sicherheitsrichtlinie, die auch Regelungen zur sicheren Konfiguration von Routern und Switches enthält?
- Erfolgt die Administration über ein eigenes Netz?
- Wenn nein, werden dann nur Protokolle benutzt (bspw. ssh), die eine gesicherte Authentisierung und verschlüsselte Übertragung unterstützen?
- Welches Tool wird für die Administration der Router und Switches eingesetzt?
- Ist sicher gestellt, dass zeitnah Security Patches bzw. Betriebssystem-Updates eingespielt werden?

- Wie erfolgt das Monitoring der Router und Switches?
- Werden, sofern vorhanden, voreingestellte Benutzerkonten ("normale" Benutzer- sowie Adminkonten) geändert?
- Sofern vorhanden: Sind normale Benutzerkonten und deren Rechte dokumentiert?
- Ist sicher gestellt, dass alle Standardpasswörter geändert werden?
- Ist sicher gestellt, dass Passwörter nicht im Klartext in den Konfigurationsdateien gespeichert werden?
- Ist sicher gestellt, dass beim Login auf den Geräten die Login-Nachricht keine Informationen enthält, die einem potentiellen Angreifer von Nutzen sein können (Stichwort: Login-Banner)?
- Werden Protokollierungsfunktionen genutzt?
- Wenn ja, sind der Umfang der Protokollierung und die Kriterien für deren Auswertung dokumentiert?
- Ist sicher gestellt, dass alle nicht genutzten Ports deaktiviert sind?
- Werden von den Konfigurationsdateien (sowohl Default-Konfiguration als auch die Konfiguration für den Produktionseinsatz) Sicherungskopien erstellt?
- Ist sicher gestellt, dass unnötige Netzdienste deaktiviert werden?
- Sind die Access-Control-Listen der Border-Router so konfiguriert, dass an den externen Schnittstellen Pakete blockiert werden, deren Absender-IP im internen Netz liegt?
- Sind die Access-Control-Listen der Border-Router so konfiguriert, dass an den internen Schnittstellen Pakete blockiert werden, deren Absender-IP nicht im internen Netz liegt?
- Wenn ja, findet hier eine Protokollierung und gegebenenfalls eine Alarmierung statt?

Prüfungsfragen speziell für Switches:

- Wird bei Switches flächendeckend ein MAC-Locking eingesetzt?
- Wird das Spanning Tree Protocol eingesetzt?
- Wenn ja, sollte eine Deaktivierung auf allen Endgeräte-Ports erfolgen.

Welche Sicherheitsmassnahmen wurden getroffen (z.B. Verschlüsselung, Ausfallsicherheit)?

- Wird das Trunking Protocol eingesetzt?
- Wenn ja, sollte eine Deaktivierung auf allen Endgeräte-Ports erfolgen.

7.2 Prüfungsschwerpunkt "passive Netzkomponenten"

Hier sollten folgende Fragen beantwortet werden:

- Welche Sicherheitsmassnahmen wurden getroffen (z.B. Verschlüsselung, Ausfallsicherheit)?
- Welche Massnahmen kommen im Störfall zur Anwendung?
- Ist die Bandbreite der Leitungen sowie der Backup-Leitungen angemessen?
- Welche Servicegrade wurden vereinbart?
- Sind diese angemessen, besonders im Hinblick auf Konformität bezüglich der Mandanten zugesagten Service Levels?
- Wie werden die Leitungen überwacht (Monitoring)?

Es empfiehlt sich außerdem, eine Vor-Ort-Besichtigung der Technikräume bzw. des Rechenzentrums durchzuführen, um eine erste Einschätzung bezüglich der baulichen Gegebenheiten, Sicherheitsvorkehrungen, Brandschutzmaßnahmen usw. zu treffen.

8 Lessons learned

Mit Prüfungen im Rahmen von § 25a Abs. 2 KWG "direkt vor Ort", also beim "Insourcer", betreten wir sowie unser Dienstleister "Neuland". Wir begannen einen Lernprozess, der bis dato noch nicht abgeschlossen ist.

Die Prüfung der WAN-Infrastruktur als ausgelagerte Dienstleistung war diesbezüglich unsere erste Prüfung. Wir machten dabei die nachfolgenden Erfahrungen, die wir stichpunktartig wiedergeben:

- Service Level Agreements waren nicht immer durchgehend vorhanden.
- Nicht alle operativen Sachverhalte waren geregelt.
- Die Verträge mit dem Dienstleister waren (teilweise) noch nicht rechtskräftig unterzeichnet.
- Die Steuerung und Kontrolle der ausgelagerten Bereiche war verbesserungsbedürftig.
- Die Aufgaben, Verantwortlichkeiten und Kontrollen zur Überwachung und Steuerung der ausgelagerten Leistungen waren noch nicht vollumfänglich geregelt.

- Spezialwissen beim Dienstleister war entgegen den Erwartungen nicht immer verfügbar.
- Es traten an verschiedenen Stellen Meinungsverschiedenheiten auf, ob die vom auslagernden Unternehmen angeforderte Leistung in Scope ist oder nicht.
- Zusatzaufträge beim Dienstleister, die nicht durch Vertrag abgedeckt sind, kosten viel Geld.
- Prüfungen gestalten sich langwierig und sind mit hohem Abstimmungsaufwand verbunden.
- Ein Bewusstsein für die Belange der IT-Revision sowie deren Prüfungstätigkeit muss sich beim Dienstleister erst etablieren.
- Für beide Parteien (Out- und Insourcer) ist es ein langwieriger Lernprozess.
- Das Erkennen von Mängeln und deren Ausräumung führte letztendlich zu einer qualitativen Verbesserung der Prozesse beim Dienstleister sowie in der dwpbank.
- Sorgfältig vorbereitete Prüfungen beim Dienstleister im Rahmen von § 25a Abs. 2 KWG können helfen, die Qualität der eingekauften Dienstleistung zu verbessern.



FKCI Fachkonferenz "CIO"

Sicherheit, Effizienz und Prüfbarkeit des IT-Betriebs



Ort: Hotel Hafen Hamburg, Hamburg
Termin: 07.12.-08.12.2006
Zielgruppe: CIOs, RZ-Leiter, Leiter IT-Revision

Anlass und Zielsetzung:

KonTraG, Sarbanes Oxley Act (SOA), Deutscher Corporate Governance Kodex (DCGK) und die daraus resultierenden Anforderungen an Geschäftsleitung und Abschlussprüfer haben unmittelbare und mittelbare Auswirkungen auch auf den IT-Betrieb, der das gesamte Unternehmen integral durchdringt. Die u.a. aus diesen Forderungen abgeleiteten Normen und Prüfungsstandards anerkannter Institutionen zur Einrichtung und nachhaltigen Etablierung eines ordnungsgemäßen, sicheren und wirtschaftlich zu betreibenden IT-Betriebs sind schier unübersehbar geworden.

Diese Konferenz

- stellt IT-Entscheidern und -Prüfern diese Vorgaben zur Diskussion,
- bewertet und relativiert sie,
- grenzt sie gegeneinander ab,
- informiert über Möglichkeiten und Grenzen dieser Vorgaben und

legt damit die Entscheidungsgrundlagen für die effiziente und effektive Implementierung, Zertifizierung und Vereinheitlichung der wesentlichen organisatorischen und technischen Regelungen und Abläufe im eigenen und "outgesourceten" IT-Betrieb.

Fordern Sie gerne die ausführliche (kostenfreie) Agenda an:

IBS Schreiber GmbH • Friedrich-Ebert-Damm 145 • 22047 Hamburg
 FON: +49 (0) 40 - 69 69 85-15 • FAX: + 49 (0) 40 - 69 69 85-31
 eMail: seminare@ibs-hamburg.com • www.ibs-hamburg.com



➔ Prüfung durch alle Schichten

Dipl.-Ing. Michael Foth
IBS Schreiber GmbH

Die Prüfungen der Revision im IT-Bereich werden nach den eindeutigen Strukturen und Vorgehensweisen der Prüfungsplanung vorgenommen.

So werden im Rahmen der Prüfungsplanung die Prüfobjekte klar definiert. Dieser Ansatz ist richtig und die Vorgehensweise sieht es auch so vor. Jedoch ist in den meisten Fällen die Bewertung des Ergebnisses der Prüfung beim genauen Hinsehen nicht ganz richtig. Mit der Aussage zu einer durchgeführten Prüfung über den Stand der Sicherheit des Prüfobjektes werden viele Aspekte, die auf diese Bewertung Einfluss nehmen können, gar nicht berücksichtigt.

Wird zum Beispiel das Berechtigungskonzept eines SAP-HR-Systems geprüft, und liefert das Ergebnis eine gute Aussage über das Berechtigungskonzept, lässt sich daraus noch nicht eine qualitative Aussage über die Sicherheit der HR-Daten ableiten.

In diesem Beitrag sollen für den Ansatz von Prüfungen Aspekte aufgezeigt werden, die zumindest in der Prüfungsplanung und in der Berichtserstattung eine Berücksichtigung aller Schichten vornimmt. Somit kann eine realistische Einschätzung der Gesamtqualität der Prüfung und vor allem die Hinweise auf nicht geprüfte Bereiche erfolgen und die Definition und die Hinweise auf das Restrisiko berücksichtigt.

Ein Prüfobjekt

Als Beispiel soll die Berechtigungsprüfung eines SAP-HR-Systems dienen. Der Prüfungsumfang ist in

der Regel schnell und eindeutig formuliert und die Vorgehensweise meistens klar.

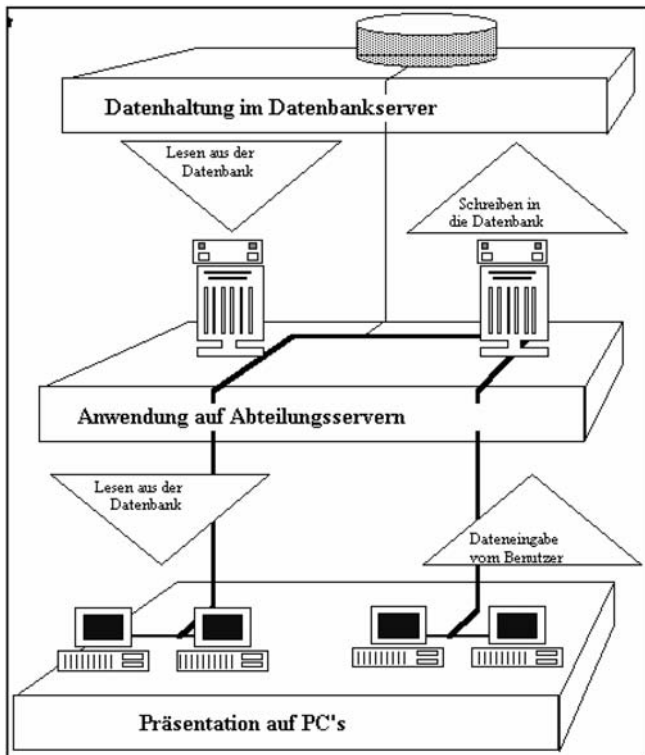
Die Aussage des Prüfungsergebnisses kann sich jedoch nur auf die Benutzerverwaltung und deren Rechte innerhalb der Anwendung SAP beziehen. Eine Aussage über Sicherheit oder gar Möglichkeiten der Manipulation des Datenbestandes des HR-Bereiches ist damit nur zum Teil möglich.

Die Kommunikation

Bereits bei der Prüfungsplanung müssen daher alle möglichen Nebenquellen der Beeinflussung, Umgehung oder Risiken, die das Prüfobjekt betreffen, definiert und in die Prüfung einbezogen werden oder im Bericht als bekannt, aber nicht geprüft, erwähnt werden, damit diese Risiken sichtbar sind und ggf. zu einem späteren Zeitpunkt berücksichtigt werden können oder das Restrisiko definiert werden kann.

Ein SAP-HR-System besteht in der Regel aus einem Anwendungsserver (mit dem eigentlichen SAP-System), einem Datenbank-Server (mit den HR-Daten) und Anwendern, die diese Daten über die Anwendung nutzen.

Es geht um alles "drumherum", wo es noch Möglichkeiten gibt, die die Sicherheit der HR-Daten einschränken oder umgehen lassen.

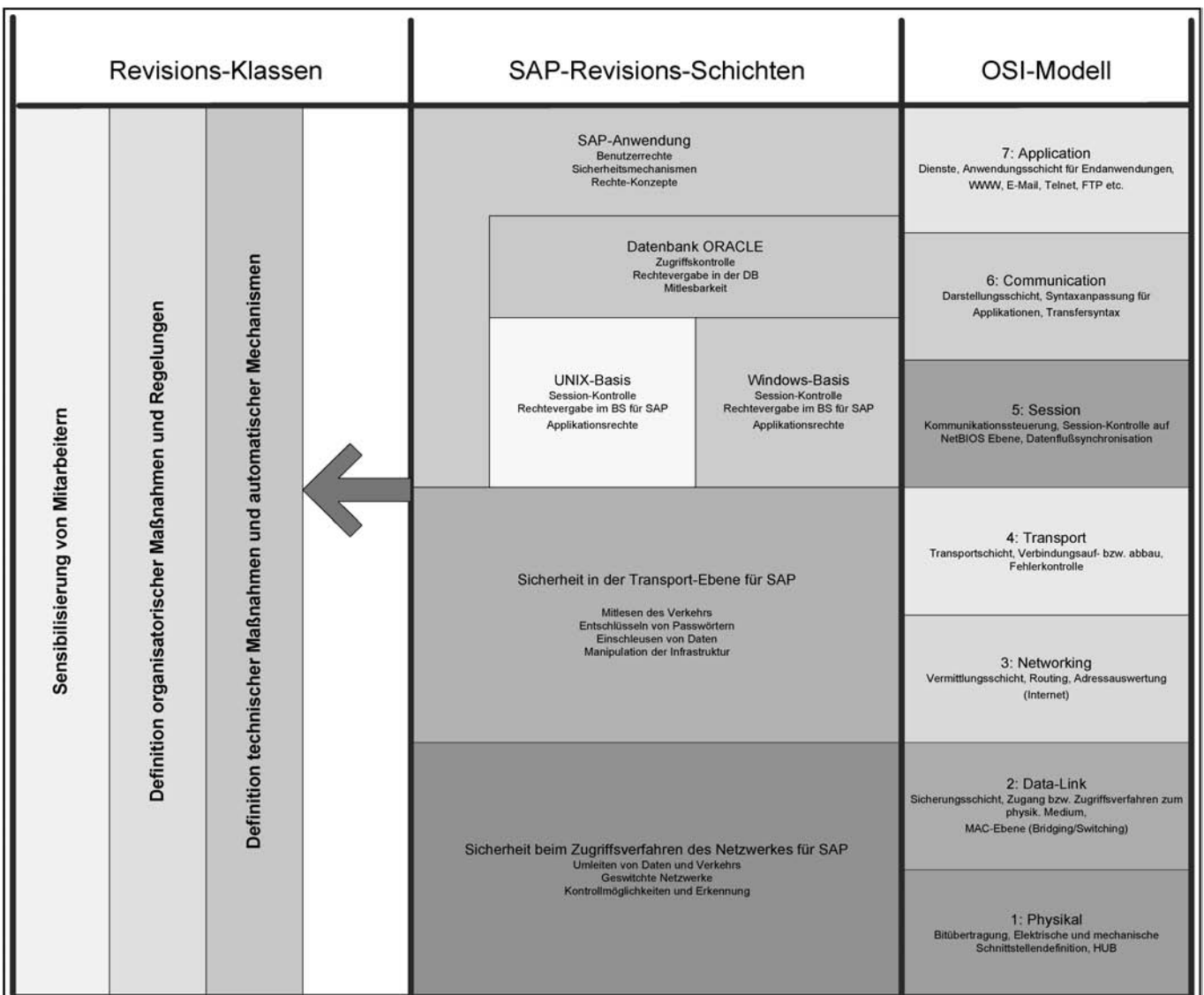


Hinzu kommt bei klassischen Systemen, dass es neben dem Produktiv-System auch das Testsystem und das Entwicklungssystem gibt. Die hier gemachten Betrachtungen gelten für alle drei Systeme gleichermaßen.

Betrachtet wird hier nicht die Prüfung des Berechtigungskonzeptes, denn das wird als eigentliches Prüfobjekt in diesem Beispiel vorausgesetzt. Es geht um alles "drumherum", wo es noch Möglichkeiten gibt, die die Sicherheit der HR-Daten einschränken oder umgehen lassen.

Definition von Schichten

Wenn strukturiert alle Bereiche erfasst werden sollen, müssen strukturierte Schichten-Modelle angewendet werden. Die meisten denken dabei an das OSI-7-Schichten-Modell, das hier nur zum Teil anwendbar ist. In der Darstellung wird dieses aber mit aufge-



führt, um eine Abbildung zu den Schichten der Revisions-Prüfung darzustellen.

Die eigentliche Prüfung des Berechtigungs-Konzeptes im SAP-HR ist Prüfung nur auf der Applikations-Ebene (max. Schicht 6 und 7 im OSI-7-Schichten-Modell).

Das SAP-System kommuniziert über seine Berechtigungsstrukturen mit einer Datenbank. Innerhalb der Datenbank gibt es keine Berechtigungsstruktur mehr. Das SAP-System kommuniziert mit einem einzigen User vom SAP-System zur Datenbank. Alle Einschränkungen und Rechte zum Anwender hin werden durch das SAP-System geregelt. Daher muss der Sicherheit und der Prüfung der Kommunikation zwischen dem SAP-System und der Datenbank viel Aufmerksamkeit gewidmet werden. Denn wenn ein direkter Zugriff auf die Datenbank erlangt werden kann, wird das gesamte Berechtigungskonzept des SAP-Systems umgangen.

Die Betriebssysteme

Beide Systeme, das SAP-System und das Datenbank-System, befinden sich auf Maschinen mit einem Betriebssystem (in der Regel UNIX, Linux oder Windows).

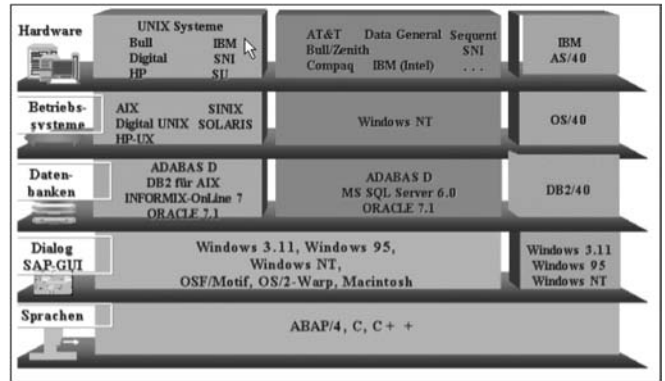
Auch hier ergeben sich schnell Angriffspunkte, über die Zugang zum Betriebssystem und von dort dann mit administrativen Rechten sehr schnell der Gesamt-Zugriff auf die Datenbank erlangt werden kann. Und somit würde auch hier wieder das gesamte Berechtigungskonzept des SAP-Systems umgangen werden.

Das Herausfinden von Schwachstellen und Lücken bei Betriebssystemen setzt heute kein Spezialistenwissen mehr voraus. Systeme, die dann nicht aktuell gepatched oder gepflegt sind, lassen sich einfach erobern und bieten somit Hintertüren, die lange unerkannt bleiben.

Das hat auch mit dem Betrieb der Systeme zu tun. Dazu aber etwas später mehr.

Und weiter unten ...

Unter den Betriebssystemen, was kommt da? Die Hardware ist zwar in den meisten Fällen unkritisch,



da der Zugang zu ihr in abgesicherten Räumen platziert ist. Doch von der Hardware gibt es eine Verbindung zum Netzwerk, über das mit den Anwendern kommuniziert wird.

Die Anwender erreichen das SAP-Anwendungssystem mit einer Kommunikations-Struktur (in der Regel mit dem Protokoll TCP/IP) über ein mehr oder weniger großes Netzwerk. In diesem Netzwerk befinden sich so genannte aktive Komponenten. Das sind Router, Hubs, Switche, Gateways, usw. Auch diese Systeme bieten Möglichkeiten für Angriffe und vor allem für das Mitlesen oder Umleiten von Netzwerk-Verkehr.

Dieses heute auszunutzen bedarf ebenfalls wenig Fachwissen. Mit einfachen Tools kann man bereits diese Funktionen nutzen. So besteht die Möglichkeit ggf. den Netzwerkverkehr zwischen einem Anwender und dem SAP-System abzuhören und an dessen Login-Daten zu gelangen.

Noch kritischer ist es, wenn die Kommunikation zwischen dem SAP-System und dem Datenbank-System belauscht werden kann. Denn damit käme man an die Login-Daten, die einen Vollzugriff direkt auf die Datenbank schaffen würden.

Es sei hier aber auch gesagt, dass sich durch entsprechende Konfigurationsmöglichkeiten (die nicht in den SAP-Standard-Installationen berücksichtigt werden) einige dieser unberechtigten Zugriffsmöglichkeiten einschränken oder verhindern lassen.

Vielfältige Möglichkeiten

Es seien hier nur einige technische Schichten aufgezeigt, die bei einer Prüfung für eine Aussage über Datensicherheit zu berücksichtigen sind.

Aber auch die technischen Möglichkeiten und Vorgänge werden vom größten Problem beeinflusst, dem Menschen.

Daher ist es unabdingbar, diese bisher horizontal betrachteten Schichten um vertikale Betrachtungen zu ergänzen.

Mensch und Betrieb

Der gesamte Betrieb dieser Systeme wird durch Menschen wahrgenommen. Menschen lassen sich nicht durch ein Software-Update oder einen Hardware-Tausch optimieren, es werden aber Verfahren benötigt, die auch prüfbar und messbar sind.

Der Betrieb der Systeme muß klar definiert und dokumentiert sein als Sollvorgabe für eine Prüfung.

Dieses trifft nicht nur für den Betrieb des SAP-Systems zu, sondern auch für den Betrieb des Betriebssystems, der Hardware, der Überwachung der Systeme, des Release-Managements (also Updates und Patches) und der Netzwerk-Systeme, da diese oft nicht alle in einer Hand oder Gruppe liegen.

Organisatorische Maßnahmen und Regelungen für die Administration auch auf den unteren Schichten müssen nachvollziehbar und prüfbar sein. Nur der Einsatz automatischer Mechanismen reicht nicht aus, sondern kann nur ein Hilfsmittel sein.

Know How als Prüfobjekt

Doch um all diese Themen auch im organisatorischen Bereich zu definieren und die sicherheitskritischen Aspekte zu berücksichtigen, muß bei den Betreibern das entsprechende Know-How vorausgesetzt werden. Know-How lässt sich in dem hier benötigten Umfang nicht nur durch "Learning-by-Doing" erreichen.

Skill, Skill-Planung, Skill-Aufbau und Know-How sind daher wichtige Bestandteile, um eine Gesamtbeurteilung der Sicherheit auch für dieses Prüfobjekt

Die Verwahrorte und Login-Daten sind leider immer noch oft schnell am Arbeitsplatz auffindbar.

der SAP-HR-Daten abgeben zu können. Denn nur, wenn man weiß, was man tut, kann man die entsprechende Qualität eines geforderten Sicherheitsstandards auch erreichen.

Und die Mitarbeiter ...

Und auch die Mitarbeiter, also die Anwender, sind Bestandteil der Gesamtsicherheit der HR-Daten. Dass natürlich die Verwendung von Passwörtern und Login-Daten sicher zu verwahren und anzuwenden sind, sollte jedem klar sein. Doch regelmäßige Kontrollen intern in Unternehmen haben gezeigt, dass es bei bis zu 15% der Arbeitsplätze möglich ist, in bis zu 5 Minuten sich am System mit den Kennungen des Mitarbeiters anzumelden.

Die Verwahrorte und Login-Daten sind leider immer noch oft schnell am Arbeitsplatz auffindbar.

Aber auch das sogenannte "Social-Hacking" nutzt einfach die Gutgläubigkeit des Menschen aus und man gelangt so in bis zu 60% der Fälle an die Login-Daten der Mitarbeiter.

Hier kann nur eine regelmäßige Mitarbeiter-Sensibilisierung greifen, die nicht nur für die Sicherheit der HR-Daten, wie in unserem Beispiel, greift, sondern zur Gesamt-Unternehmens-Sicherheit beiträgt.

Fazit

Für Revisionen im IT-Umfeld sind immer alle Schichten zu betrachten, auch wenn nur einzelne Objekte daraus der Prüfung unterzogen werden.

Es ist ein gewaltiger Unterschied, ob ein Prüfauftrag lautet

- "Prüfen des Berechtigungskonzeptes der SAP-HR-Daten" oder
- "Prüfen der Sicherheit der SAP-HR-Daten".




Beim zweiten Punkt befindet man sich zwangsläufig im gesamten Prozess-Ablauf, in dem es aus allen Schichten möglich ist, egal ob legal oder illegal, Zugriff auf sensible Daten zu bekommen.

Dabei ist es in diesem Falle nahezu unmöglich alle Schichten zu prüfen. Es sollten jedoch alle Schichten Berücksichtigung finden und erwähnt werden. ❖

 <p>Seminarcode: R3KT 12.10.-13.10.06</p> <p>Prüfung des Korrektur- und Transportwesens von SAP® Landschaften</p> <p>Inhalte u.a.: R/3®-Systemlandschaften</p> <ul style="list-style-type: none"> • Mögliche R/3®-Systemlandschaften • Test- und Freigabeverfahren <p>Transportwege</p> <ul style="list-style-type: none"> • Organisation und Schutz der Transportwege • Automatische und manuelle Transporte <p>Rollentrennung beim Transportprozess</p> <ul style="list-style-type: none"> • Entwicklung, Qualitätssicherung, Administration • Funktionstrennung <p>Das Transport Management System (TMS) Kontrolle der Importvorgänge</p> <p>Anmeldung und Auskünfte: <i>IBS</i> 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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: R3BW 12.10.-13.10.06</p> <p>Revisionsworkshop "Business Information Warehouse - BW" von SAP® Systemen</p> <p>Inhalte u.a.: Einführung</p> <ul style="list-style-type: none"> • Architektur von Data Warehouse Systemen • Einordnung in das Gesamtkonzept • Funktionalität SAP® BW <p>Datenbeschaffung prüfrelevanter Daten</p> <ul style="list-style-type: none"> • Stammdaten • Bewegungsdaten <p>Datenmodellierung und Datenaufbereitung</p> <p>Reporting und Analyse</p> <ul style="list-style-type: none"> • Erarbeitung von Musterlösungen <p>Sicherheitsrisiken BW</p> <ul style="list-style-type: none"> • Datenschutz • Datensicherheit • Berechtigungskonzeption <p>Anmeldung und Auskünfte: <i>IBS</i> 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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: R3HB 16.10.-17.10.06</p> <p>Workshop zur Berechtigungsprüfung des Moduls HR von SAP®</p> <p>Inhalte u.a.: Spezifikation der Berechtigungskonzeption für die Personalwirtschaft - HR</p> <ul style="list-style-type: none"> • Komplexität und Quantitäten • Verwendungsnachweis • Fehlerquellen - Fehleranalyse <p>Strukturelle Berechtigungen</p> <ul style="list-style-type: none"> • Konzeption - Einsatz • Prüfen kritischer Berechtigungen und kritischer Kombinationen <p>Prüfung und Dokumentation</p> <ul style="list-style-type: none"> • Abbildung der Prüfungstätigkeit • Auswertungsmöglichkeiten mit SAP® Standardreports und Tabellen <p>Anmeldung und Auskünfte: <i>IBS</i> 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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>
--	---	--

 <p>Seminarcode: R3BD 18.10.-20.10.06</p> <p>Gesamtsicherheit durch alle Schichten von SAP® Systemen</p> <p>Inhalte u.a.: Die Client/Server-Umgebung unter SAP®</p> <p>Die Protokollierung von NT/UNIX, Oracle und SAP®</p> <p>Beeinflussung der Ebenen untereinander (Schnittstellen) in hierarchischer Betrachtung</p> <ul style="list-style-type: none"> • WindowsNT/UNIX und SAP® • Sicherung der Client-Stationen <p>Risikomanagement und Sicherheitstrategien Checklisten und ihre praktische Umsetzung</p> <p>Anmeldung und Auskünfte: <i>IBS</i> 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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: R3WK 23.10.-25.10.06</p> <p>Werkzeugkasten für die Prüfung von SAP®</p> <p>Inhalte u.a.: Tipps und Tricks zu Tabellen und Reports</p> <p>Aufbau des Data Dictionary</p> <ul style="list-style-type: none"> • Domänen, Datenelemente, Felder • Analysen von Tabelleneigenschaften, Prüftabellen <p>Traces</p> <ul style="list-style-type: none"> • SQL-Trace - Finden von Tabellen • SAP® System-Trace - Analyse von Zugriffsberechtigungen <p>QuickViews</p> <p>ABAP-Programmierung</p> <ul style="list-style-type: none"> • Prüfeigene Programme mit ABAP • Analysen von ABAP-Programmen <p>Erstellen eigener Reportingbäume</p> <p>Anmeldung und Auskünfte: <i>IBS</i> 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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: R3GB 02.11.-03.11.06</p> <p>Revisionsführerschein für SAP® Systeme</p> <p>Inhalte u.a.: Einführung:</p> <ul style="list-style-type: none"> • SAP® Architektur/Leistung • Komponenten/Teilkomponenten <p>Die SAP®-Benutzeroberfläche</p> <ul style="list-style-type: none"> • Vergl. zum Windows-Standard • Matchcode und Modi <p>Transaktionscodes</p> <ul style="list-style-type: none"> • Aufrufen von Anwendungen • Historienliste <p>Individuelle Benutzereinstellungen</p> <ul style="list-style-type: none"> • Benutzerfestwerte • Das Benutzermenü <p>Reports</p> <ul style="list-style-type: none"> • Standardreports in den Modulen • Selektionskriterien <p>Anmeldung und Auskünfte: <i>IBS</i> 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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>
---	--	---

 <p>Seminarcode: BKEB 12.10.-13.10.06</p> <p>Electronic Banking aus Revisionsicht</p> <p>Inhalte u.a.:</p> <p>Techniken im eBanking</p> <p>HBCI - eBanking</p> <p>Kryptografische Verfahren beim Einsatz in Banken</p> <p>Funktion und Qualität von Zertifizierungsverkehr im Internet</p> <p>Internet als Kapitalmarkt</p> <p>Internet als Informationsmarkt</p> <p>Anmeldung und Auskünfte:</p> <p>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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: CDXR 23.10.-25.10.06</p> <p>EXCEL für Revisoren</p> <p>Inhalte u.a.:</p> <p>Handling von Tabellen, Blättern und Mappen</p> <p>Einlesen von Prüfdaten</p> <p>Selektionen / Stichprobennahmen</p> <p>Schichten von Datenbeständen (ABC-Analyse)</p> <p>Funktionen zur Aufbereitung und Analyse von Daten</p> <p>Formatierung und Darstellung</p> <p>Verknüpfen von EXCEL-Tabellen und vergleichende Auswertungen</p> <p>Automatisierungsmöglichkeiten von sich wiederholenden Prüfabfragen</p> <p>Individuelle Anpassung</p> <p>Anmeldung und Auskünfte:</p> <p>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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: GMSD 25.10.-27.10.06</p> <p>Prüfen des Vertriebs</p> <p>Inhalte u.a.:</p> <p>Einführung</p> <ul style="list-style-type: none"> Definition und Strategie von Marketing und Vertrieb Gesetzliche Randbedingungen und Vertragsbedingungen <p>Risiken im Vertriebsprozess und Prüfung der Risikosteuerung</p> <ul style="list-style-type: none"> Risikopotential und -ranking IT-Werkzeuge zur Prüfung von Umsätzen, Debitoren u.a.m. <p>Kommunikationsfluss</p> <ul style="list-style-type: none"> Richtlinien/Ethik-Werk für den Vertrieb Die Kundenakte <p>Fallbeispiele im Zusammenhang</p> <p>Anmeldung und Auskünfte:</p> <p>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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>
---	---	--

 <p>Seminarcode: DSW2 06.11.-08.11.06</p> <p>Windows® 2000 für Revisoren</p> <p>Inhalte u.a.:</p> <p>Aufbau und Struktur des Betriebssystems:</p> <ul style="list-style-type: none"> Leistungsmerkmale Eigenschaften der Serverversionen Kompatibilität <p>NTFS 5</p> <ul style="list-style-type: none"> Verschlüsselung Prüfungsansätze <p>Security</p> <ul style="list-style-type: none"> Anmeldesicherheit Restriktion für Benutzer <p>Berechtigungskonzept</p> <ul style="list-style-type: none"> Einführung in ADS Gruppen und deren Verschachtelung Freigaberechte contra NTFS-Rechte <p>Anmeldung und Auskünfte:</p> <p>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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: CDAR 06.11.-08.11.06</p> <p>ACCESS für Revisoren</p> <p>Inhalte u.a.:</p> <p>Arbeit mit Tabellen/Datenbanken</p> <p>Einlesen von Prüfdaten in ACCESS</p> <p>Erstellen von Feldstatistiken</p> <p>Schichten von Datenbeständen (ABC-Analyse)</p> <p>Analyse der extrahierten Daten</p> <p>Verknüpfen von ACCESS-Tabellen und vergleichbare Auswertungen</p> <p>SQL-Abfragen</p> <p>Zusammenfassung am Beispiel einer kompletten interaktiven Prüfung von Datenbeständen inkl. grafischer Auswertung</p> <p>Automatisierungsmöglichkeiten von sich wiederholenden Prüfabfragen</p> <p>Anmeldung und Auskünfte:</p> <p>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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>	 <p>Seminarcode: GMEI 08.11.-10.11.06</p> <p>Prüfen des Einkaufs</p> <p>Inhalte u.a.:</p> <p>Einführung</p> <ul style="list-style-type: none"> Gefährdungspotenzial des Einkaufs Der Prozess des Einkaufs <p>Risiken im Beschaffungsprozess und Risikosteuerung</p> <ul style="list-style-type: none"> Risikopotential + -ranking Risiko-Steuerungsmaßnahmen <p>Kommunikationsfluss</p> <ul style="list-style-type: none"> Richtlinien/Verfahrensweisungen für den Einkauf Der Kommunikationsweg von der Anforderung bis zur Lieferung und Abnahme und Rückkopplung <p>Fallbeispiele im Zusammenhang</p> <p>Anmeldung und Auskünfte:</p> <p>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</p> <p>www.ibs-hamburg.com seminare@ibs-hamburg.com</p>
---	---	--

Prof. Dr. Ulli Guckelsberger und Prof. Dr. Stefan Kronberger

Grundzüge der Volkswirtschaftslehre Lehr- und Übungsbuch

4. aktualisierte Auflage 2006
Kiehl Verlag,
428 S., ISBN 3 470 47854 6
24,80 €

Dieses Lehr- und Übungsbuch bereitet den Stoff der Volkswirtschaftslehre speziell für Studenten an Berufsakademien, Fachhochschulen und Universitäten mit betriebswirtschaftlicher Ausrichtung auf. Es vermittelt grundlegende Einsichten in volkswirtschaftliche Tatbestände und Zusammenhänge. Ziel ist es dabei, das volkswirtschaftliche Verständnis der Betriebswirte als Grundlage unternehmerischen Denkens zu schärfen.

Das Buch basiert in weiten Teilen auf Vorlesungen, die die Autoren an der Fachhochschule Ludwigs-hafen anbieten und deckt die traditionelle Mikro- und Makroökonomie ab. Ergänzt wird die Darstellung durch ein Kapitel zur Dogmengeschichte.

Die 4. Auflage wurde gründlich überarbeitet und der Übungsteil erweitert.

Aus dem Inhalt:

Volkswirtschaftliche Grundbegriffe, Wirtschaftsordnung, Volkswirtschaftliche Gesamtrechnung, Zahlungsbilanz, Neoklassische Unternehmens- und Haushaltstheorie, Preistheorie, Wettbewerbstheorie, Makroökonomische Ansätze, Außenwirtschaft, Grundzüge der Dogmengeschichte, Übungsteil, Lösungen.

Hans-Dietrich Koch u.a.

Der betriebliche Datenschutz- **beauftragte**

Aufgaben - Voraussetzungen - Anforderungen

6. vollständig überarbeitete und erweiterte Aufl. 2006
Datakontext-Fachverlag,
552 S., ISBN 3-89577-364-6
49,00 €

Die 6. überarbeitete Auflage berücksichtigt die Veränderungen im Datenschutzrecht (so z. B. Strei-

chung des TDSV und Erweiterung des TDDSG), sowie inzwischen erschienene Kommentierungen und Rechtsprechung.

Grundlegend erweitert wurden z. B. die Kapitel Beschreibung der Vorabkontrolle, die Datenübermittlung im Ausland und die Anwendung der DV-Programme, die Schulungsverpflichtung des Datenschutzbeauftragten und die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG. Neu hinzugekommen ist ein Kapitel über die Zusammenarbeit zwischen DSB und Revision. Auch die umfangreichen Arbeitshilfen in den Anlagen wurden überarbeitet, aktualisiert und erweitert.

Neben der thematisch umfassenden Beschreibung der Aufgaben, Voraussetzungen und der Anforderungen erfolgt auch die inhaltliche Aufbereitung datenschutzrechtlicher Zusammenhänge für Anwender/innen, die auf der Grundlage des BDSG gesetzliche Datenschutzbestimmungen in die Organisation der "verantwortlichen Stelle" umsetzen sollen. Die übersichtliche und verständliche Abhandlung dieser komplizierten Materie, die in Verbindung mit vielfältigen Arbeitshilfen und Materialien eine bis ins Detail führende Ausarbeitung des Themas darstellt, wurde in der 6. Auflage vor dem Hintergrund des geltenden Datenschutzrechts sowie der neueren Rechtsprechung vollständig überarbeitet und erweitert.

Langjährig tätige betriebliche Datenschutzbeauftragte beschreiben bewährte Vorgehensweisen zur praxisnahen Umsetzung der gesetzlichen Erfordernisse für die betriebliche Datenverarbeitung in ein unternehmensbezogenes Datenschutz- und Sicherheitsmanagement. Dabei muss erwähnt werden, dass die Kenntnisse der Autoren auch aus unterschiedlich geprägten Tätigkeitsbereichen stammen, nämlich aus Produktion und Vertrieb, Datenverarbeitungsorganisation und Programmierung, Revision, Rechtsabteilung und Betriebsrat, jeweils in verantwortlicher Funktion. Ihre praktische Erfahrung als Datenschutzbeauftragte wurde sowohl in haupt- bzw. nebenamtlicher Tätigkeit erworben.

Sowohl dem am Beginn seiner Tätigkeit stehenden Datenschutzbeauftragten als auch "mitten im Berufsleben" stehenden Datenschutzpraktikern wird beispielhaft und überschaubar eine praxisbezogene Zusammenfassung gesetzlicher und betriebsorgani-

satorischer Erfordernisse sowie bewährte Vorgehensweisen zur Realisierung des Datenschutzes an die Hand gegeben. Einschlägige technische und organisatorische Maßnahmen zur Abwendung von Gefährdungen der Datenverarbeitung, die in ihrer Gesamtheit den Datenschutz in verantwortlichen Stellen ausmachen, sind auch auf Details eingehend und verständlich - "von der Praxis für die Praxis" - abgehandelt.

Nicht die Kommentierung des Bundesdatenschutzgesetzes, sondern die praxisnahe Ergänzung vorhandener Literatur, ist charakteristisch für das gelungene Werk. Die Fülle von Verweisen auf einschlägige Literatur und Kommentierungen ermöglichen es dem Leser, auf vertiefende Lektüre zu den Themen zurückzugreifen. Dieses Fachbuch wurde ursprünglich für betriebliche Datenschutzbeauftragte entwickelt. Da die Aufgaben der Datenschutzbeauftragten in nicht öffentlichen und öffentlichen Stellen vielfach deckungsgleich sind, eignet sich dieses Werk sowohl für privat-wirtschaftliche wie auch für öffentliche Stellen.

Das Buch ist ein Ratgeber für Datenschutzbeauftragte, Unternehmensleiter und Leiter von Behörden, für Personalchefs und Betriebs-/Personalräte. Es ermöglicht einen umfassenden Überblick über das Berufs- und Funktionsbild von Datenschutzbeauftragten und auch über technische und organisatorische Erfordernisse des Datenschutzes bei verantwortlichen Stellen. Das Werk präsentiert sich als praktisches Handbuch für den Datenschutz bei datenverarbeitenden Stellen. In den bisherigen Auflagen hat es sich als "Klassiker" in der Praxis bewährt.

Peter Gola

Datenschutz im Callcenter

2. überarb. und erweiterte Auflage 2006

Datakontext-Fachverlag,

184 S., ISBN 3-89577-411-1

29,00 €

Was Call Center und deren Auftraggeber aus Wirtschaft und Verwaltung datenschutzrechtlich zu beachten haben, wie Datenschutz effektiv umgesetzt und praktiziert werden kann, hierüber informiert die

zweite überarbeitete Auflage des Ratgebers von Peter Gola. Aufgezeigt werden die bei den Tätigkeiten von Call Centern bestehenden Datenschutzprobleme und die in der Praxis oftmals festzustellenden Defizite beim Umgang mit personenbezogenen Daten sowohl der Kunden als auch der Beschäftigten der Call Center.

Ausführlich behandelt werden die Problemfelder:

- Heimliches Mithören
- Aufzeichnen von Gesprächen
- Telemarketing
- Erfassung der Kommunikationsdaten
- Testanrufe (Mystery Calls)
- Grenzen der Kommunikationskontrolle
- Kundendatenschutz
- Call Center Outsourcing
- Mitbestimmung

Daneben geht das Fachbuch auf die sich aus dem BDSG ergebenden organisatorischen Anforderungen an Call Center ein. Das ausführliche Stichwortregister und Literaturverzeichnis sowie die verständliche Sprache des erfahrenen Autors erleichtern den Umgang mit diesem für Call Center überlebenswichtigen Thema.

Dietmar Franke

Vertrauensvolle Zusammenarbeit mit dem Betriebsrat

2. überarbeitete Auflage 2006

Datakontext-Fachverlag,

208 S., ISBN 3-89577-399-9

36,00 €

Im Frühjahr 2006 werden die Betriebsräte neu gewählt. Gleichviel, ob dabei personell "alles beim alten" bleibt oder neue Mitglieder in die Gremien einziehen, in beiden Fällen bietet sich den Betriebspartnern eine Chance, die nur alle vier Jahre wiederkehrt. Die Chance nämlich, gewachsene Vorurteile, gegenseitiges Misstrauen oder gar offene Konfrontation in die Vergangenheit zu verweisen und die Zusammenarbeit auf eine Grundlage zu stellen, wie sie das Betriebsverfassungsgesetz in § 2 I vorgibt. Danach arbeiten Arbeitgeber und Betriebsrat vertrauensvoll zum Wohl der Arbeitnehmer und des Betriebs zusammen. Das ist weder frommer

Wunsch noch unverbindlicher Appell sondern verpflichtendes Gebot.

Wie es in die Praxis umgesetzt werden kann, zeigt die 2. Auflage des Buches "Vertrauensvolle Zusammenarbeit mit dem Betriebsrat". Die Neuauflage zeigt konkrete Handlungsanleitungen auf, die sowohl dem Arbeitgeber als auch dem Betriebsrat als Richtschnur dienen, eingefahrene Gleise zu verlassen und rigide Rechtspositionen im Interesse der Arbeitnehmer und des Betriebs zu "entschärfen".

Die Notwendigkeit hierzu beweisen gerade neueste Entscheidungen des Bundesarbeitsgerichts, die in der Voraufgabe noch nicht berücksichtigt werden konnten. Damit die in dem Buch ausgesprochenen Empfehlungen zwischen den Betriebspartnern verbindlichen Charakter annehmen, werden diese abschließend in einer als Textmuster angelegten Betriebsvereinbarung verankert. Denn so wie jede Organisation sich eine Verfassung oder Satzung gibt, sollte auch ein Betrieb die Grundsätze der Zusammenarbeit zwischen seinen Repräsentanten in einem "betrieblichen Grundgesetz" schriftlich regeln.

Fragen

1. Welche mitbestimmungspflichtigen Angelegenheiten sind in den letzten vier Jahren unerledigt geblieben oder "im Sand verlaufen" - und warum?
2. Wie oft und aus welchem Anlass haben Sie die Einigungsstelle bzw. das Arbeitsgericht angerufen?
3. Sehen Sie für die kommende Amtszeit des Betriebsrats Verbesserungspotenziale in der Zusammenarbeit?
4. Beabsichtigen Sie nach der Wahl auf den Betriebsrat zuzugehen, um auf Verbesserungen in der Zusammenarbeit hinzuwirken?
5. Halten Sie es für erforderlich, den Betriebsrat auch in solche Maßnahmen einzubinden, für die das Gesetz kein Beteiligungsrecht vorsieht?
6. Sollten am besten solche Mitarbeiter in den Betriebsrat gewählt werden, auf die wegen Sitzungen, Schulungen etc. am ehesten am Arbeitsplatz verzichtet werden kann?
7. Halten Sie es für angebracht, mit dem Betriebsrat für Schulungen etc. ein Jahresbudget zu vereinbaren?

8. Binden Sie den Betriebsrat von sich aus ein oder lassen Sie ihn auf sich zukommen?

Hrsg. Deutsches Institut für Interne Revision e.V.

Revision des Finanzwesens

3. völlig neu bearbeitete und wesentlich erweiterte Auflage 2006, Erich Schmidt Verlag, 100 S., ISBN 3 503 05969 5
22,80 €

Das Finanzwesen ist ein wichtiger Bereich in jedem Unternehmen, mit Aufgaben die immer komplexer und dynamischer werden. Die Integration der Finanz- und Kapitalmärkte verstärkt sich, grenzüberschreitende Kapitalanlagen bzw. -aufnahmen gewinnen an Bedeutung, innovative Finanzierungsformen entstehen. Die effektive und zukunftsweisende Überwachung des Finanzwesens stellt die Verantwortlichen täglich vor eine schwierige Aufgabe. Für die Arbeit der Internen Revision eröffnet sich damit ein ebenso wichtiges wie anspruchsvolles Prüfungsgebiet. Denn es sind gerade Mängel im Finanzwesen, die vielfach zu Schief lagen von Unternehmen führen. Das neue Buch des Arbeitskreises "Revision des Finanz- und Rechnungswesens" vom renommierten Deutschen Institut für Interne Revision (IIR) zeigt anschaulich, wie die Prüfung des Finanzwesens erfolgreich zu bewältigen ist. Die nunmehr bereits dritte Auflage berücksichtigt die zentralen aktuellen organisatorischen, rechtlichen und technischen Entwicklungen der letzten Jahre.

Das Buch vermittelt, wie

- Maßnahmen der Mittelbeschaffung und -rückzahlung
- Gestaltungen der Zahlungs-, Informations-, Kontroll- sowie
- Sicherheitsbeziehungen zwischen Unternehmen und Kapitalgebern

unter den Gesichtspunkten der Sicherheit, Ordnungsmäßigkeit und Wirtschaftlichkeit auf allen Ebenen wirkungsvoll und zukunftsgerichtet zu prüfen sind.

Dabei führt der Leitfaden mit kommentierten Prüfungsfragen sowie der Darstellung wichtiger Inhalte, Verantwortlichkeiten und essentieller Aufgaben systematisch durch die schwierige Prüfungsarbeit.

Ronald Gleich und Karsten Oehler

Corporate Governance umsetzen

Auflage 2006, Schäffer-Poeschel Verlag,
300 S., ISBN 3-7910-2276-8
59,95 €

Eine Reihe von Unternehmenskrisen hat das Vertrauen des Kapitalmarkts, von Stakeholdern, sowie Shareholdern erschüttert und die Diskussion über Corporate Governance intensiviert. Regulatorische Maßnahmen wie z. B. der Sarbanes-Oxley-Act, die neuen Eigenkapitalregelungen durch Basel II oder der Deutsche Corporate Governance Kodex sollen das Corporate Governance-System transparent sowie nachvollziehbar gestalten und das Vertrauen in die Leitung und Überwachung börsennotierter Unternehmen wieder herstellen. Diese Maßnahmen haben weitreichende Auswirkungen auf alle Unternehmensbereiche. Vor diesem Hintergrund ist es die Zielsetzung dieses anwendungsorientierten Werkes, die zentrale Bedeutung des Controlling im Aufbau neuer corporate governance-orientierter Managementstrukturen aufzuzeigen. Die Kernthemen befassen sich dabei mit dem Risikomanagement als unverzichtbarem Teil des Performance Measurement Systems, dem Aufbau eines internen Sicherungssystems, der Fundierung der Planung und des Forecasting, dem Einsatz fundierter IT-Werkzeuge sowie der notwendigen Zusammenarbeit zwischen Controlling und Interner Revision. Umsetzungs- und Anwendungsempfehlungen sowie Fallbeispiele und Erfahrungsberichte aus der Praxis unterstützen den Anwendungsbezug. Damit bietet dieses Werk Hilfestellung bei der effizienten Anpassung bzw. beim Aufbau der Geschäftsprozesse und IT-Systeme an corporate governance-orientierte Managementstrukturen.

Norbert Pfitzer / Peter Oser / Christian Orth

Reform des Aktien-, Bilanz- und Aufsichtsrechts

2., aktualisierte und erweiterte Auflage 2006,
Schäffer-Poeschel Verlag,
297 S., ISBN 3-7910-2498-1
39,95 €

Die deutsche Rechnungslegungspraxis ist in den letzten Jahren mit einer Vielzahl von Reformgesetzen

Hintergrund der Vielzahl neuer Gesetze und Gesetzesvorhaben ist zum einen die Zielsetzung des Gesetzgebers, durch die Schaffung von Rahmenbedingungen den Finanzplatz Deutschland zu stärken...

konfrontiert worden, die zu tiefgreifenden Veränderungen in der Bilanzierungs- und Prüfungspraxis geführt haben. Hintergrund der Vielzahl neuer Gesetze und Gesetzesvorhaben ist zum einen die Zielsetzung des Gesetzgebers, durch die Schaffung von Rahmenbedingungen den Finanzplatz Deutschland zu stärken. Darüber hinaus ist die nationale Gesetzesgebung zunehmend durch internationale Einflüsse sowie europäische Vorgaben geprägt.

Dieses Werk befasst sich mit den verabschiedeten und geplanten Reformgesetzen, zu denen z. B. das Bilanzrechtsformgesetz (BilReG), das Bilanzkontrollgesetz (BilKoG), das Abschlussprüferaufsichtsgesetz (APAG), das Anlegerschutzverbesserungsgesetz (AnSVG) und das Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts (UMAG) gehören.

In der 2. Auflage erfolgte eine Überarbeitung des Werkes und die Aufnahme der zwischenzeitlich neu erlassenen Gesetze wie beispielsweise das Kapitalanleger-Musterverfahrensgesetz (KapMuG), das Vorstandsvergütungs-Offenlegungsgesetz (VorstOG) und das Wertpapier-Prospektgesetz (WpPG). Ferner fanden die EU-Transparenzrichtlinie und die 8. EU-Richtlinie sowie die sich daraus ergebenden Umsetzungserfordernisse für das deutsche Recht Berücksichtigung.

Zielsetzung ist es, einen Überblick über die aktuelle internationale und nationale Rechtsentwicklung im Aktien-, Bilanz- und Aufsichtsrecht zu geben. Darüber hinaus werden die mit den Gesetzen verbundenen offenen Anwendungs- und Auslegungsfragen aufgezeigt und Umsetzungshilfen sowie -empfehlungen erteilt. Damit wird es Entscheidungsträgern ermöglicht, eine normkonforme Umsetzung der gesetzlichen Anforderungen vorzunehmen und die erforderlichen unternehmerischen Maßnahmen zu ergreifen. ❖

ABO-Bestellung für PRev

Ein Abo von *Revisionspraxis* beinhaltet folgende Verlagssdienstleistungen:

- Zusendung von *PRev*
- IBS-Prüfmanual (Beilage in PRev I-III)
- Jahrbuch Interne Revision (Beilage in PRev IV)
- 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: _____