➲ Liebe Leserinnen und Leser,

das Aufgabenfeld der Internen Revision erweitert sich ständig: das "Zusammenspiel" mit Vorstand und geprüften Fachbereichen als direkten "Kunden", und weiterhin mit bDSB, WP, Audit Commitee und nicht zuletzt innerhalb der IR selber. In diesem volatilen Umfeld will **ReVision** Motor in der permanenten Weiterentwicklung pragmatischer Ansätze zur Beförderung effizienter und effektiver Revision sein:

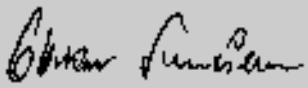
- So wird ab dieser Ausgabe I/05 das komplexe und risikobehaftete Prüffeld "SAP®" als gesondertes **Supplement für SAP®-Revisoren** in **ReVision** dauerhaft integriert.
- Des Weiteren wird jeder Ausgabe von ReVision ein IBS-Prüfmanual beigelegt, gesponsert von der IBS Schreiber GmbH. In diesen IBS-Prüfmanuals werden knapp auf jeweils 20 bis 30 Seiten im Sinne eines risiko-orientierten Prüfungsansatzes die Komplexität (Prozesse) und die daraus folgenden Risiken und signifikanten Soll-Vorgaben zum jeweiligen Prüffeld zusammengestellt, beginnend mit **Baurevision** in dieser Ausgabe. **ReVision** II/05 wird das IBS-Prüfmanual **Projektrevision** enthalten.

Die Beiträge in dieser Ausgabe fokussieren auf die Professionalisierung der IR, in der Bewertung von Ausbildungen zum CISA u.a. und in der Diskussion der mit höchster Priorität einzuhaltenden Soll-Vorgaben, gegen die zu prüfen ist, nämlich der Einhaltung von Gesetzen:

- Die IR und der bDSB (BDSG)
- Ordnungsmäßigkeit der Buchführung mit IT-Unterstützung (GoB, GoBS, FAIT 1)
- Soll-Vorgaben und Probleme der digitalen Dokumentation und Archivierung (GDPdU, AO, HGB)

Viel Erfolg bei der Professionalisierung Ihrer Prüftätigkeit wünscht Ihnen

Ihr



Ottokar R. Schreiber

Revision | IT-Revision | Archivierung

Supplement für SAP R/3® Revisoren Seite I-XII

Beilage: IBS-Prüfmanual "Baurevision"

Impressum

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

Herausgeber: Ottokar R. Schreiber

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

Beiträge

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

eMail: redaktion@osv-hamburg.de

Anzeigen

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

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

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

DTP-Produktion

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

Druck: Druckerei Zollenspieker Kollektiv GmbH
Zollenspieker Hauptdeich 54
21037 Hamburg

Printed in Germany. • Gedruckt auf chlorfrei gebleichtem Papier

Allgemein

Verlagshinweis

Nächste Ausgabe der
ReVision
Mai 2004

Redaktions-/ Einsendeschluss für diese Ausgabe: 15.04.2005

➲ Professionalisierung in der Internen Revision: Kompetenzkontinuität durch Zertifizierungen

Dipl.-Betriebswirt
Christoph Wildensee
Stadtwerke Hannover AG

Einführung

Professionalisierung und Mitarbeiterqualifizierung sind bereits seit einigen Jahren "Dauerbrenner" in der Internen Revision. Der Anspruch einer kontinuierlichen Qualitätssteigerung revisorischer Leistungserbringung im Kontext unternehmensinterner Kostensenkungsprogramme und externer Konkurrenz hat zu Recht dazu geführt, dass u.a.

- die Interne Revision die Prüfungsplanung risikoorientiert durchführt,
- die Interne Revision Anlehnung an Standards findet, im Planungs- und Prüfungsprozess adäquat dokumentiert und somit Transparenz entsteht,
- Revisoren stetig ihr Know-how-Profil bedarfsgerecht erweitern.

Insbesondere der letzte Punkt stellt sowohl die Mitarbeiterbeschaffung als auch die Personalförderung vor eine Herausforderung. Welche Qualifikation muss ein Bewerber - neben persönlich-sozialer Kompetenz - mitbringen, um im Arbeitsalltag hochwertige Ergebnisse in der Internen Revision zu produzieren? Wie kann sichergestellt werden, dass der Revisor auch nach Jahren eine ansprechende Arbeitsqualität liefert? Was kann das Unternehmen zur Mitarbeitermotivation beitragen ohne ihn dabei zu überfordern? Neben den meist mehrtägigen Seminarbesuchen ohne Leistungsnachweis, bei denen die Inhalte über einen längeren Zeitraum oft nur unzureichend zugänglich bleiben, stellen externe Qualifizierungsprogramme mit Zertifizierung und Weiterbildungsnachweispflicht (continuing education policy) einen hohen Standard zur Verfügung, der eine kontinuierliche intensive Erarbeitung hochkomprimierten Lernstoffes bedeutet.

Neben den meist mehrtägigen Seminarbesuchen ohne Leistungsnachweis, bei denen die Inhalte über einen längeren Zeitraum oft nur unzureichend zugänglich bleiben, stellen externe Qualifizierungsprogramme mit Zertifizierung und Weiterbildungsnachweispflicht (continuing education policy) einen hohen Standard zur Verfügung, der eine kontinuierliche intensive Erarbeitung hochkomprimierten Lernstoffes bedeutet.

Funktionszertifizierungen beziehen sich auf Produkte am Markt (Hard- und Software) und notwendige Aktivitäten rund um deren Funktionsumfang (Installation, Administration, Wartung etc.)

Der nachfolgende Artikel soll beispielhaft wichtige Zertifizierungen für IV-Revisoren darstellen. Er erhebt keinen Anspruch auf Vollständigkeit, zeigt jedoch Möglichkeiten zur Qualitätssteigerung auf.

Unterschiedliche Zertifizierungsformen

Die Unterscheidung zwischen Berufs- und Funktionszertifizierung kann sehr leicht getroffen werden. Eine Berufszertifizierung schließt mit einem Zertifikat eines Berufsverbandes oder einer Interessenvertretung als praxisnah-anerkannte Institution ab und vermittelt üblicherweise Methodenkompetenz. Die jeweilige Einrichtung definiert selbst oder orientiert sich an Best-Practice-Standards - so z.B. die IIA/IIR, die ISACA oder andere (weltweite Dach-)Organisationen. Entscheidend ist hier der Nachweis, dass der Absolvent die grundlegenden Rahmenbedingungen und Methodengrundlagen für das Aufgabenfeld erlernt hat und adäquat anwenden kann.

Funktionszertifizierungen beziehen sich auf Produkte am Markt (Hard- und Software) und notwendige Aktivitäten rund um deren Funktionsumfang (Installation, Administration, Wartung etc.). Sie sind durch die Produktnähe "techniklastig" und schließen beim Hersteller oder meist bei einem Trainingspartnerunternehmen mit einer Prüfung zu einem definierten Releasestand ab.

Revisoren, die zuvor in der operativen Linie Funktionen ausübten, haben häufig bereits produktbezogene Weiterbildungen absolviert und kennen daher den berufsbegleitenden Lernprozess. Funktionszertifizierungen werden meist abgestuft in den großen Unternehmensanwendungssystemen absolviert

Revisoren, die zuvor in der operativen Linie Funktionen ausübten, haben häufig bereits produktbezogene Weiterbildungen absolviert und kennen daher den berufsbegleitenden Lernprozess. Funktionszertifizierungen werden meist abgestuft in den großen Unternehmensanwendungssystemen absolviert - beispielsweise Microsoft-, CISCO- oder Oracle-Zertifikate zur Server-, Traffic-, Datenbankadministration oder (Anwendungs-) Entwicklung. Aber auch "exotische" Anwendungen wie z.B. Datenretrievalsysteme oder Bildmanipulationssoftware können eine eigene Zertifizierungsreihe aufweisen. Solche Qualifizierungsprogramme bestehen somit üblicherweise bei Produkten, die einen hohen Komplexitätsgrad aufweisen. Da die Produkte einen bestimmenden Standard am Markt bilden, sind die Zertifikate hochwertig und international anerkannt, sofern man das Wissen regelmäßig bei Release- / Technologiewechsel über Delta-Schulungen aktualisiert.

Da die Produkte einen bestimmenden Standard am Markt bilden, sind die Zertifikate hochwertig und international anerkannt, sofern man das Wissen regelmäßig bei Release- / Technologiewechsel über Delta-Schulungen aktualisiert.

Zertifizierungsprogramme

Die nachfolgenden Zertifizierungsprogramme sollen als Anregung dienen und einen kurzen Überblick über die Voraussetzungen, Inhalte und Rahmenbedingungen geben. Intensive Zertifizierungsprogramme mit hohem persönlichem Zeitaufwand und Praxisbezug sind als sinnvolle Option mit Nachhaltigkeitsgarantie zu sehen. Folgende Programme sind für die IV-Revision interessant:

Zertifizierungsprogramm, Inhalte	Anbieter, Voraussetzungen, Prüfung
Certified Internal Auditor (CIA) - IIA/IIR Methodenkompetenz allgemeine Revision, wird in Deutschland über die Präsenzveranstaltungen des IIR abgedeckt, ansonsten Literaturstudium, vier Prüfungsteile, die sich auf folgende Inhalte beziehen: · • Rolle und Aufgaben der Internen Revision, die Revisionsfunktion bezüglich Führung, Risiko und Kontrolle • Durchführung einer IR-Prüfung • Geschäftsanalyse und IT • Unternehmens-(Geschäfts-)führungskompetenz WP, vBP, CPA, CISA können sich für den letztgenannte Teil auf Antrag befreien lassenDieses Programm gilt anerkannt als eine hochwertige Hauptsäule der Revisorenqualifizierung.	Berufszertifikat allgemein, Interner Revisor Deutsches Institut für Interne Revision (IIR), Frankfurt am Main, **www.iir-ev.de**; The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201, USA, **www.theiia.org**. Kosten: individuell, kursabh., ca. 3.000,-- EUR, Voraussetzung zur Neuzulassung als CIA: - Universitäts- oder Fachhochschulabschluss und mindestens 2 Jahre Berufserfahrung im Bereich Revision (WP, Beratung, QS, Controlling u.ä.) - Sonderregelung im Bereich der Ausbildung mit zusätzlicher Berufserfahrung möglich - Erfolgreiches Absolvieren des Examens (>= 80 %) - 4 x 125 Fragen in jeweils 3,5-stündigen Prüfungen - Berufserfahrung kann nach der Prüfung nachgeholt werden - Anerkennung/Einhaltung des IIA-Ehrenkodex - Bestätigung der charakterliche Eignung durch Vorgesetzten, Hochschullehrer, anderen CIA Leitfäden u. Vorbereitungsbücher sind vorhanden Regelmäßige Weiterbildung (80 Std innerhalb von 2 Jahren) Prüfungen: 3. Woche in Mai und November, Frankfurt/Main
Certified Information Systems Auditor (CISA) - ISACA Methodenkompetenz IV-Revision Seminare je Prüfungsteil und Literaturstudium,Prüfungsgebiete: · IS-Prüfungsprozess · IS-Management, Planung und Organisation · Technische Infrastruktur und Betriebspraktiken · Schutz von Informationswerten · Fehlerbehebung nach Störungen, Betriebskontinuität · Anwendungskonzeption, Erwerb, Inbetriebnahme, Instandhaltung · Beurteilung von Betriebsabläufen und Risikomanagement Teilprüfungssubstitutions- und Verzichtsmöglichkeiten bei Vorliegen bestimmter Abschlüsse (z.B. CIA, CPA, FH- oder Universitätsstudium)Die Programme der ISACA gelten anerkannt als hochwertige Hauptsäule der Revisorenqualifizierung und werden von Unternehmensberatungen bei der Nachwuchsförderung favorisiert.	Berufszertifikat, IV-Revisior Information Systems Audit and Control Association (ISACA), Rolling Meadows, Illinois 60008, USA, **www.isaca.org**, Berufsverband der EDV-Revisoren ISACA German Chapter, Dinslaken, **www.isaca.de**. Kosten: individuell, kursabh., ca. 3.000,-- EUR++, Voraussetzung zur Neuzulassung als CISA: Ø Mindestens 5 Jahre Berufserfahrung in den letzten 10 Jahren auf dem Gebiet der IS-Prüfung, -Steuerung und -Sicherheit Ø Erfolgreiches Absolvieren des Examens (>= 75 Punktwerte) Ø Beantworten von 200 Fragen in einer 4-stündigen Prüfung Ø Berufserfahrung kann nach der Prüfung nachgeholt werden Ø Anerkennung/Einhaltung des ISACA-Ehrenkodex Regelmäßige Weiterbildung (20 Std/Jahr und 120 Std/3Jahre) Weitere Information: **www.isaca.org/cisaexam** Leitfäden u. Vorbereitungsbücher sind vorhandenPrüfung erfolgt im Juni jedes JahresPrüfungsorte in Deutschland: B, M, D, F, HH

Certified Information Security Manager (CISM) - ISACA Methodenkompetenz IT-SicherheitsmanagementSeminare je Prüfungsteil und Literaturstudium,Prüfungsgebiete: • Information Security Governance • Risk-Management • Information Security Program(me) Management • Information Security Management · Response ManagementSubstitutionsmöglichkeiten bei Vorliegen bestimmter Abschlüsse, z.B. für CISA, CISSP, MCSE, FH- oder Universitätsstudium. Wie zuvor, aber besonders auch für praxisnahe Ausbildung im Bereich der IT-Sicherheit als Alternative zu sehen.	Berufszertifikat, IT-SicherheitsmanagerInformation Systems Audit and Control Association (ISACA), Rolling Meadows, Illinois 60008, USA, www.isaca.org, Berufsverband der EDV-Revisoren ISACA German Chapter, Dinslaken, www.isaca.de.Kosten: individuell, kursabh., ca. 3.000,-- EUR++,Voraussetzung zur Neuzulassung als CISM:Ømindestens 5 Jahre Berufserfahrung im Bereich Information Security, 3 Jahre davon als Information Security ManagerØ Erfolgreiches Absolvieren des Examens (>= 75 Punktwerte)Ø Beantworten von 200 Fragen in einer 4-stündigen PrüfungØ Anerkennung/Einhaltung des ISACA-EhrenkodexRegelmäßige Weiterbildung (20 Std/Jahr und 120 Std/3Jahre)Weitere Information: www.isaca.org/cismexamLeitfäden u. Vorbereitungsbücher sind vorhanden Prüfung erfolgt im Juni eines JahresPrüfungsorte in Deutschland: B, M, D, F, HH
Certified Information Forensics Investigator (CIFI) - IISFA Methodenkompetenz im Bereich der forensischen Informatik, IT-Systemverhaltensanalyse etc., Prüfungsgebiete: • Auditing • Incident Response • Law and Investigation • Tools and Techniques • Traceback • Countermeasures Sehr praxisnah und in Teilen stark techniklastig, sie wird sicherlich in den nächsten Jahren an Bedeutung gewinnen, wenn es zu Partnerschaften zu Seminaranbietern kommt.	Berufszertifikat, Forensische Informatik International Information Systems Forensics Association (IISFA), 300 Satellite Bld., Suwanee, Georgia 30024, USA, **www.iisfa.org**. Kosten: individuell, kursabh., ca. 4.500,-- USD (+ Auslandsaufenthalt) Bisher ist diese Ausbildung nur in den USA zu absolvieren, dabei ist sie sehr praxisnah, bisher stehen in Deutschland keine Ausbildungsseminare zur Verfügung, Inhalte werden per Fernstudium erarbeitet, die Prüfung muss (noch) in den USA abgelegt werden, Trainingspartnerunternehmen werden aber gesucht, inhaltlich orientiert sich die Prüfung an den Standards der CISSP-, CISA / CISM-Ausbildung, jedoch verstärkt mit Fokus auf Computer-Crime / Investigation / Malware etc., engl. Literatur steht umfangreich zur Verfügung, aber wenig deutsche vorhanden, Voraussetzung zur Neuzulassung als CIFI: - Mindestens 5 Jahre Berufserfahrung im Bereich Informationstechnologie und nachweislich 5 Jahre in forensischer Informatik/Computeranalyse o.ä. - Erfolgreiches Absolvieren des Examens (>= 75%) - Beantworten von 200 Fragen in einer 4-stündigen Prüfung - Anerkennung/Einhaltung des IISFA-Ehrenkodex Leitfäden u. Vorbereitungsbücher sind bisher fast ausschließlich in englischer Sprache vorhanden

Certified Information Systems Security Professional (CISSP) - ISC² Methodenkompetenz IT-Security, eine der hochwertigsten und umfangreichsten Ausbildungen weltweit.Prüfungsgebiete: · Access Control Systems & Methodology · Appl. & Systems Development · Business Continuity Planning · Cryptography · Law, Investigation & Ethics · Operations Security · Physical Security · Security Architecture & Models · Security Management Practices · Telecommunications, Network & Internet Security Diese Ausbildung gilt bereits heute als eine der tragenden Säulen im IT-Sicherheitsbereich. Für IV-Revisoren ist sie wahrscheinlich zu umfangreich, bei Personalakquisition ist sie aber ein erheblicher Bonus/Benefit.	Berufszertifikat, IT-Sicherheitsmanager/SecurityInternational Information Systems Security Certification Consortium (ISC)2, Europe Operations, Golden Cross House, 8 Duncannon Street, Strand, London WC2N 4JF, UK, **www.isc2.org**. Kosten: individuell, ca. 3.500,-- EUR++Voraussetzung zur Neuzulassung als CISSP: - mindestens 4 Jahre Berufserfahrung im Bereich Information Security in einem oder mehreren der 10 Prüfungsgebiete oder 3 Jahre analoge Berufserfahrung und ein BA / BBA / BSc-Grad (Fachhochschuldiplom) oder 2 Jahre analoge Berufserfahrung und ein Master-Grad (Universitätsdiplom - Erfolgreiches Absolvieren des Examens (>=70%) - Beantworten von 250 Fragen in einer 6-stündigen Prüfung - Anerkennung/Einhaltung des ISC2-Ehrenkodex - Bestätigung der charakterliche Eignung durch einen CISSP oder durch einen anderweitig Qualifizierten, gestufte Auswahl, **nicht alle Kandidaten werden ausgewählt!** Regelmäßige Weiterbildung (120 Std/3Jahre) Leitfäden u. Vorbereitungsbücher sind vorhandenPrüfungsorte in Deutschland: München, Neuss
Systems Security Certified Practitioner (SSCP) - ISC² Methodenkompetenz IT-Security, eine der hochwertigsten Ausbildungen weltweit, Abstufung / Ergänzung zum CISSP. Beurteilung analog.Prüfungsgebiete: • Access Controls • Administration • Audit and Monitoring • Risk, Response and Recovery • Cryptography • Data Communications • Malicious Code/Malware	Berufszertifikat, IT-Security International Information Systems Security Certification Consortium (ISC)2, Europe Operations, Golden Cross House, 8 Duncannon Street, Strand, London WC2N 4JF, UK, **www.isc2.org**. Kosten: individuell, ca. 2.500,-- EUR++Voraussetzung zur Neuzulassung als SSCP: - Mindestens 1 Jahr Berufserfahrung im Bereich Information Security in einem oder mehreren der 7 Prüfungsgebiete - Erfolgreiches Absolvieren des Examens (>=70%) - Beantworten von 125 Fragen in einer 3-stündigen Prüfung - Anerkennung/Einhaltung des ISC2-Ehrenkodex Regelmäßige Weiterbildung (60 Std/3Jahre) Leitfäden u. Vorbereitungsbücher sind vorhanden Prüfungsorte in Deutschland: München, Neuss
Microsoft Certified Professional (MCP) - Microsoft Hochwertige Funktionsausbildung in einer Microsoft-Zertifizierungprüfung, Abstufungsprüfungen bis zum Engineer oder Developer, Absolvent zeigt technische Expertise. *	Techn. Funktionszertifikat, MS-Produktreihe Microsoft Deutschland GmbH, Konrad-Zuse-Str. 1, Unterschleißheim, **www.microsoft.com/germany**; Microsoft lokale lizenzierte Trainingspartner, siehe **www.microsoft.com/germany/learning/mcp/default.mspx** **www.microsoft.com/germany/learning/zertifizierung/default.mspx**, Kosten: ca. 1.500,-- EUR Voraussetzung zur Neuzulassung als MCP: - Detailwissen in angestrebter Spezialisierung - Erfolgreiches Absolvieren der jeweiligen Prüfung Leitfäden u. Vorbereitungsbücher sind vorhanden Deltaschulungskonzept/Upgrading

Microsoft Certified Systems Administrator (MCSA) - Microsoft Hochwertige Funktionsausbildung im Bereich der Administration auf Basis Windows 2000- und Server 2003- Plattformen, Implementierung, Verwaltung und Fehlerbehebung in vorhandenen Netzwerk- und Systemumgebungen, unterschiedliche Produktschwerpunkte, Windows 2000, Server 2003, Security u. Messaging / Exchange. *	Techn. Funktionszertifikat, MS-Produktreihe Microsoft Deutschland GmbH, Konrad-Zuse-Str. 1, Unterschleißheim, **www.microsoft.com/germany**; Microsoft lokale lizenzierte Trainingspartner, siehe **www.microsoft.com/germany/learning/mcsa/ default.mspx** **www.microsoft.com/germany/learning/ zertifizierung/default.mspx,** Kosten: ca. 5-7.000,-- EUR Voraussetzung zur Neuzulassung als MCSA: - 12 Monate Berufserfahrung im Betriebssystem-, Netzwerk- und Netzinfrastrukturbereich - Erfolgreiches Absolvieren von 4 Prüfungen, 3 aus dem Pflicht- (Core) und eine aus dem Wahlbereich Leitfäden u. Vorbereitungsbücher sind vorhandenDeltaschulungskonzept/Upgrading
Microsoft Certified Systems Engineer (MCSE) - Microsoft Hochwertige Funktionsausbildung für Planung / Konfiguration / Installation / Administration / Support von IT-Infrastruktur auf Basis der MS-Produkte, Prüfungen auf Basis unterschiedlicher Produktschwerpunkte, z.B. Windows 2000, Server 2003 u. Security, Messaging/Exchange etc. *	Techn. Funktionszertifikat, MS-Produktreihe Microsoft Deutschland GmbH, Konrad-Zuse-Str. 1, Unterschleißheim, **www.microsoft.com/germany**; Microsoft lokale lizenzierte Trainingspartner, siehe **www.microsoft.com/germany/learning/mcse/ default.mspx** **www.microsoft.com/germany/learning/ zertifizierung/default.mspx,** Kosten: ca. 8-12.000,-- EUR Voraussetzung zur Neuzulassung als MCSE: - 12 Monate Berufserfahrung mit Bezug zum gewählten Zertifizierungsschwerpunkt / Spezialisierung - Erfolgreiches Absolvieren von 7 Prüfungen aus einer Vielzahl von Möglichkeiten mit der Maßgabe einer Spezialisierung, mindestens 4 Prüfungen sind Core-Prüfungen, hinzu kommen Spezialisierungsprüfungen mit Bezug zu Design-Elementen (Netzwerkdesign, Directory-Service) und wahlweise Prüfungsteile mit Bezug zu Installation / Konfiguration / Support bestimmter MS-Produkte Leitfäden u. Vorbereitungsbücher sind vorhanden Deltaschulungskonzept/Upgrading
Microsoft Certified Database Administrator (MCDBA) - Microsoft Hochwertige Funktionsausbildung zur Implementierung und Verwaltung von Microsoft SQL Server-basierten Datenbanken, dabei Beachtung von Data Services mithilfe von Transact- SQL, Datenbankoptimierung, Monitoring und Security. *	Techn. Funktionszertifikat, MS-ProduktreiheMicrosoft Deutschland GmbH, Konrad-Zuse-Str. 1, Unterschleißheim, **www.microsoft.com/germany**; Microsoft lokale lizenzierte Trainingspartner, siehe **www.microsoft.com/germany/learning/mcdba/ default.mspx** **www.microsoft.com/germany/learning/ zertifizierung/default.mspx,** Kosten: ca. 5-7.000,-- EUR Voraussetzung zur Neuzulassung als MCDBA: - 12 Monate Berufserfahrung im DBA-Bereich - Erfolgreiches Absolvieren von 4 Prüfungen, 3 aus dem Pflicht- und eine aus dem Wahlbereich, Pflicht: SQL-Server-Administration, SQL-Server-Design und Windows 2000 Server oder Server 2003. Leitfäden u. Vorbereitungsbücher sind vorhanden Deltaschulungskonzept/Upgrading

Microsoft Certified Solution Developer (MCSD) - Microsoft Hochwertige Funktionsausbildung im Bereich des Designs und der Entwicklung von Anwendungen, Premium-Zertifizierung für leitende Entwickler, die neueste Unternehmenslösungen mit Microsoft-Entwicklungswerkzeugen, -Technologien und dem Microsoft .NET Framework entwerfen und entwickeln. *	Techn. Funktionszertifikat, MS-Produktreihe Microsoft Deutschland GmbH, Konrad-Zuse-Str. 1, Unterschleißheim, **www.microsoft.com/germany**; Microsoft lokale lizenzierte Trainingspartner, siehe **www.microsoft.com/germany/learning/mcsd/default.mspx** **www.microsoft.com/germany/learning/zertifizierung/default.mspx**, Kosten: ca. 6-8.000,-- EUR Voraussetzung zur Neuzulassung als MCSD in .NET: - 2 Jahre Berufserfahrung im Konzipieren und Entwickeln von Anwendungen - Erfolgreiches Absolvieren von 5 Prüfungen, 4 aus dem Pflicht- (Architektur, ADO, XML, Visual C#, Framework) und eine aus dem Wahlbereich (Server-Produkte / Security, Commerce Server) Leitfäden u. Vorbereitungsbücher sind vorhanden Deltaschulungskonzept/Upgrading
Microsoft Certified Application Developer (MCAD) - Microsoft Hochwertige Funktionsausbildung im Bereich des Designs und der Entwicklung und Wartung von Anwendungen, Komponenten, Web- oder Desktop-Clients sowie Back- End Data Services.*  *Abb. 1: Abgrenzung MCAD zu MCSD - Microsoft Corp.*	Techn. Funktionszertifikat, MS-Produktreihe Microsoft Deutschland GmbH, Konrad-Zuse-Str. 1, Unterschleißheim, **www.microsoft.com/germany**; Microsoft lokale lizenzierte Trainingspartner, siehe **www.microsoft.com/germany/learning/mcad/default.mspx** **www.microsoft.com/germany/learning/zertifizierung/default.mspx**, Kosten: ca. 4-6.000,-- EUR Voraussetzung zur Neuzulassung als MCAD in .NET: - Detailwissen in angestrebter Spezialisierung - Erfolgreiches Absolvieren von 3 Prüfungen, 2 aus dem Pflicht- (Architektur, ADO, XML, Visual C#, Framework) und eine aus dem Wahlbereich (Server-Produkte / Security, Commerce Server) Leitfäden u. Vorbereitungsbücher sind vorhanden Deltaschulungskonzept/Upgrading
SAP-ABAP-Entwickler - SAP Beispiel für die funktionsbezogene Weiterbildung in SAP-Modulen, der technologischen Basis u/o der SAP-Anwendungs- / Funktionsentwicklung, Möglichkeit der kundenspezifischen Definition des Bildungsangebotes. Ein ähnlicher Aufbau ergibt sich bei Anwender- (Funktionsmodulen) und Beraterzertifizierungen (z.B. mySAP ERP, mySAP Business Information Warehouse, SAP NetWeaver), bei älteren Release-Ständen Delta-Schulungen in Zeitintervallen sinnvoll. Bei release-abhängigen Zertifikaten endet die Gültigkeit des Zertifikats, wenn SAP die Wartung des Releases einstellt.	Techn. Funktionszertifikat, SAP-Produktreihe SAP Deutschland AG & Co. KG, Neurottstraße 15a, Walldorf, **www.sap.com/germany**; Für IV-Revision (und IT-Sicherheitsmanagement) sinnvoll: - SAP NetWeaver u/o SAP Programming Curriculum - Schulungen sind modular aufgebaut, max. Ausbaustufe bei SAP-Programmierung bei ca. 50-70 Tagen bis zur Zertifizierungsstufe mit Expertenwissen. Für den Aufbau von Beurteilungskompetenz bei IV-Revisoren sind ca. 20-30 Tage sinnvoll analog dem ehemaligen Kurs TABC40 ([5-wöchige Entwicklerschulung,] z.B. hoher Anteil der BC4- und BIT6-Reihe), auch Zusatzkurse sinnvoll wie Datenarchivierung, DART (WDE614/ 680, BIT660) etc.

Bsp. für Schulungsangebote: http://www.sap.com/germany/services/education/kundenschulung/kundenschulung_netweaver.aspx https://websmp205.sap-ag.de/~sapidp/011000358700000123222003D http://www.unilog.de/training/seminare/sap_abapentwickler.html **SAP-Bildungspartner innerhalb Deutschlands:** http://www.sap.com/germany/services/education/bildungspartner/bpartner.aspx	Voraussetzung zur Teilnahme am Entwickler-Zertifizierungskurs: • Grundkenntnisse des SAP-Systems • Grundkenntnisse über DBMS und SQL • Grundkenntnisse des Programmierens, Einstieg in Scriptsprachen • Grundlagen Objektorientiertes Programmieren Kosten: individuell, hier muss ein sinnvolles Maß gefunden werden, eine sinnvolle Kurssammlung für IV-Revisoren liegt bei ca. 8-10.000,-- EUR Leitfäden u. Vorbereitungsbücher sind vorhanden, SAP-Verlag bietet verstärkt Vertiefungsliteratur, Deltaschulungskonzept/Upgrading

* Die Microsoft-Zertifizierungen können - je nach Anbieter - entweder praxisnah, d.h. incl. Praxis- / Szenarientraining, oder aber theoretisch, d.h. in kurzer Zeit ohne Praxisblock und als fast ausschließliches Literaturstudium, angelegt sein. Als Ausbildungsgrundstock für Revisoren sind auch die theorielastigen Ausbildungsgänge zum Aufbau von Beurteilungskompetenz positiv zu sehen. Microsoft schenkt seit kurzer Zeit dem IT-Sicherheitsaspekt vermehrt Aufmerksamkeit, was sich auch in den Ausbildungsgängen niederschlägt. So kann in fast jedem Qualifizierungsprogramm der Bereich Security durch Belegen bestimmter Kurse/Leistungsscheine als Schwerpunkt bei der Zertifizierung gewählt werden. Dieser Schwerpunkt wird auch als solcher herausgestellt.

Als Ausbildungsgrundstock für Revisoren sind auch die theorielastigen Ausbildungsgänge zum Aufbau von Beurteilungskompetenz positiv zu sehen.

Neben den o.g. Zertifizierungen können noch weitere genannt werden, die jedoch weit über den Aufbau von Beurteilungskompetenz hinausgehen. Im Bereich der hardwarenahen Zertifikate gibt es Ausbildungen, die über Vollzeit-

Im Bereich der hardwarenahen Zertifikate gibt es Ausbildungen, die über Vollzeitunterricht erheblich umfangreicher und kostenintensiver sind als die dargestellten Qualifizierungen.

Oracle: Oracle Certified Professional (OCP)/Database Administrator (DBA)/Oracle Certified Master (OCM): Professionelle, international anerkannte und höchst-niveauvolle Ausbildung im Oracle-Umfeld, Deltaschulungskonzept/Upgrading (Zertifizierung für Administration, Operator und Entwickler).
Cisco (www.cisco.com/en/ US/learning/): Cisco Certified Network Professional (CCNP): Netzwerkinstallation, -konfiguration und -sicherheitCisco Certified Security Professional (CCSP): Sicherheitsmanager in NetzwerkenCisco Certified Academic Instructor (CCAI): Trainer für Netzwerkmanagement auf hohem NiveauCisco Certified Internetwork Expert (CCIE): Hochwertiges Expertenzertifikat, Themen u.a. Routing / Switching, Security, Service Providing, Storage Networking, VoIP.
Beispiele für sonstige Basis- und plattformübergreifende Systeme: Certified Linux Engineer (CLE): Professionelle Konzeption und Implementierung im Linux-UmfeldCertified Unix Administrator (CUA): Professionelle Administration im Unix-UmfeldSun Certified Java Developer (SCJD): Berufserfahrener Java-Applikationsentwickler[...]

Ausgesuchte Zertifizierungsprogramme können helfen, eine zusätzliche Struktur in der Wissensvermittlung zu erreichen und ggf. auftretende Defizite in der Methoden- und Fachkompetenz auszugleichen.

unterricht erheblich umfangreicher und kostenintensiver sind als die dargestellten Qualifizierungen. Hier sind als Beispiele Cisco und Lucent als Vertreter hochwertiger berufsqualifizierender Ausbildungsgänge zu nennen, die jedoch für einen Revisor üblicherweise nicht in Frage kommen. Auch der Datenbankbereich bietet wie oben bereits angeklungen eigenständige Ausbildungsgänge, die weit über das notwendige Maß eines Revisors hinausgehen. Sie sollen jedoch durch die Möglichkeit der sinnvollen Belegung von Teilqualifikationen hier kurz Erwähnung finden.

Fazit

Durch Fachliteratur, Selbststudium und Erfahrungsaustausch erfolgt ein regelmäßiger Know-how-Transfer zwischen Revisoren und Praktikern. Ausgesuchte Zertifizierungsprogramme können helfen, eine zusätzliche Struktur in der Wissensvermittlung zu erreichen und ggf. auftretende Defizite in der Methoden- und Fachkompetenz auszugleichen. Im Zuge dessen zeigt dies die Bereitschaft des Einzelnen, sich den Neuerungen des Marktes zu stellen, d.h. neue Entwicklungen aus Forschung, Lehre und Praxis zu verinnerlichen, der operativen Ebene "auf gleicher Höhe zu begegnen" und somit den Bezug zum eigentlichen operativen Geschäft nicht zu verlieren. Gleichzeitig tragen sie dem Grundsatz des lebenslangen Lernens im Unternehmen dokumentiert Rechnung. Voraussetzung ist, dass die Führungsebene diese Leistungsbereitschaft fördert und bereitwillig honoriert.

Gleichzeitig tragen sie dem Grundsatz des lebenslangen Lernens im Unternehmen dokumentiert Rechnung. Voraussetzung ist, dass die Führungsebene diese Leistungsbereitschaft fördert und bereitwillig honoriert.

*Die Kostenangaben sind lediglich Richtwerte, die in Abhängigkeit der Vorkenntnisse, bevorzugten Fachliteratur und der Trainingspartnerangebote variieren. Sie spiegeln die Einschätzung über die Prüfungsgebühren und obligatorischen Kosten der Vorbereitungsseminare einschließlich üblicher Literatur ohne Reisekosten, Übernachtung und sonstige Kosten (ohne staatliche Förderungsmöglichkeit) wider. Berufserfahrung bezieht sich immer auf Vollzeitbeschäftigung. Testfragen werden als Multiple-Choice mit "4-1-Regel" gestellt.

Literatur:

A Geschonneck
Computer-Forensik
iX-Edition, Heidelberg 2004

Internetseiten:

www.lanworks.de - CISSP/SSCP

www.microsoft.com/germany/learning/mcp/default.mspx - MCP/MCSE/MCDBA

www.microsoft.com/learning/default.asp - MCP/MCSE/MCDBA

www.microsoft.com/learning/mcp/default.asp - MCP/MCSE/MCDBA

www.microsoft.com/germany/learning/zertifizierung/default.mspx - MCP/MCSE/MCDBA

www.sap.com/germany/services/education/kundenschulung/kundenschulung_netweaver.aspx - ABAP

www.unilog.de/training/seminare/sap_abapentwickler.html - ABAP

www.oracle.com/education/certification/certpaths.html - ORACLE

www.cisco.com/en/US/learning/ - Cisco-Produktzertifizierung

www.donau-uni.ac.at/de/ - Weiterbildungsprogramme der Donauuniversität Krems ✣

➲ Auditierung des Datenschutzes: Neue Aufgaben für Revisoren

Der Revision sind in den letzten Jahren neue Aufgaben zugewachsen. Diese haben sich daraus ergeben, dass sich in vielen Gebieten die externen Bedingungen in Form von neuen und anders gearteten Gesetze in Bezug auf Unternehmensbewertungs- und Beurteilungskriterien geändert haben und darüber hinaus das Durchdringen der Unternehmen mit moderner Informationstechnologie andere Bedingungen für die Arbeit des Revisors geschaffen haben.

Prof. Dr.
Reinhard Vossbein
UIMCert GmbH

Als Folge hieraus sollte der Revisor heute Aufgaben wahrnehmen, die seine Position im Unternehmen stärken, neue Herausforderungen an seine Kompetenz stellen und in Kooperationen mit Dritten enden wie z. B. dem Sicherheitsbeauftragten oder dem Datenschutzbeauftragten. Datenschutz als Revisionsaufgabe gehört heute bereits in vielen Unternehmen zum Alltag.

Zur Problematik

1. Datenschutz als Revisionsaufgabe

Die Funktion des Revisors in Sachen Datenschutz ergibt sich aus seiner Stellung im Unternehmen sowie daraus, wie die Beziehung zwischen ihm und dem Datenschutzbeauftragten ist. In einer beachtlichen Anzahl von Unternehmen ist der Revisor gleichzeitig Datenschutzbeauftragter, sodass die Revisionstätigkeit in Sachen Datenschutz sich aus der Datenschutzbeauftragtenfunktion ergibt. Wichtig ist hierbei die Feststellung, dass der Datenschutzbeauftragte grundsätzlich weisungsfrei und unabhängig arbeitet und - sofern keine Personalunion zwischen Revisor und Datenschutzbeauftragten gegeben ist - der Revisor zwar den Datenschutzbeauftragten unterstützen kann, er jedoch nicht berechtigt ist, Kontrollfunktionen auszuüben.

Somit bestimmen die konkreten situativen Unternehmensbedingungen, welche Aufgaben der Revisor tatsächlich vom Datenschutzbeauftragten (DSB) übernehmen kann. Da der Datenschutzbeauftragte ebenfalls eine Vielzahl von Prüfaufgaben wahrzunehmen hat, wäre es im Sinne einer Arbeitsteilung sinnvoll - zumal der Datenschutzbeauftragter im Regelfall nur ein sehr begrenztes Zeitbudget zur Verfügung hat -, wenn der Revisor einen Teil dieser Prüfaufgaben dem DSB abnimmt und ihm die Prüfberichte zur Verfügung stellt.

Sein Verhältnis zum bDSB bestimmt damit, in welchem Umfang Prüfaufgaben entweder vom Revisor in seiner Funktion als Datenschutzbeauftragter bei Personalunion wahrgenommen werden oder aber in wieweit er solche Aufgaben nach vorheriger Absprache mit dem Datenschutzbeauftragten wahrnimmt.

Die Prüfungsgebiete und Prüfobjekte ergeben sich aus

- gesetzlichen Grundlagen und der Notwendigkeit ihrer Einhaltung sowie
- unternehmensinternen Verpflichtungen, Regelungen und Vorgaben.

Die Prüfstandards und Prüfnormen lassen sich damit aus diesen Gebieten ableiten.

2. Gesetzliche Anforderungen als Prüfgrundlagen

Nachdem das Bundesdatenschutzgesetz BDSG die Grundlagen für den personenbezogenen Datenschutz geschaffen hat, wurden im Verlaufe der Jahre weitere Gesetze um datenschutzrelevante Tatbestände erweitert bzw. es wurden aus ihnen datenschutzrelevante Forderungen durch Auslegung konkreter Gesetzestatbestände abgeleitet. Ohne Anspruch auf Vollständigkeit sind folgende wesentliche Gesetze zu nennen, die datenschutzrelevante Anforderungen beinhalten.

Gesetz	**Kurzkommentar**
• Richtlinie 1995/46/EG vom 24.10.1995 (Datenschutzrichtlinie); Richtlinie 2002/58/EG vom 12.07.2002 (Datenschutzrichtlinie für elektronische Kommunikation)	• Grundlage für die Datenschutzgesetze bzw. Telegesetze der EU-Mitgliedstaaten, bedürfen zur Wirksamkeit der Umsetzung in nationales Recht
• Bundesdatenschutzgesetz (BDSG) vom 20.05.2001	• Allgemeine Regelung des Schutzes personenbezogener Daten durch Bundesbehörden und nicht-öffentliche Stellen
• "Gesundheitsdatenschutzgesetze" der Länder	• Spezialgesetz für den Gesundheitssektor, u. a. Gesundheitsdatenschutzgesetz NW (GDSG NW) vom 22.02.1994 oder konkurrierende Krankenhausgesetze der Länder
• "Telegesetze"	• Gesetzessammlung im Anwendungsbereich der Telekommunikation; etwa TKG, TDG, TDDSG, SigG, SigV etc.
• Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 05.03.1998	• Enthält insbesondere die Pflicht zur Erstellung und Durchführung eines angemessenen Risikomanagementsystems für Aktiengesellschaften sowie mittelbar für große GmbHs und andere Rechtsformen
• Strafgesetzbuch (StGB) vom 15.05.1871	• Enthält eine Vielzahl von Normen, die mit dem Datenschutz in Zusammenhang stehen, etwa§ 202a StGB Ausspähen von Daten, § 203 StGB Verletzung von Privatgeheimnissen, § 206 StGB Verletzung des Post- und Fernmeldegeheimnisses
• Sozialgesetzbuch (SGB)	• Enthält in einer Mehrzahl von Büchern Regelungen, die den Schutz personenbezogener Daten im Zusammenhang mit der gesamten Sozialgesetzgebung betreffen, insb. § 35 SGB I Sozialgeheimnis, §§ 50ff SGB II Datenübermittlung und Datenschutz im Bereich der Grundsicherung für Arbeitssuchende (ALG II), §§ 67ff SGB X Schutz der Sozialdaten
• Betriebsverfassungsgesetz vom 25.09.2001 (BetrVG)	• Enthält insbesondere Auswirkungen auf die Nutzung personenbezogener Daten zur Leistungs- und Verhaltenskontrolle, § 87 I Nr. 6 BetrVG

Abb. 1: Gesetzliche Regelungen und Datenschutz

Am Beispiel des KonTraG soll verdeutlicht werden, inwiefern ein Zusammenhang zwischen KonTraG als Gesetz und der Datenschutzgesetzgebung gegeben ist und darüber hinaus sich hieraus Revisionsnotwendigkeiten ergeben.

Zielsetzung des KonTraG

Das KonTraG will
- risikobehaftete Geschäfte,
- Unrichtigkeiten der Rechnungslegung,
- Verstöße gegen gesetzliche Vorschriften,

die sich auf die Vermögens-, Finanz- und Ertragslage wesentlich auswirken, offenlegen mit der Zielsetzung, sie durch geeignete Maßnahmen beseitigen zu lassen. Faktisch bedeutet dies, dass der dritte Punkt, der sich mit Verstößen gegen gesetzliche Vorschriften beschäftigt, in diesem Zusammenhang Berücksichtigung finden muss. So legen die Datenschutzgesetze fest, dass z. B. Ordnungswidrigkeiten nach § 43 BDSG mit Strafen bis zu 25.000 € geahndet werden können. Wenn dies als Auswirkung auf die Vermögens- oder Finanzlage nicht ausreicht, um auf einer Einhaltung der gesetzlichen Vorschriften zu bestehen, kann eine Risikobetrachtung im Zusammenhang mit den Risiken der Informationstechnologie - die in der Anlage zum § 9 BDSG niedergelegt sind - zu einer weiteren Rechtfertigung für eine Beschäftigung mit dem Datenschutz führen. Hier ist dann von der Risikoseite her die unmittelbare Beziehung zu den typischen IT-Sicherheitsrisiken wie mangelhaften Berechtigungssystemen, Zugangskontrollesystemen, Protokollierungssystemen oder ähnlichem gegeben.

3. Nichtgesetzliche Prüfgrundlagen

Die nicht auf Gesetzesgrundlagen bestehenden Prüfungsgebiete sind solche, die sich aus unternehmensspezifischen Regelungen ergeben. Hier sind insbesondere zu nennen:
- Unternehmensverpflichtungen (Code of Conduct)
- Organisationsanweisungen
- Interne Richtlinien

Unternehmensverpflichtungen im Sinne eines Code of Conduct finden sich zunehmend mehr in Großunternehmen, wobei zum Teil ein Zusammenhang mit dem Aspekt der Einhaltung von Datenschutzforderungen im grenzüberschreitenden Datenverkehr in nicht zur EU gehörigen Ländern gegeben ist. Unabhängig hiervon gibt es jedoch auch Unternehmen, die im Rahmen ihrer Datenschutzstrategie und ihres Datenschutzmanagementsystems unternehmensinterne Verpflichtungen aufgestellt haben, die damit in ihrer Einhaltung zum Prüfgegenstand werden.

Ähnliches gilt für erlassene Organisationsanweisungen im Hinblick auf entweder aus dem Gesetz ableitbare Forderungen oder aber solchen, die sich z. B. aus der Kooperation mit den Mitarbeitervertretungen ergeben und sich möglicherweise bevorzugt auf Arbeitnehmerdaten beziehen.

Eine entsprechende Aussage ist für interne Richtlinien zu

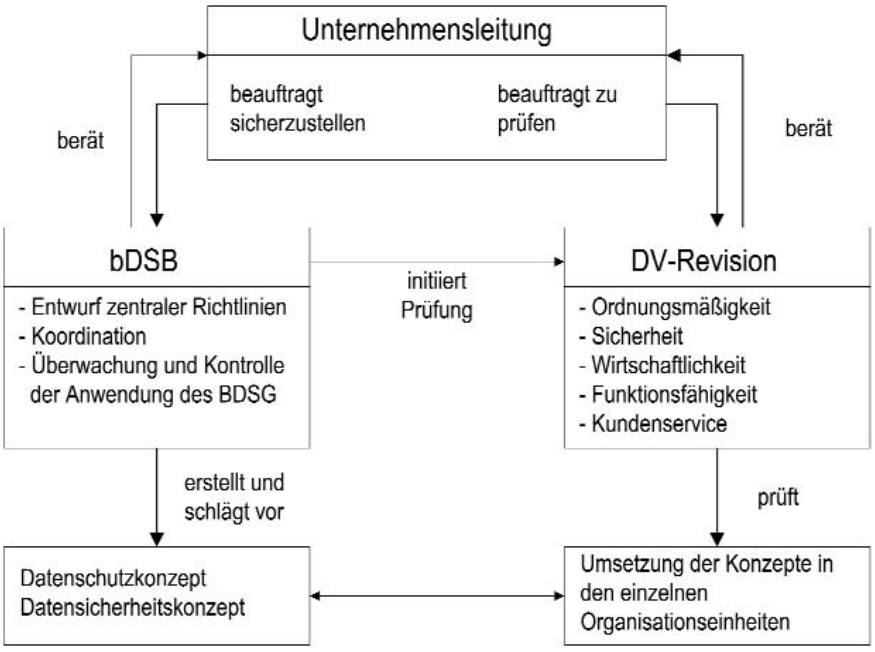


Abb. 2: Beziehung Datenschutzbeauftragter - Revision

machen, bei denen z. B. Betriebsvereinbarungen datenschutzrelevante Aspekte enthalten und damit im Hinblick auf ihre Einhaltung zum Prüfgegenstand werden.

4. Zusammenarbeit Revisor/ Datenschutzbeauftragter

Die Abbildung 2 verdeutlicht die Beziehungen zwischen dem Datenschutzbeauftragten und der DV-Revision.

Während die gestalterischen Aufgaben im Wesentlichen beim Datenschutzbeauftragten liegen, kann die Prüfung des gesamten Richtlinienwesens, der Überwachung und Kontrolle der Anwendungen des BDSG sowie der Einhaltung des Datenschutzkonzepts der DV-Revision übertragen werden. Die Sinnhaftigkeit der Zusammenarbeit lässt sich auch aus der folgenden Tabelle ableiten.

Die Aufgaben des Datenschutzbeauftragten sind zum einen solche, die er de facto in persona wahrzunehmen hat und zum anderen solche, bei denen die Unterstützung der Revision sinnvoll, bei einer Beschränkung des Zeitbudgets des Datenschutzbeauftragten sogar notwendig ist. So können Überwachungsaufgaben grundsätzlich in Zusammenarbeit mit der Revision wahrgenommen werden, die Durchführung von Vorabkontrollen wird in wesentlichen Punkten ebenfalls eine gemeinsame Aufgabe sein können. Es gibt weiterhin bestimmte Aufgaben, bei denen die Revision z. B. Prüfaufgaben wahrzunehmen in der Lage ist, wenn bestimmte Konzepte vorhanden sind. Dies trifft z. B. auf den gesamten Bereich der Schulung zu.

Ein im Prinzip ausgesprochen kritisches Gebiet ist das der Aus- und Weiterbildung des Datenschutzbeauftragten, bei dem die Revision den Datenschutzbeauftragten kontrollieren würde, was im Sinne der Verantwortlichkeit des Datenschutzbeauftragten - er ist lediglich dem Gesetz verpflichtet - nicht rechtens wäre. Die Frage, was jedoch eine Revisionsfeststellung bewirken würde, dass der Datenschutzbeauftragte die Aus- und Weiterbildungsverpflichtung seiner eigenen Person nicht wahrnimmt, bleibt jedoch hierbei unbeantwortet.

	Aufgaben des Datenschutzbeauftragten
1	Überwachung bei der Führung von Übersichten
2	Überwachung der ordnungsgemäßen Anwendung der DV-Programme
3	Durchführen der Vorabkontrolle
4	Bekanntgabe der Vorschriften an die mit der Datenverarbeitung beschäftigten Personen und deren Schulung
5	Verpflichtung auf das Datengeheimnis im Sinne des § 5 BDSG
6	Beratung über technische und organisatorische Maßnahmen
7	Erarbeitung und Pflege eines Datenschutz-Handbuches
8	Kontrolle und Wahrung der Rechte Betroffener
9	Aus- und Weiterbildung des Datenschutzbeauftragten
10	Erstellen eines Tätigkeitsberichtes
11	Sonstiges

Abb. 3: Aufgaben des bDSB

Ein wichtiges Gebiet der Kooperation zwischen Datenschutzbeauftragten und Revision ist das Datenschutz-Audit. Das Gesetz sagt hierüber folgendes:

Datenschutzaudit § 9 a BDSG[1]

"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."

Unabhängig davon, dass das Gesetz zur Zeit ein Datenschutzaudit nicht verbindlich vor-

schreibt, kann jedoch die nachstehende Zielsetzung für ein Datenschutz Audit formuliert werden.

Zielsetzung für ein Datenschutz-Audit

Ein Datenschutz-Audit soll den Stand der Realisierung der Forderungen des BDSG, TKG sowie anderer relevanter, den personenbezogenen Datenschutz betreffender Gesetze in einer Institution abbilden, beurteilen sowie Möglichkeiten zu seiner Verbesserung/Anhebung bieten. Wegen der Gültigkeit möglicherweise spezifischer Gesetze (SGB, LDSG o. a.) ist die Zielsetzung individuell auf die Institution abzustimmen.

Bei dieser "Philosophie" hat das Datenschutzaudit die überaus wichtige Funktion, die Qualität des Datenschutzes in einer Institution ganzheitlich zu überprüfen. Dies ist jedoch im Prinzip die Hauptaufgabe des Datenschutzbeauftragten, sodass ein Datenschutzaudit - fachkundig von einem Revisor durchgeführt - einen wesentlichen Baustein für die effiziente und qualitativ hochwertige Arbeit eines Datenschutzbeauftragten darstellt. Unter diesem Aspekt ist es ein wesentliches Gebiet der Kooperation zwischen Datenschutzbeauftragten und Revision.

5. Arbeitsparende Hilfsmittel und Tools

Zum Zweck der Effizienzerhöhung und Rationalisierung sollte es eigentlich selbstverständlich sein, verfügbare Hilfsmittel und Tools zur Arbeitserleichterung einzusetzen. Generell üblich ist es, Handbücher, Regelsystemsammlungen und andere altbewährte Instrumente einzusetzen, um durch Standardisierung die hiermit verbundenen Vorteile zu realisieren.

Die nachstehende Struktur gibt ein Beispiel dafür, wie ein Datenschutzhandbuch gegliedert werden kann.

Datenschutz-Handbuch

1 *Einleitung*
2 *Funktionsträger des Datenschutzes*
- Überblick über die Funktionsträger
- Zielsetzung von Stellenbeschreibungen und Ergänzungen zu Stellenbeschreibungen.
- Kooperationspartner des Datenschutzbeauftragten

3 *Allgemeine datenschutzrelevante Regelungen für Mitarbeiter*
- Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Schulungskonzept

4 *Spezielle datenschutzrelevante Regelungen für bestimmte Organisationsbereiche*
- Zielsetzung der nachstehenden datenschutzrechtlichen Regelungen und Überblick
- Technische und organisatorische Maßnahmen
- Richtlinie zur Beschaffung von Hard- und Software
- Richtlinie zu den Meldepflichten

5 *Organisationsmittel des Datenschutzbeauftragten*

6 *Formale Regelungen*

Abb. 4: Struktur Datenschutz-Handbuch

Ein weiteres Hilfsmittel zur Rationalisierung der Revisionsarbeit ist die Nutzung eines Checkup Tools. Ein solches Tool rationalisiert die Analyse, erleichtert die Berichterstattung und hat darüber hinaus den Vorteil, dass es durch seine Standardisierung auf unterschiedliche Organisationseinheiten voll identisch anwendbar ist oder aber zu unterschiedlichen Zeitpunkten vergleichbare Erhebungs- und Berichtsergebnisse liefert.

Der Datenschutz-Checkup

Umfang des Datenschutz-Checkups

Der Umfang des Datenschutzcheckups unterhält folgende Prüfungsfelder:

- das realisierte Datenschutzniveau gem. BDSG und die sich hieraus ergebenden Schwachstellen
- das generell realisierte Datenschutzniveau und die sich hieraus ergebenden Schwachstellen
- die bisher eingesetzten BDSG-relevanten Datensicherungsmaßnahmen und die aus dem derzeitigen Niveau sich ergebenden Schwachstellen.
- das im Unternehmen vorhandene Sicherheitsbewußtsein und die hieraus sich ergebenden Probleme für die Anhebung des Sicherheitsniveaus bei der Realisierung.

Die Präzisierung der Prüfungsfelder geschieht durch Einzelmodule, die in Form von Checklisten aufgebaut sind.

Die Präzisierung der Prüfungsfelder geschieht durch Einzelmodule, die in Form von Checklisten aufgebaut sind. Hierbei sind die Checklistensammlungen der einzelnen auf dem Markt erhältlichen Tools/Produkte unterschiedlich aufgebaut, wobei das wesentliche jedoch sein muß, dass das gesamte Gebiet des Datenschutzes hinreichend abgebildet ist. Dies bedeutet, dass ein Tool gegebenenfalls durch Zusatzmodule ergänzt werden muss, die branchen- oder unternehmensspezifischen Belangen Rechnung tragen. Die folgende Aufstellung ist daher als Beispiel zu bewerten.

Der Datenschutz-Checkup: Checklisten für die Prüfung

Checklisten bestehen z. B. für die nachstehenden Gebiete. Sie bauen auf Prüfungsfeldern auf und strukturieren diese vertieft. Die derzeit realisierte Konzeption beinhaltet folgende Prüfgebiete:

- Datenschutzstrategie der Institution
- Grundlegende organisatorische Fragestellungen
- Allgemeine Bestimmungen des BDSG
- Rechtsgrundlagen der Datenverarbeitung
- Rechte der Betroffenen (u.a. Berichtigung, Löschung und Sperrung von Daten)
- Der Beauftragte für den Datenschutz (Fachkunde, Zuverlässigkeit)
- Kontrollorgane (Aufsichtsbehörde)
- Sondervorschriften und ihre Bedeutung für das Unternehmen
- Allgemeine Benutzung des DV-Systems (Zutritt, Zugang, Zugriff, Protokollierung)
- Personaleinsatz, Motivation und Schulung
- Datensicherung
- Datenträgerlagerung, -verwaltung und -vernichtung
- Organisation und Verfügbarkeit von Netzsystemen
- Revision des Datenschutzes

Diese allgemein gültigen Prüfungsgebiete werden noch ergänzt um solche, die spezifisch sind für z. B. das Gesundheitswesen, Landesbehörden oder ähnliche Institutionen.

6. IT-Sicherheit und Datenschutz - gemeinsame Revisionsobjekte?

Ein häufig vorgebrachter Einwand gegen den Datenschutz besteht darin, dass er "nur Kosten verursacht". Es soll hier nicht diskutiert werden, dass diese Auffassung die Notwendigkeit des Datenschutzes in einer modernen Informationsgesellschaft nicht hinreichend berücksichtigt. Es soll vielmehr vorgehoben werden, dass ein beachtlicher Anteil des Datenschutzes auf den Prinzipien der IT-Sicherheit besteht und damit dem Unternehmen insgesamt zu sicheren Systemen verhilft bzw. geradezu die Voraussetzung für den Einsatz der modernen Informationstechnologie im Unternehmen schafft. Die nachstehende Aufzählung der so genannten technisch-organisatorischen Maßnahmen des Datenschutzes müsste jeden Skeptiker davon überzeugen, dass Datenschutz und IT-Sicherheit nicht trennbar sind. Der Zusammenhang zwischen IT-Revision und Datenschutzrevision erschließt sich bei einer sorgfältigen Betrachtung der nachstehenden Prüffelder von selbst.

Ein häufig vorgebrachter Einwand gegen den Datenschutz besteht darin, dass er "nur Kosten verursacht".

Es soll vielmehr vorgehoben werden, dass ein beachtlicher Anteil des Datenschutzes auf den Prinzipien der IT-Sicherheit besteht und damit dem Unternehmen insgesamt zu sicheren Systemen verhilft bzw. geradezu die Voraussetzung für den Einsatz der modernen Informationstechnologie im Unternehmen schafft.

Technisch-organisatorische Maßnahmen des Datenschutzes gemäß der Anlage zu § 9 BDSG	
1. Zutrittskontrolle	Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren
2. Zugangskontrolle	zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können
3. Zugriffskontrolle	zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können
4. Weitergabekontrolle	zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist
5. Eingabekontrolle	zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssyteme eingegeben, verändert oder entfernt worden sind
6. Auftragskontrolle	zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden
7. Verfügbarkeitskontrolle	zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind
8. Trennungsgebot	zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

Abb.5: Technisch-organisatorische Maßnahmen gem. BDSG

Die Erfahrung hat gezeigt, dass die Realisierung technischer Bedingungen allein nicht ausreicht...

Die Erfahrung hat gezeigt, dass die Realisierung technischer Bedingungen allein nicht ausreicht, um sichere oder datenschutzordnungsmäßige Systeme zu schaffen. Dies bedeutet, dass der Einsatzumgebung im Sinne der organisatorischen Bedingungen der Nutzung der IT eine besondere Bedeutung für den Betrieb sicherer Systeme zukommt und sie damit also gleichermaßen bedeutungsvoll für die Revision der IT-Sicherheit ist.

7. Fazit/Zusammenfassung

Die dargelegten Überlegungen zur Kooperation zwischen Datenschutzbeauftragtem und Revision haben belegt, dass eine sinnvolle Trennung der Tätigkeitsgebiete beider Funktionsträger kaum möglich ist. Dies bedeutet, dass bei dem notorischen Zeitmangel des Datenschutzbeauftragten seine Effizienz durch eine gute Kooperation mit der Revision beträchtlich erhöht werden kann. Diese Chance zur Verbesserung sollte der Datenschutzbeauftragte auf jeden Fall nutzen, wobei auch die Revision durch die Einbeziehung von Datenschutzrevisionsaufgaben eine deutliche Aufwertung erfahren kann. ✣

➲ IT-Sicherheit: Voraussetzung für die Ordnungsmäßigkeit der Buchführung und den Datenschutz im Unternehmen

Revision des Sicherheitsmanagements in vier Schritten

Dipl.-Volkswirt, CISM
Bernd Kamlah
ReviSec

Das Thema IT-Sicherheit wird zunehmend als Wettbewerbsfaktor anerkannt. Darüber hinaus ist die Sicherheit in der Informationstechnik aber auch die Voraussetzung einer ordnungsmäßigen IT-gestützten Buchführung und für den gesetzeskonformen Datenschutz. Die Revision muss sich daher auch dem Thema IT-Sicherheit unter verschiedenen Blickwinkeln nähern. Im Zentrum steht aber stets ein angemessenes IT-Sicherheitsmanagement. Dessen Revision kann in vier Schritten erfolgen.

Lange Zeit wurde das Thema IT-Sicherheit auf den technischen Aspekt reduziert. Mit dem Einsatz von Virenschutzprogrammen und Firewalls war das Thema für viele Unternehmen ausgeschöpft. Doch die Gefährdungen der IT-Sicherheit sind nicht auf den technischen Aspekt zu begrenzen.

Durch Social Engineering etwa werden Mitarbeiter dazu gebracht, Informationen weiterzugeben, die unter Umständen zu erheblichen Schäden für das Unternehmen führen können. Hier bedarf es einer restriktiven Rechtevergabe für den Zugriff auf sensitive Daten, damit nicht unbeabsichtigt Daten weitergegeben werden können, zu denen ein Mitarbeiter eigentlich gar keinen Zugriff benötigt. Hierzu müssen die Mitarbeiter hinsichtlich der möglichen Folgen für das Unternehmen (Existenzbedrohung) und der rechtlichen Auswirkungen für den Mitarbeiter (strafgesetzliche Verfolgung) sensibilisiert und geschult werden.

Weitere Bedrohungen sind Umweltgefährdungen, wie etwa Naturkatastrophen oder auch Unfälle mit Auswirkungen auf den eigenen Standort. Hierzu müssen rechtzeitig, d.h. vor Eintritt eines Schadensereignisses, Szenarien für die Aufrechterhaltung des Systembetriebs zur Unterstützung der Aufrechterhaltung der Geschäftstätigkeiten erarbeitet und möglichst getestet werden. Eine Notfallplanung für den IT-Betrieb liegt somit im vitalen Interesse eines jeden Unternehmens, das seine Geschäftsabläufe IT-gestützt durchführt. Hierzu ist aber mehr als ein Datensicherungskonzept erforderlich. Es müssen Analysen zur gegenseitigen Abhängigkeit der IT-Systeme sowie deren tolerierbaren Ausfallzeiten durchgeführt werden. Wiederbeschaffungs- und Wiederanlaufpläne gehören ebenso zur Notfallvorsorgeplanung wie die Untersuchung mög-

licher Ausweichlösungen und die Festlegung einer Eskalationsstrategie.

Allein aus diesen wenigen Beispielen wird ersichtlich: Die weitaus größte Gefährdung für die IT-Sicherheit geht aus organisatorischen Schwächen hervor, und das größte Risiko liegt darin, die Risiken nicht zu erkennen.

Hierauf hat auch der Gesetzgeber reagiert und in einer Fülle von Vorgaben zur Sensibilisierung für das Thema IT-Sicherheit beigetragen. Aber auch der Druck durch den Wettbewerb selbst und durch den Wettbewerb beeinflussende Institutionen ist gestiegen.

Wer das Thema IT-Sicherheit heute noch nicht zur Chefsache gemacht hat, handelt fahrlässig. Genau dies wird durch die gesetzlichen Regelungen noch unterstrichen. Es gibt zwar gesetzliche Regelungen, die den Verrat von Datengeheimnissen, das Ausspähen von gespeicherten Informationen oder Computersabotage unter Strafe stellen, es werden aber genauso Maßnahmen gefordert, die es einem Täter nicht zu einfach machen, an die Daten und Systeme heranzukommen.

Kaum beachtet wurden bisher die Auswirkungen auf die Haftung der Unternehmen bei Gesetzesverstößen durch Mitarbeiter, die hierzu die IT-Infrastruktur ihres Arbeitgebers nutzen. Nach aktueller Rechtsprechung müssen sich die Verantwortlichen fragen, inwieweit illegale Handlungen der Mitarbeiter zur Mitverantwortung des Unternehmens bzw. der Geschäftsleitung führen können.

Die obergerichtliche Rechtsprechung orientiert sich in Bezug auf die Haftungssystematik an der Erfüllung von Verkehrssicherungspflichten, die aus betrieblichen Organisationspflichten und Aufsichtsmaßnahmen gegenüber den Arbeitnehmern bestehen. Zur Erfüllung der Anforderungen sind Maßnahmebündel aus informationstechnischen, infrastrukturellen, personellen und organisatorischen Maßnahmen umzusetzen. Bei einer Missachtung können betriebliche Kontrollschwächen, die z.B. zu Raubkopien von Software oder zu strafbaren Downloads von Dateien (Musik-Dateien, Dateien mit pornographischen Inhalten) geführt haben, nach der aktuellen Rechtsprechung zur Mithaftung im Unternehmen führen.

Auch Banken oder Investoren können die IT-Sicherheit prüfen, zum Beispiel im Rahmen eines Ratings (Basel II - Prüfung operativer Risiken, wozu auch IT-Risiken zählen) oder eines Gutachtens zur Bewertung der Risiken. Bei der Vergabe von Aufträgen im Rahmen öffentlicher Ausschreibungen wird zunehmend der Nachweis einer ausreichenden IT-Sicherheit zur Bedingung.

Bei der Vergabe von Aufträgen im Rahmen öffentlicher Ausschreibungen wird zunehmend der Nachweis einer ausreichenden IT-Sicherheit zur Bedingung.

Weiterhin sind die Wirtschaftsprüfer im Rahmen der Prüfung des Jahresabschlusses verpflichtet zu beurteilen, ob die Unternehmensleitung die erforderlichen Maßnahmen zur Einrichtung eines geeigneten Überwachungssystems getroffen hat und ob dieses System seine Aufgabe auch erfüllen kann. Hierzu wurden durch das IDW eigene Rechnungslegungs- und Prüfungsstandards etabliert, und es besteht eine Berichtspflicht bei wesentlichen Mängeln.

Schließlich können auch die zuständigen Aufsichtsbehörden, die Gewerbeaufsicht und die berufsständischen Kammern die IT-Sicherheit in einem Unternehmen prüfen. Fällt ein Unternehmen im Geschäftsbetrieb immer wieder wegen Lücken in der IT-Sicherheit auf, kann es zum Beispiel von Wettbewerbern beim Gewerbeamt angezeigt werden. Die Gewerbeerlaubnis kann dann wegen fehlender Zuverlässigkeit eingezogen werden.

Wer gedacht hat, dass er sich mit Versicherungen der Verantwortung zur Etablierung eines angemessenen IT-Sicherheitsmanagements ein Stück weit entzie-

Insbesondere bei Verstößen gegen die im BDSG geregelten Bestimmungen drohen den Unternehmen hohe Bußgelder (fahrlässige Verstöße bis 25.000 € und vorsätzliche Missachtung bis 250.000 €).

hen kann, liegt auch hier falsch. Auch der Versicherungsschutz ist in Gefahr, wenn fahrlässige Lücken bei der IT-Sicherheit nachweisbar sind. Tritt ein Schaden ein, der in Zusammenhang mit Defiziten in der IT-Sicherheit steht, kürzen Versicherer in der Regel die vereinbarte Leistung unter dem Vorbehalt des Mitverschuldens. Nebenbei haben die IT-Risiken und der Umgang mit ihnen häufig auch einen Einfluss auf die Höhe der Versicherungsprämie.

Mit der Novellierung des Bundesdatenschutzgesetzes können die Landesaufsichtsbehörden ohne Vorliegen konkreter Hinweise auf Verstöße jederzeit eine Prüfung der Einhaltung der im BDSG und den Landesgesetzen festgelegten Datenschutzbestimmungen durchführen. Hierbei werden auch die im Verfahrensverzeichnis aufzuführenden, technisch-organisatorischen Regelungen zum Schutz personenbezogener Daten (Anhang § 9 BDSG - z.B. Zutrittskontrollen, Zugriffskontrollen, Weitergabekontrollen etc.) geprüft.

Insbesondere bei Verstößen gegen die im BDSG geregelten Bestimmungen drohen den Unternehmen hohe Bußgelder (fahrlässige Verstöße bis 25.000 € und vorsätzliche Missachtung bis 250.000 €). In Zeiten knapper Staatskassen wird diese Einnahmequelle sicher künftig an Bedeutung gewinnen.

Es ist sicher besser den Handlungsbedarf aus eigener Initiative zu ermitteln und anzugehen, als diesen durch die Aufsichtsbehörden feststellen zu lassen und dann innerhalb gegebener Fristen nachzuarbeiten und Bußgeldverfahren zu riskieren.

Es gibt somit ausreichend Gründe, warum sich die Revision mit dem Thema IT-Sicherheit beschäftigen sollte. Zum einen dient eine interne Revision in diesem Bereich dazu, zur Sensibilisierung der Unternehmensleitung beizutragen, und somit das Unternehmen vor rechtlichen Konsequenzen bei Missachtung zu bewahren. Zum anderen dient die Prüfung im Sinne einer sog. High-Level Control (Bezeichnung aus IDW FAIT 1 und IDW PS 330) dem Nachweis, dass sich die Unternehmensleitung der IT-Risiken bewusst ist und an der Optimierung des Sicherheitsniveaus arbeitet. In jedem Fall trägt die Durchführung einer Revision im IT-Security Umfeld zur Optimierung des Sicherheitsmanagements bei.

Die Revision muss schließlich prüfen, ob die Anforderungen an die Datensicherheit im Sinne der GoB/GoBS (Verfügbarkeit und Integrität) im rechnungslegungsrelevanten IT-Umfeld umgesetzt werden. Sie muss aber auch auf die Einhaltung der gesetzlichen Forderungen zum Datenschutz achten. Neben der schriftlichen Bestellung eines fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten sind auch das Verfahrensverzeichnis und die Umsetzung der technisch-organisatorischen Regelungen zur Datensicherheit im Sinne des § 9 BDSG (Anhang) zu prüfen.

Im Fokus der Prüfungshandlungen steht dabei immer das IT-Sicherheitsmanagement im Unternehmen. Denn hier laufen die Fäden in Sachen IT-Sicherheit zusammen. Hier werden die strategischen Richtlinien durch die Unternehmensleitung vorgegeben, und hier wird die Auseinandersetzung mit dem Thema **IT-Sicherheit** zentral dokumentiert und verwaltet. Ein angemessenes Sicherheitsmanagement verfügt auch über Kontrollinstanzen zur Überwachung der Einhaltung und Wirksamkeit der festgelegten Sicherheitsmaßnahmen, auf deren Analysen die Revision zurückgreifen kann oder die sie selbst zum Thema einer Prüfung machen kann.

Was gehört nun zu einem angemessenen IT-Sicherheitsmanagement? Vier Schritte einer IT-Security Revision:

Das Sicherheitsmanagement im Unternehmen ist die Sub-

summierung aller Vorgaben und Maßnahmen, die sich mit dem Thema **IT-Sicherheit** beschäftigen. Ausgehend von den strategischen Vorgaben der Unternehmensleitung zur Vorgehensweise und zur Sicherheitsorganisation (IT-Security Policy/ Sicherheitsrichtlinie) sind die konzeptionelle Umsetzung der Vorgaben sowie die Realisierung der Maßnahmebündel und deren Wirksamkeit zu betrachten. Der Regelkreis von der Strategie über die Planung zur Umsetzung und Überwachung wird auch als IT-Sicherheitsprozess betrachtet.

Schritt 1:

Für die Revision ist also an erster Stelle die Prüfung der IT-Sicherheitsrichtlinie von Bedeutung. In ihr müssen verbindliche Regelungen der Unternehmensleitung getroffen werden, die sich auf folgende Bereiche erstrecken:

- Bedeutung der IT für das Unternehmen
- Berücksichtigung gesetzlicher Regelungen (insbesondere Datenschutzregelungen)
- Festlegung der Vorgehensweise zur Etablierung des Sicherheitsmanagementsystems
- Festlegung von Verantwortlichkeiten (IT-Sicherheitsorganisation)
- Kategorisierung des Schutzbedarfs für Informationen und IT-Systeme mit Festlegung der tolerierbaren Ausfallzeiten
- Regelungen zum Verfahren bei Verstößen gegen die Regelungen

Da in der Praxis insbesondere die strategischen Vorgaben häufig fehlen, möchte ich an dieser Stelle etwas stärker auf die revisionsrelevanten Punkte einer IT-Security Policy eingehen.

Die Beschreibung der Bedeutung der IT erfolgt individuell auf Basis der Abhängigkeit der Geschäftsprozesse von der IT-Unterstützung und dient in erster Linie der Sensibilisierung der Mitarbeiter.

Die Benennung wesentlicher gesetzlicher Regelungen dient der Veranschaulichung, der relevanten Normen, die zur Umsetzung bestimmter Maßnahmen zwingen und trägt so zur Akzeptanz einzelner Maßnahmen durch die Mitarbeiter und zur Schaffung klarer rechtlicher Rahmenbedingungen innerhalb des Unternehmens bei.

Die Festlegung der Vorgehensweise richtet sich sinnvollerweise an bereits in der Praxis etablierten Standards aus. Auf operativer Ebene hat sich das Vorgehensmodell nach dem IT-Grundschutzhandbuch bewährt und wird in immer mehr Unternehmen als Standard akzeptiert. Neben einem Vorgehensmodell werden auch praktische Hilfen und eine Referenz für Sollvorgaben für ein "Grundschutzniveau" angeboten. Der Umgang mit dem IT-Grundschutzhandbuch ist leicht zu erlernen und bietet dem Unternehmen die Möglichkeit, mit einem überschaubaren Berateraufwand eine umfassende Dokumentation zur IT-Sicherheit aufzubauen.

Die Organisationsstruktur sichert eine interdisziplinäre Zusammenarbeit und breite Fächerung des Themas **IT-Sicherheit**. Insbesondere für die Durchführung einer Schutzbedarfsfeststellung und der erforderlichen Kategorisierung von Informationswerten ist die Betrachtung von Fachpersonal außerhalb der IT-Abteilung nicht nur sinnvoll, sondern zwingend.

In der Praxis hat sich eine Unterteilung der IT-Sicherheitsorganisation in folgende Bereiche bewährt:

- Unternehmensleitung
- IT-Leitung
- IT-Sicherheitsbeauftragter (ggf. externer Dienstleister)
- Ressourcenverantwortliche (System-, Netzwerk- und Datenbankadministratoren)
- Informationsverantwortliche (Abteilungs- und/oder Gruppenleiter)

Eine Kategorisierung des Schutzbedarfs ermöglicht eine Schutzbedarfsanalyse der Informationswerte durch die Ressourcenverantwortlichen in Zusammenarbeit mit den Informationsverantwortlichen.

- Betrieblicher Datenschutzbeauftragter (ggf. externer Dienstleister).

Eine Kategorisierung des Schutzbedarfs ermöglicht eine Schutzbedarfsanalyse der Informationswerte durch die Ressourcenverantwortlichen in Zusammenarbeit mit den Informationsverantwortlichen. Hierbei werden die Informationswerte den abgestuften Schutzbedarfskategorien zugeordnet und deren Verfügbarkeitsanforderung festgelegt. Die Einstufung ist für die wirtschaftliche Bewertung der zum Schutz der Informationen umzusetzenden Maßnahmen von Bedeutung. Die Revision kann hier also auch zur Einhaltung der Wirtschaftlichkeit bei der Implementierung einzelner Schutzmaßnahmen beitragen.

Die Festlegung von Regelungen bei einem Verstoß gegen die von der Unternehmensleitung verabschiedeten Regelungen unterstreicht die Bedeutung der IT-Sicherheit für das Unternehmen. Insbesondere eine Darstellung der strafrechtlichen Konsequenzen, die sich bei einer Missachtung der Regelungen für die Mitarbeiter ergeben können, trägt zur Sensibilisierung bei. Aber nur durch die Durchführung von Kontrollen kann auch der ernsthafte Wille zur Durchsetzung der Vorgaben unterstrichen werden.

Liegt keine IT-Security Policy vor, wird es für die Revision ungleich schwieriger, die etablierten Maßnahmen zu bewerten. Mit fehlenden Vorgaben kann kein Soll/Ist-Vergleich durchgeführt werden. Hier ist der Hinweis auf die Anforderung einer transparenten und nachvollziehbaren Dokumentation der Auseinandersetzung mit IT-Risiken in Verbindung mit der möglichen Haftung der Unternehmensleitung oft Anlass für die Erarbeitung entsprechender Richtlinien.

Schritt 2:

Im zweiten Schritt sollte die Revision sich der Dokumentation des IT-Sicherheitskonzeptes widmen. Dabei werden folgende Punkte betrachtet:

- Umsetzung der strategischen Richtlinien
- Nachvollziehbarkeit der Dokumentation von Analysen und Untersuchungen
- Dokumentation des Handlungsbedarfs und Nachvollziehbarkeit der Entscheidungsgrundlagen zur Einführung einzelner Maßnahmen
- Schwerpunktbildung in Teilkonzepten (z.B. Notfallkonzept, Datenschutzkonzept, Datensicherungskonzept, Kryptokonzept etc.)

Bei der Realisierung der Maßnahmen ist neben der Einhaltung der Vorgaben durch die Unternehmensleitung auch die Einhaltung gesetzlicher Vorgaben zu prüfen.

- Verfahren zur Auswahl von Einzelmaßnahmen oder Produkte zur Erhöhung der IT-Sicherheit
- Realisierungsplanung unter Berücksichtigung der Priorität der Sicherheitsmaßnahmen und der wirtschaftlichen Gesamtsituation des Unternehmens

Zentrale Fragestellungen bei der Betrachtung der vorgenannten Punkte sind:

- Liegt eine nachvollziehbare Dokumentation vor, aus der die Entscheidungsfindung ersichtlich wird?
- Werden die gesetzlichen Anforderungen angemessen umgesetzt?

Schritt 3:

Bei der Realisierung der Maßnahmen ist neben der Einhaltung der Vorgaben durch die Unternehmensleitung auch die Einhaltung gesetzlicher Vorgaben zu prüfen. Bestimmte Protokollierungsfunktionen unterliegen der Mitbestimmung der Personalvertretung (Betriebsrat). Für bestimmte Nutzungsverbote sind ggf. betriebliche Vereinbarungen zu verfassen. Neben den rechtlichen Aspekten sollte sich die Realisierung aber auch nach der Priorisierung des IT-Sicherheitskonzeptes und den wirtschaftlichen Rahmenbedingungen richten.

Mögliche Revisionsfragestellungen sind:

- Werden die gesetzlichen Bestimmungen eingehalten? (z.B. Anbieterkennzeichnungspflicht beim Internetauftritt, Bestellung eines Datenschutzbeauftragten, Erstellung eines Verfahrensverzeichnisses für datenschutzrelevante Anwendungen mit Darstellung der Maßnahmen zur Datensicherheit im Sinne der Vertraulichkeit)
- Wurden Mitbestimmungsrechte der Personalvertretung beachtet? (z.B. beim Einsatz von SPAM-Filtern - soweit eine teilweise private Nutzung des e-mail-Dienstes nicht ausdrücklich verboten wurde und bei Protokollierungen von LAN-Aktivitäten)
- Wurden gesetzliche Haftungsregelungen bei der Formulierung und Festlegung bestimmter Organisationsanweisungen berücksichtigt? (z.B. Verbot der privaten Internetnutzung)
- Erfolgt die Auswahl sicherheitsrelevanter Produkte (z.B. Virenscanner, Firewall) entsprechend den Qualitätsanforderungen des Bedarfsträgers? (z.B. objektive Entscheidungsfindung auf Basis nachvollziehbarer Auswahlkriterien)

Die Überwachung des IT-Sicherheitsprozesses sollte stets unabhängig von den unmittelbar am Sicherheitsprozess beteiligten Akteuren erfolgen.

Schritt 4:

Die Überwachung des IT-Sicherheitsprozesses sollte stets unabhängig von den unmittelbar am Sicherheitsprozess beteiligten Akteuren erfolgen. Nur eine unabhängige Überwachung stellt eine objektive Beurteilung der Wirksamkeit sicher. Einzelne Sicherheitskontrollen am Arbeitsplatz von Mitarbeitern oder die Durchführung von Notfallübungen können dabei natürlich durch die IT-Sicherheitsorganisation durchgeführt werden. Die Auswertung der Kontrollergebnisse sollte aber durch die Revision erfolgen. Das Ziel der Prüfungen ist eine Aussage zum Sicherheitsmanagement selbst. Aber auch die Prüfung einzelner Entscheidungsfindungsprozesse anhand der Qualitätsstandards im Unternehmen ist möglich.

Werden regelmäßig Übungen für das Zusammenspiel der IT-Sicherheitsorganisation durchgeführt?

Fragestellungen der Revision können sein:

- Erfolgt das Zusammenspiel der Sicherheitsorganisation im Sinne der Vorgaben der Unternehmensleitung? (z.B. Kommunikation zwischen den Akteuren)
- Werden regelmäßig Übungen für das Zusammenspiel der IT-Sicherheitsorganisation durchgeführt? (z.B. Notfallübungen, Planspiele zur Prüfung von Meldewegen und Reaktionszeiten)
- Wie werden Entscheidungsfindungsprozesse innerhalb der Sicherheitsorganisation beeinflusst? (z.B. unabhängige Produkteinführung bei Einsatz externer Berater)

Die Erreichung der klassischen Ziele der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) ist die Voraussetzung für die Datensicherheit im Sinne der GoB (Verfügbarkeit und Integrität) und des Datenschutzes (Vertraulichkeit).

Fazit

Die Erreichung der klassischen Ziele der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit) ist die Voraussetzung für die Datensicherheit im Sinne der GoB (Verfügbarkeit und Integrität) und des Datenschutzes (Vertraulichkeit). Die Zielsetzungen und Verfahren eines modernen IT-Sicherheitsmanagements decken die gesetzlichen Anforderungen an die Verarbeitung rechnungslegungsrelevanter und personenbezogener Daten ab. Die Revision muss sich daher dem Thema IT-Sicherheit stellen und das Sicherheitsmanagement im Unternehmen verstärkt zum Prüfungsobjekt machen. ✣

➲Die Midlife-Crisis des Mainframe

Noch weit vom Rentenalter entfernt stellt der Mainframe nach wie vor das Rückgrat zahlreicher Unternehmen dar. Aber mit breiteren Zugriffsmöglichkeiten und strikteren Vorschriften bedarf er dringend einer besseren Abschirmung.

Thomas-Daniel Schmidt
RheinLand Versicherungen

VOR ZWANZIG JAHREN befanden sich Mainframes noch sicher in abgeschlossenen Glashäusern, und nur eine begrenzte Anzahl Mitarbeiter konnte darauf zugreifen. Heutzutage sind Mainframes nach wie vor eine Stütze der Betriebsabläufe des Unternehmens. Alle Prognosen über ein unmittelbar bevorstehendes Ende der Mainframes sind genauso schnell verschwunden wie diejenigen über das Ende des traditionellen ("brick-and-mortar") Handels. Tatsächlich schätzen Branchenquellen, dass täglich 30 Mrd. COBOL-Transaktionen verarbeitet werden - das ist mehr als die gesamte Anzahl aller möglichen Webseiten-Treffer.

In den Unternehmen der heutigen Zeit haben die Mainframes ihre Glashäuser zerbrochen und sind über eine Vielzahl von Netzwerkdiensten zugänglich. Zusätzlich zu den konventionellen Benutzern der zentralen CICS- oder IMS-basierten Transaktionen verlagern große Unternehmen (wie zahlreiche Finanzdienstleister) Anwendungen von Intel auf Linux auf dem Mainframe, um Kosten zu sparen und Performance und Zuverlässigkeit zu erhöhen. Und Web-basierte Anwendungen, die auf der Linux- oder UNIX-Umgebung auf dem Mainframe untergebracht sind, ermöglichen Millionen Kunden den Zugriff auf die zentralen, für den Geschäftsablauf erforderlichen Transaktionsdaten.

Bei einem derart umfangreichen Datenverkehr von so vielen Quellen - und einer neuen Generation von Verordnungen, die auf die Privatsphäre der Kunden und die Sorgfalt der Unternehmen ausgerichtet sind - ist es höchste Zeit, dass Unternehmen sich erneut Gedanken darüber machen, wie sie den Mainframe schützen können.

Verdrossenheit, Unerfahrenheit und Selbstüberschätzung schaden der Sicherheit.

Isoliert, in begrenzter Vernetzung mit der Außenwelt, waren Mainframes stets relativ einfach zu verwalten und zu schützen. Es war nicht ungewöhnlich für Unternehmen, sprichwörtlich einen Mainframe-Techniker pro Benutzer zu haben. Mittlerweile sprechen wir eher von einem Techniker pro 1.000 Benutzer. Dies hat zur Folge, dass erfahrene Mainframe-Spezialisten überlastet und schwer zu finden sind. Man kann nicht einfach

einen Firewall-Administrator einsetzen und erwarten, dass er sich durch einen Wirrwarr von Anwendungen und Dienstprogrammen findet, die geschrieben wurden, bevor er überhaupt geboren wurde.

Zusätzlich zur verstärkten Vernetzung und zum fehlenden und unzureichend ausgebildeten Personal stellen unter anderem Selbstgefälligkeit und Selbstüberschätzung die größten Gefahren für die Mainframe-Sicherheit dar. Die meisten Unternehmen gehen davon aus, dass Mainframes sicher sind, nur aufgrund ihrer Glashaus-Vergangenheit. Eine europäische Großbank, die sich ihrer Mainframe-Sicherheit rühmte, machte es bei vielen Anwendungen auf dem Mainframe relativ einfach für einen Insider, in das System einzudringen und es zu missbrauchen. Vertrauliche Daten könnten kopiert, gelöscht und alle Spuren dieser Aktivität verwischt werden.

Mainframes sind insbesondere anfällig für die drei folgende Gefahren:

- Böswilliger Datenzugriff:
  Hacker und "vertrauenswürdige" Benutzer haben ein erhöhtes Potential, um auf das zentrale Daten-Repository des Mainframe wie auf jede andere Plattform zuzugreifen. Sarbanes-Oxley, HIPAA, GLBA und andere Standards weisen alle auf die Notwendigkeit hin, Datenzuverlässigkeit und -integrität zu schützen. Der Mainframe darf hiervon nicht ausgenommen werden.
- Selbstverursachte Fehler:
  Eine ganze Generation von Mainframe-Meistern geht in Kürze in Rente, und weniger qualifizierte oder erfahrene Techniker (vielfach unter Zeitdruck oder überlastet) können unbeabsichtigt Code oder Einstellungen ändern und dadurch Zugangsmöglichkeiten schaffen oder zu weitreichende Zugriffsberechtigungen auf das System erteilen.
- Veraltete Software:
  Die Stärke des Mainframe liegt darin, dass sie ohne übermäßigen Wartungsaufwand nach wie vor die alte, zuverlässige, Software von früher ausführen können. Aber auch Mainframe-Software benötigt Kontrollen, Patches und aktuelle Software, um Lücken zu schließen oder einfach die Sicherheit zu erhöhen.

Unternehmen müssen tief Luft holen und damit beginnen, die am besten geeigneten traditionellen Sicherheitspraktiken auf den Mainframe anzuwenden. Hier eine kurze Checkliste der Praktiken, welche die Sicherheit der Mainframes dramatisch verbessern:

- **Mainframe-Sicherheits-Dashboard** installieren. Mit weniger Personal und täglich zunehmenden Bedrohungen müssen Unternehmen ein Mainframe-Sicherheits-Dashboard installieren, aus dem der Fortschritt der Sicherheitsinitiativen ersichtlich wird. Das Dashboard sollte eine Übersicht darüber bieten, wer auf die Mainframe-Daten zugreift, auf welche Datengruppen am häufigsten zugegriffen wird, und - vorzugsweise - ob ein Zugriff Ihre Sicherheitsmaßnahmen verletzt. Darüber hinaus geben Ihnen Übersichten über die Anzahl der Benutzer, die hinzugefügt und entfernt wurden, die Anzahl ruhender Benutzerkonten und Informationen über die schwächsten Passwörter die Sicherheit, dass Ihr Mainframe-Sicherheitsteam die Sache im Griff hat.
- **Geschickte Zentralisierung**. Sie müssen Ihre verfügbare Mainframe-Wissensbasis besser nutzen, indem Sie einen Teil der Sicherheitsfunktionen - insbesondere Administration und Überprüfung - auf weniger spezialisierte Ressourcen zentralisieren. Das kann mit Hilfe "idiotensicherer" Mainframe-Software oder mit unternehmensweiten Systemen erfolgen, welche die auf Rollen basierte und durch Richtlinien gesteuerte Versorgung von Benutzern sowie die unternehmensweite Überprüfung von Dateizugriff und Konfigurationen ermöglichen. Die Expertise Ihrer Mainframe-Experten sollte besser ge-

nutzt werden, indem Ihr zentrales Sicherheitsteam und der Help Desk zahlreiche der alltäglichen Aufgaben, wie Überprüfung und Verwaltung des Mainframe, übernehmen, die sie auch für die offenen Systeme durchführen.

- **Verstärkte Kontrollen**. Viele Kunden, die ich besuche, sind stolz auf die Anzahl der Zugriffsverletzungen, die sie durch Beobachtung fehlgeschlagener Anmeldungen und Datenzugriffe verhindern konnten. Aber was ist mit denjenigen, die sie nicht verhindern konnten, das heißt, die Mehrzahl? Sorgen Sie dafür, dass die Protokollierung von Mainframe-Betriebssystemen und darauf befindlichen Anwendungen ordnungsgemäß konfiguriert ist, um sicherzustellen, dass Sie verfolgen können, wer auf welche Daten zugegriffen hat. Sehen Sie sich dann systematisch die Schlüsseldateien (Datensets) an, insbesondere diejenigen, die unter gesetzliche Verordnungen fallen, wie Sarbanes-Oxley, GLBA oder HIPAA, und stellen Sie sicher, dass Ihre Maßnahmen befolgt werden. Automatisierte Tools, mit denen eine derartige Überwachung durchgeführt werden kann, ermöglichen diese Art der Routine-Überprüfung auch ohne eine ganze Armee von Administratoren.
- **Verstärkte Kontrollen**. Sehen Sie zu, dass die Sicherheitskontrollen auf dem Mainframe verbessert werden. Warnmeldungen über Zugriffsverletzungen oder Fehlkonfigurationen in Echtzeit sind eine Überlegung wert. Sie haben derartige Einbruchserkennungssysteme auf dem offenen System installiert; stellen Sie sicher, dass Sie in Ihre Mainframe-Sicherheit ein ähnliches Vertrauen haben können. Gleichermaßen sollten Sie sicherstellen, dass Sie über Lösungen verfügen, welche die Fehler verhindern können, die von den weniger erfahrenen und weniger technischen Mitarbeitern begangen werden, die Sie beschäftigen müssen, um die Verwaltungsaufgaben des Mainframe zu übernehmen. Schließlich sollten Sie sicherstellen, dass Ihre Verwaltungs- und Prüffunktionen tatsächlich unabhängig voneinander sind und als Gegenseitigkeitskontrolle dienen.

Auch wenn Sicherheitsbedrohungen für den Mainframe lange nicht so glamourös sind wie viel beschriebene Viren oder Würmer, stellen sie doch eine ernste Bedrohung für die unternehmenskritischen Dienste und Informationen dar, die typischerweise im Glashaus angesiedelt sind. Die gute Nachricht lautet, dass sich die Technologien zur Überwachung der Sicherheit weiterentwickelt haben und auch die einfacheren der oben beschriebenen Maßnahmen können die Mainframe-Sicherheit enorm verbessern, ohne dass ein Vermögen für Personal oder Software ausgegeben werden müsste.

Zusätzliche Softwareprodukte wie RACF von IBM, ACF2 und TOP SECRET von Computer Associates bieten die Möglichkeit, durch ihren organisierten Einsatz die Sicherheit für den Mainfraime zu erhöhen.

Das Sicherheitsniveau des Mainfraime festzustellen und Maßnahmen zu beschreiben, um vom Ist- zum Sollzustand zu gelangen, ist eine wichtige - aber bisher oft nicht durchgeführte - Aufgabe der IT-Revision.

Im neuen Seminarkatalog 2005/2006 der Firma IBS Hamburg finden Sie ein speziell auf die IT-Revision abgestimmtes Seminar zum Thema "RACF". Dieses Seminar wird abgerundet durch einen praxisorientierten Teil, d.h. jeder Seminarteilnehmer kann in einem RACF-System arbeiten und das erworbene Wissen direkt testen.

Zudem werden Produkte der Firma Consul risk management vorgestellt, die den Umgang mit z.B. RACF für Administratoren, aber auch speziell für Revisoren vereinfachen. Dies sind spezielle Administrationswerkzeuge sowie Security Event Management Systeme in denen RACF nur ein Baustein ist.

➲ Archivierung: Notwendiges Übel oder Beitrag zur Verhinderung von Datenmüll?

Dr. sc.
G. W. Wähner
Berlin

HGB und AO, ergänzt durch die GDPdU sowie die GoBS, regeln recht eindeutig die Archivierung von Daten im kaufmännischen Anwendungsbereich (vgl. Quellenverzeichnis). Trotzdem gibt es in der betrieblichen Praxis nach wie vor in größerem Umfange Unkenntnis bezüglich der geltenden gesetzlichen Anforderungen bzw. Unsicherheit bei ihrer Auslegung. Die Folge dieser Defizite sind oft gravierende Verstöße gegen gesetzliche Anforderungen oder kostspielige Anhäufungen von Datenmüll oder auch beides.

Dieser Beitrag vermittelt einen Lösungsansatz, mittels dessen sich die Archivierung sowohl nicht codierter als auch codierter Daten auf das aus den externen Anforderungen resultierende Minimum reduzieren lässt, verbunden mit der Einsparung von Kosten in beträchtlichem Umfange.

1 Häufig anzutreffende Schwachstellen im Bereich der Archivierung

Im Rahmen seiner Prüfer- und Beratertätigkeit ist der Autor wiederholt auf folgende Schwachstellen gestoßen:

- Es werden Daten gelöscht, die im Rahmen der Beleg- und Journalfunktion der Archivierungspflicht unterliegen, darunter "originäre digitale Unterlagen", die gemäß GDPdU zu archivieren sind.
- Es erfolgt die mehrfache Archivierung gleicher Archivierungsobjekte, beispielsweise von Eingangsrechnungen sowohl im Einkauf als auch in Controlling und Buchhaltung oder von Ausgangsrechnungen sowohl im Vertrieb als auch in Controlling und Buchhaltung.
- Daten werden ohne eindeutige Vorgaben bezüglich Archivierungsform, Archivierungsfrist, Anforderungen an die Wiederherstellung aufbewahrt, weil der Archivierung kein eindeutiger Auftrag zu Grunde lag, der alle erforderlichen Festlegungen enthielt.
- In mehr als einem Fall wurden in Größenordnungen Altlasten von auf magnetischen Datenträgern archivierten Datenbeständen vorgefunden. Diese Datenbestände waren herrenlos, d.h., es ließ sich kein Dateneigner mehr ermitteln, weil der Zusammenhang zwischen den technischen Ordnungsmerkmalen der Speicherung (Name des Jobs, der die Datei erzeugt hat, Dateiname, Datum der Erstellung der Datei, Sperrfrist etc.) und ihren sachlich-inhaltlichen Merkmalen (Anwendungssystem, Dateneigner, Belegart, Buchungsperiode, gesetzliche Archivierungsfrist etc.) nicht mehr hergestellt werden konnte. Folge: Tausende Magnetbandkassetten wurden seit mehr als 10 Jahren mit archivierten Daten unter Nutzung modernster Archivierungstools "mit offenem Ende" aufbewahrt, gesichert und gepflegt. Hier ist wohl der Ausdruck **Datenmüll** zutreffend.

- "Um sicher zu gehen" erfolgt die Archivierung von Objekten, die weder aus internen, noch aus externen (gesetzlichen) Anforderungen heraus archiviert werden müssten.
- Daten werden unter Verweis auf gesetzliche Vorgaben gelöscht, obwohl andere, übergeordnete gesetzliche Vorgaben deren Archivierung fordern. Beispiel: Nach dem BDSG sind personenbezogene Daten zu löschen, wenn der Zweck ihrer Erfassung, Speicherung und Verarbeitung erfüllt ist. Handelt es sich dabei jedoch um steuerlich relevante Daten, wie beispielsweise Debitoren- oder Kreditorenstammdaten für natürliche Personen, Einzelnachweise für Kunden von Telefongesellschaften, Internet-Providern etc. sind sie nicht zu löschen, sondern gemäß HGB und AO sechs bzw. zehn Jahre zu archivieren.

In den genannten Fällen handelt es sich ausschließlich um die Auswirkungen von ausgeprägten organisatorischen und technologischen Defiziten im jeweiligen Verantwortungsbereich. Diese gehen meist auf zwei Ursachenbereiche zurück:

1. Es fehlen wesentliche organisatorische Grundlagen für eine gesetzeskonforme und dabei kostenminimierte Archivierung, wie
   - eine brauchbare Aufstellung und Klassifikation aller im Anwendungsbereich relevanten Archivierungsobjekte,
   - eine Archivordnung, welche den Lebensweg eines Archivierungsobjektes, vom Datenanfall bis zur expliziten Freigabe und Löschung/Vernichtung, verbindlich fixiert,
   - Organisationsmittel, welche a priori für jeden einzelnen Archivierungsvorgang sicher stellen, dass alle sowohl für den Fachbereich als auch den DV-Bereich erforderlichen Vorgaben erteilt werden, einschließlich der wichtigen Vorgaben bzw. Anforderungen an die Rekonstruktion/Wiederherstellung im Bedarfsfalle, deretwegen ja genau genommen archiviert wird.
2. Es fehlen Verfahren zur professionellen Kontrolle, Freigabe, Vernichtung von Archivierungsobjekten nach Ablauf der Archivierungsfristen. Diese müssen insbesondere sicherstellen, dass der Zusammenhang zwischen dem sachlich-fachlichen Inhalt der Daten und den technischen Merkmalen der Speicherung niemals verloren geht.

Genaue Vorgaben an die inhaltlich zuständigen Fachbereiche reichen erfahrungsgemäß für eine derartige Bestandsaufnahme nicht aus.

2 Lösungsansatz

2.1 Bestandsaufnahme und Klassifikation von Archivierungsobjekten

Am Beginn einer ganzheitlichen Lösung zur Archivierung sowohl nicht codierter als auch codierter Daten sollte immer die möglicht vollständige Aufnahme und Klassifikation aller im jeweiligen Anwendungsbereich vorhandenen Daten stehen. Das sollte nach Fachbereichen getrennt erfolgen, beispielsweise Finanzbuchhaltung, Personalwesen, Vertrieb, Einkauf und Controlling.

Genaue Vorgaben an die inhaltlich zuständigen Fachbereiche reichen erfahrungsgemäß für eine derartige Bestandsaufnahme nicht aus. Natürlich kennen die Mitarbeiter des Fachbereiches am besten relevante Daten und Systemumfeld, in dem diese erzeugt und/oder verarbeitet werden. Die Zuordnung der Datenbestände und ihrer unterschiedlichen Ausprägungen zu den abstrakten Kategorien von archivierungspflichtigen Objekten gemäß HGB, AO oder GDPdU überfordert aber erfahrungsgemäß den einzelnen Mitarbeiter des Fachbereiches.

Eben diese Zuordnung der spezifischen Ausprägung eines Datenobjektes in seiner System-

umgebung zu dem in HGB und AO genannten aufbewahrungspflichtigen Unterlagen ist aber der Schlüssel zur Bestimmung von Archivierungsfristen, Archivierungsformen und Anforderungen an die Wiederherstellung. Deshalb bietet es sich an, diese und weitere Aufgaben durch diesbezüglich geeignete Mitarbeiter im Rahmen eines Projektes lösen zu lassen.

Im Rahmen der Projektarbeit sind zunächst folgende drei Arbeitsschritte zu realisieren:

1. Aufnahme aller relevanten Archivierungsobjekte (nicht codierte und codierte).
2. Ordnung der aufgenommenen Objekte nach Datenträger-Art, Archivierungsfrist, Zugriffsanforderungen und anderen für den Archivierungsprozess benötigten Ordnungsmerkmalen.
3. Aufbereitung / Dokumentation der Ergebnisse je Sachgebiet in tabellarischer Form.

Abb. 1 zeigt eine derartige Tabelle mit Archivierungsobjekten nicht codierter Art aus dem Bereich Finanzbuchhaltung (aufgenommen im Umfeld eines SAP R/3 Systems).

Die Tabelle enthält je Archivierungsobjekt folgende Merkmale:

a) Bezeichnung des Archivierungsobjektes im Anwendungsumfeld
b) Art des Datenträgers, z.B. Formular, Druckliste/Report, Papierbeleg, Datei, Datenbanktabelle u.a.
c) Externe und/oder interne Archivierungsfrist (in Jahren, beginnend mit dem 01.01. des Folgejahres nach Erzeugung/ Anfall)
d) Ursprung des Datenträgers bzw. der Daten (Quelle)
e) Ort der Aufbewahrung (im Beispiel Registratur der Finanzbuchhaltung)
f) Organisationsmerkmale/ Sortiermerkmale für eine geordnete Ablage (im Beispiel Belegnummer, Datum, Kontenbereich u.a.)
g) Aufbewahrungszeitraum im Fachbereich bis zur Abgabe ans Archiv
h) Anzahl der Exemplare eines Objektes und deren Verteilung
i) Datenanfall (DA = Anzahl Ordner, GB = GigaByte) pro Geschäftsjahr
j) Periodizität des Datenanfalls

2.2 Erarbeitung einer Archivordnung für nicht codierte Daten

Das Beispiel gemäß Abb. 1 enthält ausschließlich nicht codierte Daten, also Schriftgut in Papierform, Primärbelege, Drucklisten, Reports u.a. Deren ordnungsgemäße Archivierung erfordert im kaufmännischen Anwendungsbereich lediglich einiger ablauforganisatorischer Festlegungen. Das erfolgt am Besten in der Form einer einheitlichen, bereichsübergreifenden Archivordnung. In diese können neben grundsätzlichen Festlegungen zur Archivierung erfahrungsgemäß auch gut die wenigen bereichsspezifischen Anforderungen aufgenommen werden.

Die gemäß Abschnitt 2.1 erstellten und einem zuverlässigen Änderungsdienst zu unterwerfenden Tabellen bilden den Kern einer derartigen Archivordnung. In dieser ist vor allen Dingen der äußere, durch Organisation bestimmte Ablauf des Archivierungsprozesses zu regeln, und zwar in allen seinen Phasen, also

- beginnend bei der Erfassung und Klassifikation neuer Archivierungsobjekte, einschließlich des erforderlichen Änderungsdienstes,
- über die laufende Kennzeichnung, Verwaltung und Pflege anfallender Archivierungsobjekte, die Nachweisführung über den Archivbestand und die Kontrolle der Archivierungsfristen,
- über die Bereitstellung bzw. Wiederherstellung von Archivierungsobjekten zu Prüfungs- und Kontrollzwecken
- bis hin zur ordnungsgemäßen Freigabe und Vernichtung jener Archivierungsobjekte, deren Aufbewahrungsfristen abgelaufen sind.

Aus diesen Anforderungen ergibt sich folgende Struktur einer Archivordnung:

1 Gegenstand der Archivordnung
2 Geltungsbereich

3 Klassifikation des Archivgutes
4 Verantwortlichkeit
5 Ablage- und Archivorganisation
5.1 Organisation der Ablage von Schriftgut im Fachbereich
5.1.1 Kennzeichnung der Ordner und Drucklisten
5.1.2 Aufbewahrung und Ablageorganisation im Fachbereich
5.1.3 Auslagerung des Schriftgutes in das Archiv
5.2 Verwaltung des Archivs
5.2.1 Zugangsregelung
5.2.2 Nachweisführung
5.2.3 Kennzeichnung des Schriftgutes
5.2.4 Einordnung des Schriftgutes
5.2.5 Vernichtung des Schriftgutes in Verantwortung des Fachbereiches
6 Bereichsübergreifende Festlegungen
6.1 Aktualisierung der Archivordnung
6.2 Kontrolle der Einhaltung der Archivordnung

(Hinweis: Das Beispiel einer vollständigen Archivordnung findet sich in WÄH02, Abschnitt 3.2.5.).

2.3 Bestimmung und Klassifizierung zu archivierender codierter Daten

Bei der Bestimmung und Klassifizierung zu archivierender codierter Daten gilt es zwischen drei Gruppen von Datenbeständen zu unterscheiden:

1. Daten, die sich direkt den in § 257 HGB und § 147 AO genannten Kategorien zuordnen lassen
2. Daten, die sich nicht den in HGB und AO genannten Kategorien zuordnen lassen, aber bei Einsatz "DV-gestützter Buchführungssysteme" gemäß GoBS oder anderen Regelwerken archivierungsrelevant sind
3. Originär digitale Unterlagen im Sinne der GDPdU

Zu 1.

HGB und AO gestatten es bis auf wenige Ausnahmen Archivierungsobjekte statt in Papierform in codierter Form aufzubewahren. Im § 257 HGB heißt es:

"Mit Ausnahme der Eröffnungsbilanzen, Jahresabschlüsse und der Konzernabschlüsse, die gemäß § 257 HGB und § 147 AO können die in Abs. 1 aufgeführten Unterlagen auch als Wiedergabe auf einem Bildträger oder anderen Datenträger aufbewahrt werden, wenn dies den Grundsätzen ordnungsgemäßer Buchführung entspricht und sichergestellt ist, daß die Wiedergabe oder die Daten

- mit den empfangenen Handelsbriefen und Buchungsbelegen bildlich und mit anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden,
- während der Dauer der Aufbewahrungsfrist verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können."

Daraus ergibt sich für die Archivierung von Daten in codierter Form folgende, im Vergleich zu den nicht codierten Daten (Papierform) erweiterte Zielsetzung:

a) Gewährleistung der Einhaltung gesetzlicher Archivierungsanforderungen
b) Gewährleistung der Einhaltung interner Archivierungsanforderungen
c) Realisierung einer vom Aufwand her günstigeren Form der Archivierung, im Vergleich zur Archivierung in nicht codierter Form
d) Gewährleistung einer rationellen Verwaltung des Archivbestandes (Nachweisführung, Pflege, Sicherung, Freigabe, Löschung usw.) und eines schnellen Zugriffs auf Archivobjekte
e) Erhöhung der Performance des EDV-Systems und Reduzierung des Bedarfes an Plattenplatz durch Auslagerung älterer Datenbestände

Die ersten beiden Ziele sind mit denen der Archivierung nicht codierter Daten identisch, während die drei Letztgenannten Rationalisierungsziele darstellen.

Zu 2.

Bei diesen Daten, die primär in Dateiform oder als Datenbanktabellen vorliegen, handelt es sich beispielsweise um folgende:

- Protokolle über abgebrochene Verbuchungen u.a.
- Bestandteile der gemäß GoBS, Abschnitt 6, zu führenden Verfahrensdokumentation
- Stammdaten und Stammdatenänderungen
- Benutzerstammsätze (einschließlich Historie)
- Zugriffsrechte der Benutzer (einschließlich Historie)
- Job-Protokolle , Batch-Input-Protokolle, Transportprotokolle u.a.
- Fehlerprotokolle / Fehler-Logs
- System-Logs und andere Dateien mit Aufzeichnungen über den Verarbeitungsablauf und seine Ergebnisse (wie Ergebnisse maschineller Abstimmungen und Kontrollen).

Zu 3.

Im Zuge der Verabschiedung des Steuersenkungsgesetzes (StSenkG) wurde die Abgabenordnung unter anderem hinsichtlich der Ordnungspflichten für die Buchführung und für Aufzeichnungen (§ 146) sowie der Ordnungspflichten für die Aufbewahrung von Unterlagen (§ 147) geändert. Die weitergehenden Rechte der Finanzbehörde und Archivierungsanforderungen wurden mit BMF-Schreiben vom 16. Juli 2001 - IV D2 - S0316 -136/02 - unter dem Titel "Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)" veröffentlicht.

Der Sinn dieser Vorgabe ist klar: Steuerlich relevante Daten, die "originär digital" anfallen...

Abschnitt III der GDPdU formuliert neue, weitgehende Anforderungen an die Archivierung digitaler Unterlagen. Uns interessiert im gegebenen Zusammenhang die Anforderung, originär digitale Unterlagen nach § 146 Abs. 5 AO (d.h."Bücher und die sonst erforderlichen Aufzeichnungen") auch digital (d.h."auf maschinell verwertbaren Datenträgern") zu archivieren.

Der Sinn dieser Vorgabe ist klar: Steuerlich relevante Daten, die "originär digital" anfallen, beispielsweise

- Eingangsrechnungen in der Form einer EDIFACT-Nachricht vom Typ "INVOICE",
- maschinell erzeugter Buchungsbelege oder auch
- Rechnungseingangs-, Rechnungsausgangs- oder Belegkompaktjournale

sind nicht bzw. nicht nur in ihrer im Ergebnis mehrerer Verarbeitungsschritte entstehenden transformierten bzw. visualisierten Form zu archivieren, also als interner Buchungsbeleg oder ausgedrucktes Journal, sondern in ihrer primären, originären, digitalen Form.

Nur so lässt sich im Bedarfsfalle ein Geschäftsvorfall im Sinne der gemäß HGB und AO zu gewährleistenden Belegfunktion tatsächlich von der Datenquelle bis zu Datensenke über alle Transformations- und Bearbeitungsstufen verfolgen.

Ob das tatsächlich erforderlich und derzeit für die Finanzbehörden praktikabel ist, sei dahingestellt.

Jedenfalls ist offensichtlich, dass auch im Bereich der codierten Daten kein Weg an der sorgfältigen und vollständigen Erfassung und Klassifikation vorbeiführt. Methodisch kann das wie im Abschnitt 2.1 und 2.2 anhand nicht codierter Daten dargestellt erfolgen.

Bezogen auf Daten der ersten Gruppe, die auch in ihrer spezifischen codierten Form eindeutig auf ihre Beleg-, Konten- oder Journalfunktion gemäß HGB und AO zurückgeführt werden können, ist das sicher kein Problem:

- Ein Beleg bleibt ein Beleg, egal welche Transformationen er bezüglich Datenträger und Format in den Phasen der Erzeugung, Übertragung, Konvertierung, Verarbeitung, Speicherung und Archivierung auch annimmt.
- Ein Journal bleibt ein Journal, egal ob es periodisch ausgedruckt und in Papierform archiviert wird oder ob es - unter Zugriff auf die Belegdatei - nur bei Bedarf aufbereitet und ausgegeben wird.

Die Archivierungsfristen bleiben gleich, die Anforderungen

und Möglichkeiten an die Wiederherstellung sind allerdings grundlegend anders und wesentlich komplexer.

Bei den Daten der zweiten Gruppe, die im Kontext der GoBS archivierungsrelevant sind, gibt es mangels Eindeutigkeit der Vorgaben eine Grauzone oder - positiv ausgedrückt - einen Interpretationsspielraum, innerhalb dessen Notwendigkeit, Nützlichkeit und vertretbarer Aufwand angemessen berücksichtigt werden können.

Bewährt haben sich einvernehmliche Festlegungen, die durch Fachbereich, DV-Bereich, Revision und Wirtschaftsprüfer gleichermaßen getragen werden.

Bleiben die Daten der dritten Gruppe, die "originär digitalen Unterlagen". Diese Gruppe ist in den meisten Anwendungsbereichen zumindest derzeit noch nicht relevant oder es handelt sich um wenige, sicher bestimmbare Objekte. Sie existieren hauptsächlich im Bereich EDI- oder Internet-basierter Teilsysteme, die dem Buchführungssystem vorgelagert sind.

In grober Differenzierung ergeben sich für codierte Daten aus allen drei Bereichen folgende Archivierungsfristen:

- Handelsbücher (Journale) und Buchungsbelege: 10 Jahre (vgl. HGB §238 Abs. 1)
- Handelsbriefe: 6 Jahre (vgl. HGB § 257 Abs. 4)
- Stammdaten Debitoren, Kreditoren, Sachkonten: Wie Buchungsbelege, auf die sie sich beziehen, also 10 Jahre
- Bestandteile der Verfahrensdokumentation: 10 Jahre (vgl. GoBS, Abschnitt 6 und 7)
- Sonstige revisionsrelevante Daten, wie Job-Protokolle, Logs: Nicht explizit geregelt (sinnvoller Weise 12 bis 18 Monate)
- Histories: Bis auf Stammdaten (siehe oben) nicht explizit geregelt (sinnvoller Weise nur solange, wie für Fehlersuche, Nachvollzug, Rekonstruktion erforderlich)

Nach Bestimmung und Klassifikation der zu archivierenden codierten Daten ist die erforderliche Archivorganisation und Technologie zu bestimmen und auszugestalten.

2.4 Archivorganisation und -technologie für codierte Daten

Archivorganisation und -technologie für codierte Daten müssen nicht nur den einmaligen Vorgang der Archivierung, sondern vor allen Dingen die Rekonstruierbarkeit dieser Daten über den gesamten Archivierungszeitraum zuverlässig gewährleisten. Rekonstruierbarkeit jedoch ist ein vager Begriff, der im Zusammenhang mit der Archivierung jedes einzelnen Objektes zu präzisieren ist.

In Abhängigkeit von den zeitlichen und inhaltlichen Anforderungen an die Rekonstruierbarkeit hat der Dateneigner zu entscheiden, ob nur die Daten selbst oder zusätzlich sonstige codierte Informationen zusammen mit den Daten zu archivieren sind.

In Abhängigkeit von den zeitlichen und inhaltlichen Anforderungen an die Rekonstruierbarkeit hat der Dateneigner zu entscheiden, ob nur die Daten selbst oder zusätzlich sonstige codierte Informationen zusammen mit den Daten zu archivieren sind.

Die Anwendungssysteme, mit denen die archivierten Daten erstellt wurden und das EDV-Umfeld (Hardware, Betriebssysteme, Verarbeitungstechnologien u.a.) sind in der Regel innerhalb der Archivierungsfrist Veränderungen unterworfen. Daraus folgt, dass eine Wiederherstellung der archivierten Daten in der ursprünglichen Anwendungsumgebung oft nicht mehr oder nur eingeschränkt möglich sein wird und in jedem Falle mit einem hohen Rekonstruktionsaufwand verbunden wäre.

Bewährt hat sich in vielen Fällen folgender praktikabler Ansatz:

- Davon ausgehend, dass bei den meisten der im vorangegangenen Abschnitt aufgezählten codierten Archivierungsobjekten im Geltungsbereich der GoBS eine Re-

konstruktion zum Zwecke der Nachweisführung sehr unwahrscheinlich ist, werden zur Reduzierung des Aufwandes nur die archivierungspflichtigen Daten selbst archiviert. Das geschieht in dem Wissen, dass sich die Rekonstruktionsfähigkeit dann auf die physische Rekonstruierbarkeit der Daten reduziert.
Physische Rekonstruierbarkeit heißt in diesem Falle, dass zwar die Lesbarkeit des Datenträgers und die "einfache Visualisierbarkeit" (Umwandlung und Ausdruck mit Hilfe von Dienstprogrammen) gewährleistet werden kann, nicht aber eine Bereitstellung der Daten in der ursprünglichen Anwendungsumgebung, verbunden mit allen diesbezüglichen Auswertungsmöglichkeiten.

- Sofern durch den Dateneigner weitergehende Anforderungen an die Revisionsfähigkeit und Wiederherstellung der archivierten Daten gestellt werden, sind auch Bestandteile des "Verfahrens" selbst, also des Betriebssystems, des Datenbanksystems, der Laufzeitumgebung (Bibliotheken, Steuerparameter etc.) mit zu archivieren, und zwar jeweils mit dem zum Zeitpunkt der Archivierung gültigen Stand.
  Diese erweiterte Form der Archivierung bedingt einen sehr großen Aufwand und bedarf deshalb der besonderen Begründung. Von der gelegentlich anzutreffenden Praxis, in Unkenntnis des technologischen Hintergrunds, des Aufwandes und der gesetzlichen Anforderungen, derartige Forderungen zu stellen oder Empfehlungen auszusprechen, sollte deshalb Abstand genommen werden.

Bei der Archivierung und Rekonstruktion codierter Daten handelt es sich um einen komplexen Prozess, an dem arbeitsteilig mehrere Struktureinheiten beteiligt sind. In derartigen Fällen bietet es sich von der Form und Methode her an, die erforderlichen Festlegungen in einer Verfahrensanweisung zu treffen.

Die Struktur einer Verfahrensanweisung zur Archivierung codierter Daten, im Sinne der Aufgabenbereiche, zu denen eindeutige, verbindliche und kontrollfähige Festlegungen zu treffen sind, könnte wie folgt aussehen:

1. Erteilung des Auftrages zur Archivierung

   Ein interner oder externer Auftrag zu Archivierungsleistungen sollte folgendes beinhalten:

   a) Auftragsinhalt (Anlegen, Pflegen, Löschen von Archivierungsobjekten)
   b) Kurzbeschreibung des Archivbestandes
   c) Name des Auftraggebers, Kostenstelle und Telefonnummer
   d) Datenbestands/-dateiname
   e) Zeitpunkt(e) der Archivierung (Stichtag/Per-Datum, Periode o.a.)
   f) Datenträger (Magnetbandkassette, CD ROM, Laser DiskM o.a.)
   g) Name und Struktureinheit des Dateneigners
   h) Anzahl der Kopien zum Zwecke der Sicherung des Archivbestandes
   i) Aufbewahrungsfrist
   j) Freigabetermin
   k) Freigabeverfahren (Löschen nach Ablauf Sperrfrist oder explizite Freigabe)
   l) Datum und Unterschrift des Auftraggebers

2. Erteilung des Auftrages zur Datenrekonstruktion

Genau genommen dient die Archivierung ausschließlich dem Zweck, bei Bedarf den archivierten Datenbestand zum Zwecke der Kontrolle oder Prüfung wieder bereitstellen zu können.

Wenn das problemlos funktionieren soll, müssen bereits zum Zeitpunkt der Archivierung die dazu erforderlichen Festlegungen getroffen werden. Zu diesen Festlegungen gehören vor allen Dingen eindeutige Vorgaben des Dateneigners/Auftraggebers zur

- Organisationsform der wieder herzustellenden Daten und zu den
- zeitlichen Anforderungen an die Wiederherstellung, gerechnet vom Zeitpunkt der Anforderung.

In Abhängigkeit vom beauftragten Archivierungsumfang, daraus resultierenden Rekonstruktionsmöglichkeiten und den konkreten Anforderungen an die Rekonstruktion der Daten seitens des Dateneigners sind folgende Stufen der Rekonstruktion zu unterscheiden:

a) Visualisierung, d.h. auszugsweisen oder vollständigen Andruck/Ausdruck der Daten in decodierter Form (einfache Visualisierung).
b) Recovery, d.h. Rückführung der relevanten Daten in die ursprüngliche DV-Umgebung und Nachvollzug / Revision innerhalb des Anwendungssystems, aus dem heraus sie archiviert wurden.
c) Aufbereitung mittels spezieller Tools, d.h. Aufbereitung und Überführung der zu rekonstruierenden Daten vom Archivierungsmedium (Magnetband, WORM-Datenträger o.a.) in eine Form bzw. eine Systemumgebung, in der die Durchführung der notwendigen Prüfungs- bzw. Auswertungsaufgaben möglich ist.

Diesbezügliche Festlegungen können weit reichende Konsequenzen haben und bedürfen deshalb sorgfältiger Vorbereitung und - mit Blick auf den je Stufe enorm wachsenden Aufwand - sorgfältiger Begründung. Sie können nicht ad hoc, d.h. erst im Bedarfsfalle getroffen werden.

Es hat sich bewährt, im direkten Zusammenhang mit dem Auftrag zur Archivierung derartige Vorgaben in Form eines vorbereiteten "Auftrages zur Datenwiederherstellung" erstellen zu lassen, der zum gegebenen Zeitpunkt natürlich präzisiert werden muss.

Der Auftrag zur Datenrekonstruktion ist die "Kehrseite" des Auftrages zur Archivierung und deshalb diesem in Inhalt und Aufbau sehr ähnlich.

3. Festlegung der für Archivierung und Wiederherstellung zu nutzenden Tools und Technologien, deren Parametrisierung etc.
4. Festlegungen zu Art und Ort der Aufbewahrung der Archivbestände
5. Festlegung zur Sicherung der Archivbestände (Datensicherungsverfahren, einschließlich Generationsverwaltung)
6. Festlegungen zur Kontrolle und Pflege der physischen Beschaffenheit (Sicherung der Lesbarkeit) der Archivbestände über den gesamten Archivierungszeitraum
7. Festlegungen zu Form und Inhalt der Bestands- und Nachweisführung sowohl aus technischer Sicht (Arbeit mit Datenträger- und Dateikennsätzen), als auch aus fachlich-inhaltlicher Sicht (Dateneigner, Dateninhalt, Geschäftsjahr, Buchungsperiode etc.)
8. Festlegungen zu den Verfahren zur Freigabe von Archivierungsobjekten, beinhaltend "explizite", d.h. durch den Dateneigner veranlasste, und "implizite" Freigaben, d.h. nach Ablauf der Sperrfristen "automatisch" vorgenommene Freigaben
9. Festlegungen zu den anzuwendenden Verfahren der Löschung von Daten, Vernichtung von Datenträgern

(Hinweis: Weitergehende Aussagen und Beispiele zu den unter 1. bis 9. genannten Bereichen einer Verfahrensanweisung finden sich in WÄH02).

Es zeigt sich, dass es sich bei der Archivierung und Wiederherstellung von codierten Daten um eine weit kompliziertere und komplexere Aufgabenstellung handelt als das bei nicht codierten Daten der Fall ist.

Ausgereifte Anwendungssysteme, wie das System SAP R/3, unterstützen zwischenzeitlich weitgehend den Prozess der Archivierung codierter Daten. Sie können dem Anwender aber nicht die zu treffenden Entscheidungen über Art, Zeitpunkt, Form, Umfang und Dauer der Archivierungsverfahren sowie zu den Wiederherstellungsanforderungen anzuwendenden Freigabeverfahren abnehmen.

Fazit:

Es führt kein Weg vorbei an der

(1) Erhebung, Klassifizierung und laufenden Aktualisierung

von Archivierungsobjekten, sowohl im Bereich der nicht codierten als auch der codierten Daten,

(2) Erarbeitung einer die Archivierung und Verwaltung nicht codierter Daten im Detail regelnden Archivordnung,

(3) Erarbeitung und Implementation praktikabler, sicherer und möglichst aufwandsarmer Verfahren zur Archivierung codierter Daten, ausgehend von den an die Wiederherstellung/Rekonstruktion zu stellenden Anforderungen.

Nur ein diese drei Elemente beinhaltendes, in sich stimmiges Gesamtkonzept zur Archivierung, einschließlich der erforderlichen Orgware, Software und Hardware, kann den Widerspruch lösen, in dem viele Anwender befangen sind:

Sie begreifen die Archivierungspflicht verständlicherweise als "notwendiges Übel". Statt sich dieses "Übels" aber mit Anstand zu entledigen, gefährden sie durch lückenhafte Vorgaben Nachvollziehbarkeit und Prüfbarkeit des Buchführungsprozesses und/ oder erzeugen andererseits mit hohem Aufwand "Datenmüll".

Sich des "Übels der Aufbewahrungspflichten" mit Anstand entledigen kann im gegebenen Zusammenhang nur bedeuten, den gesamten Archivierungsprozess grundlegend zu reorganisieren und auf ein sachlich begründetes, praktikables und in der Anwendung möglichst aufwandsarmes Archivierungskonzept zu gründen.

Quellennachweis

AO Abgabenordnung, AO 1977, veröffentlicht in dtv (1997)

GDPdU Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) - BMF-Schreiben vom 16.7.2001 - IV D 2 - S 0316 - 136/01 -

GoBS Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) Bundessteuerblatt 1995, Teil 1, S. 738 - 747

HGB Handelsgesetzbuch, veröffentlicht in dtv (1996)

FAIT Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1), Stand 08.03.2001

WÄH02 Wähner, G. W., DV-Revision - Prüfung der Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit, Friedrich Kiehl Verlag, Ludwigshafen, 2002

Datenträgerbezeichnung	Datenträger	DT-Urs.	Archivfrist	Archivort	Ordnungsmerkmale	Abgabe ans Archiv	Exemplare/ Verteiler	DA	Periodizität
Dauerbuchungsbelege	Formular	FAt	10	FiBu-Reg.	Beleg Nr.	1 Jahr; 31.03. FJ	1 Original	0	unterschiedlich
Eingangsrech-nungen	Papier	L	10[7]	FiBu-Reg.	Beleg Nr.	1 Jahr; 31.03. FJ	1 Original	80	täglich
Einzelposten Deb/Kred/SK	Druckliste	SAP FI	10	FiBu-Reg.	Jahr, D/K/S	1 Jahr; 31.03. FJ	2 Original	0	jährlich
Einzugsliste Debitoren	Druckliste	SAP FI	10	FiBu-Reg.	Datum, Debitoren	1 Jahr; 31.03. FJ	1 Original	2	14 tägig
FW-Bewertung	Druckliste	SAP FI	10[2]	FiBu-Reg.	Deb, Kred, SK	1 Jahr; 31.03. FJ	1 Original	5	jährlich
GuV	Druckliste	SAP FI	10	FiBu-Reg.	Jahr	1 Jahr; 31.03. FJ	1 Original	0	jährlich
Interner & externer Deb.-Schriftwechsel	Papier	K	6	FiBu-Reg.	Alphab.	1 Jahr; 31.03. FJ	1 Exemplar	12	täglich
Kassenbelege	Formular	manu-ell	10	FiBu-Reg.	Beleg Nr.	1 Jahr; 31.03. FJ	1 + Anlage	8	täglich
Kopien ausgangs-schecks	Papier		10	FiBu-Reg.	Scheck-Nr.	3 Mona-te	1 FiBu 1 Buchhalt.	1	wöchentlich
Kreditlimite Vertrieb	Diskette	Exc	6[5]	FiBu-Reg.	Jahr	1 Jahr; 31.03. FJ	1 Original	0	jährlich
LZB Meldungen	Druckliste	SAP FI	6	FiBu-Reg.	Art, Monat	1 Jahr; 31.03. FJ	1 Kopie	0	monatlich
Mahnungen (D)	Druckliste	SAP FI	6	FiBu-Reg.	Mahnlauf, Deb	1 Jahr; 31.03. FJ	1 Kopie	10	14 tägig
Mahnungen (K)	Papier	L	6	FiBu-Reg.	Alphab., GJ	1 Jahr; 31.03. FJ	1 Original	6	täglich

Abbildung 1: Nicht codierte Archivierungsobjekte Finanzbuchhaltung (Auszug)

+++ SEMINARE +++

Seminarcode: **R3GB**
14.04.-15.04.05

Revisionsführerschein für SAP R/® Systeme

Inhalte u.a.:

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

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

Transaktionscodes
- Aufrufen von Anwendungen
- Historienliste

Individuelle Benutzereinstellungen
- Benutzerfestwerte
- Das Benutzermenü

Reports
- Standardreports in den Modulen
- Selektionskriterien

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **R3DP**
18.04.-19.04.05

Datenprüfung im Umfeld des SAP-Systems

Inhalte u.a.:

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

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

Datenprüfung FI
- Kreditoren
- Debitoren
- Anlagen

Datenprüfung MM
- Stammdaten (MARA)
- Materialbewegung
- Inventuren

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **R3BK**
21.04.-22.04.05

Prüfung des Berechtigungskonzeptes von SAP R/3® Systemen

Inhalte u.a.:

Aufbau des Berechtigungskonzeptes
- Objekte / Berechtigungen / Profile
- Transaktionsberechtigungen

Die Problematik des Berechtigungskonzeptes
- Komplexität und Quantität
- Kritische Berechtigungen

Konzepte zur Implementierung des Berechtigungskonzept

Tipps und Tricks beim Umgang mit dem Berechtigungskonzept

Der Profilgenerator

Möglichkeiten zur Prüfung mit externen Werkzeugen

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **R3SY**
25.04.-27.04.05

Systemprüfung von SAP R/3®

Inhalte u.a.:

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

Benutzerverwaltung
- Grundkonzeption

Protokollierungskomponenten
- Auditing

Verbuchungsprinzip
- Organisatorische und systemseitige Handhabung

Tabellensteuerung
- Protokollierung
- Technische Konzeption der Änderungsbelege

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **R3FI**
28.04.-29.04.05

Revisionsworkshop „Finanzbuchhaltung" von SAP R/3® Systemen

Inhalte u.a.:

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

Modul FI
- Transaktionen
- Plausibilitätsprüfungen
- Kreditoren und Rechnungsprüfung

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

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **R3KT**
02.05.-03.05.05

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

Inhalte u.a.:

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

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

Rollentrennung beim Transportprozess
- Entwicklung, Qualitätssicherung, Administration
- Funktionstrennung

Das Transport Management System (TMS)

Kontrolle der Importvorgänge

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

+++ SEMINARE +++

Seminarcode: **GMPR**
04.04.-06.04.05

Praktische Projektrevision

Inhalte u.a.:

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

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

Projektrevision (Fallbeispiele)

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **CACL**
04.04.-06.04.05

ACL für Revisoren

Inhalte u.a.:

Datenprüfung in Theorie und Praxis
- Werkzeuge der Datenprüfung

Datenprüfung mit ACL
- Die Datenübernahme in ACL

Funktionen von ACL
- Datenverwaltung
- Zusammenführen / Verbinden
- Stichprobenverfahren

Fallbeispiel Datenprüfung SAP-FI
- Kreditoren / Debitoren
- Anlagen

Fallbeispiel Datenprüfung SAP-MM
- Stammdaten (MARA)
- Buchhaltungssicht der Artikel: Preise / Materialbewegungen

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **BKEB**
07.04.-08.04.05

Electronic Banking aus Revisionssicht

Inhalte u.a.:

Techniken im eBanking

HBCI - eBanking

Kryptografische Verfahren beim Einsatz in Banken

Funktion und Qualität von Zertifizierungsverkehr im Internet

Internet als Kapitalmarkt

Internet als Informationsmarkt

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **DSDM**
11.04.-13.04.05

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

Inhalte u.a.:

Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

Grundsätze der ordnungsmäßigen Archivierung originärer elektronischer Dokumente

Theoretische Grundlagen

Praktische Übungen / Workshop

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **DSIT**
13.04.-15.04.05

Einführung in die IT-Revision

Inhalte u.a.:

GoDV Grundsätze ordnungsgemäßer Datenverarbeitung

FAMA/FAIT-Verlautbarungen

Prüfungsstandard des IDW (PS 330 - Abschlussprüfung bei Einsatz von IT)

GDPdU (Grundsätze der Datenprüfung digitaler Unterlagen)

GSH / BSI

FAIT 2 (GoB und eCommerce)

Internet-Workshop

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

Seminarcode: **DSW2**
18.04.-20.04.05

Windows 2000 für Revisoren

Inhalte u.a.:

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

NTFS 5
- Verschlüsselung
- Prüfungsansätze

Security
- Anmeldesicherheit
- Restriktion für Benutzer

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

Anmeldung und Auskünfte:

IBS Schreiber GmbH
Frau Christina Robrock
TEL: +49 40 69 69 85-15
FAX: +49 40 69 69 85-31
Friedrich-Ebert-Damm 145
22047 Hamburg

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

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Intensiv-Training für Datenschutzbeauftragte

Inhalte u.a.:

Das Bundesdatenschutzgesetz vom 23. Mai 2001

Der Datenschutzbeauftragte

Die Aufgaben des Datenschutzbeauftragten

Outsourcing und Datenschutz

Datenschutz und neue Medien

Der Referent:

RA Dr. Hans-Jürgen Schaffland, Dipl.-Volksw. Friedhelm Wolf

Termin und Ort:

12. - 13. April 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050424.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Datenschutz im Krankenhaus

Inhalte u.a.:

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

DSB im Krankenhaus

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

Typische Schwachstellen

Neue Techniken - neue Herausforderungen

Outsourcing - Wege und Grenzen

Der Referent:

Dr. Eugen Ehmann, Regierungsdirektor

Termin und Ort:

19. September 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050946.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Was muss ein Datenschutzbeauftragter bei vernetzten Systemen beachten?

Inhalte u.a.:

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

Die Referenten:

Holger Wöhle,
Arcor AG, Eschborn
Dipl.-Volkswirt Friedhelm Wolf,
Externer Datenschutzbeauftragter, Königstein

Termin und Ort:

26. - 27. Oktober 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **051023**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Datenschutz und Bankgeheimnis

Inhalte u.a.:

Das neue SCHUFA-Verfahren

Datenschutz-Klauseln bei Verbundgeschäften

Datenschutz und vorrangige Rechtsvorschriften

Cold Calling

Telefax / E-Mail

Informationsveranstaltungen für Führungskräfte

Die Referenten:

Dipl.-Volksw. Friedhelm Wolf, Kronberg

Termin und Ort:

11. Mai 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050524**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Projektmanagement

Inhalte u.a.:

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

Der Referent

Dr. Klaus Reiter,
GTZ Deutsche Gesellschaft für Technische Zusammenarbeit, Eschborn

Termin und Ort:

09. - 10. Mai 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee.
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050532**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Controlling im Ideenmanagement

Inhalte u.a.:

Warum Controlling?

Controlling für das Ideenmanagement

Kennzahlensystem

Beteiligungs-Nutzen-Portfolio

Wirtschaftlichkeit

Fallbeispiele - Diskussion

Der Referent:

Dr. Karola Läge, Unternehmensberater, Korb bei Stuttgart

Termin und Ort:

29. April 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050443.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Human Ressources Grundlagen der Personalarbeit

Inhalte u.a.:

Das Personalwesen auf dem Weg vom Verwalter zum Kundenbetreuer

Der Kreislauf eines Beschäftigungsverhältnisses

Erfahrungsaustausch / Fragen der Teilnehmer/-innen

Der Referent

Uwe Ebling, Dipl.-Betriebswirt (FH), Unternehmensberater und mit mehrjähriger Erfahrung als Personalleiter und -entwickler

Termin und Ort:

16. März 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050455.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Deckungsbeitrags-rechnung

Inhalte u.a.:

Grundzüge der Deckungsbeitrags-rechnung

Marktorientiertes Kalkulieren

Möglichkeiten und Grenzen der Deckungsbeitragsrechnung

Controlling auf der Grundlage von Deckungsbeiträgen

Erfolgsorientiertes Berichtswesen

Der Referent

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

Termin und Ort:

13. April 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050425.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Schreiben fürs Internet

Inhalte u.a.:

Unterschiede zwischen Print- und Online-Medien

Schreiben fürs Internet

Onlinegerechte Texte und Hypertexte verfassen

Neue Textformen: Teaser und Newsletter

Der Referent

Dr. Katrin Bischl,
Journalistin & Sprachwissenschaftlerin, Schwetzingen Lehrbeauftragte der Universität Mannheim und Heidelberg

Termin und Ort:

14. - 15. April 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050449**.

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Welcoming Visitors and telephoning in English

Inhalte u.a.:

Gesprächspartner durch gezieltes Abfragen von Informationen erfolgreich verbinden

Informationsanforderungen formulieren und angemessene Auskünfte erteilen.

Strategien: um Unsicherheiten beim freien Sprechen abzubauen.

Der Referent:

Elaine Litchfield, Englischtrainerin, Heppenheim

Termin und Ort:

14. - 15. April 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050445.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Ideenmanagement im Gesundheitswesen

Inhalte u.a.:

Ideenmanagement im Gesundheitswesen

Barrieren des Ideenmanagements

Welches sind die Erfolgsfaktoren im Ideenmanagements

Ganzheitliches Ideenmanagement im Gesundheitswesen

Der Referent:

Hans-Rüdiger Munzke, Dipl.-Ing., Inhaber, IdeenNetz - Partner of ablony, Lengerich

Termin und Ort:

14. April 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050439.**

dib Unternehmenspolitik
Deutsches Institut für Betriebswirtschaft GmbH

Krisen-PR für Praktiker

Inhalte u.a.:

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

Der Referent:

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

Termin und Ort:

23. - 24. Juni 2005
im dib-Seminargebäude,
Frankfurt am Main, Friedrichstr. 10-12.

Anmeldung und Auskünfte:

Bitte melden Sie sich an bei
Dipl.-Volkswirt Margit Burkhardt-Lee .
Sie beantwortet auch gerne Ihre Fragen.
telefonisch: (069) 9 71 65 -13
schriftl.: dib, Friedrichstr. 10-12,
60323 Frankfurt am Main
per Fax: (069) 9 71 65 -25
eMail: Margit.Burkhardt-Lee@dib-ev.de
Die Seminarnummer ist **050649.**

Prof. Dr. Frank Körsgen

SAP R/3® Arbeitsbuch

Grundkurs mit Fallstudien

Erich Schmidt Verlag,
208 S., ISBN 3 503 08347 2
22,80 €

Die erfolgreiche Umsetzung von Bankstrategien ist ein schwieriges Problem. Dieses Arbeitsbuch stellt SAP® R/3®-Anwendern anschaulich und Schritt für Schritt dar, wie eine Kundenauftragsbearbeitung im SAP® R/3®-System abgebildet werden kann.

Gezeigt wird eine typische Wertschöpfungskette eines auftrags-bezogenen Montagefertigers, der nach Auftrag eines gewerblichen Kunden eine größere Anzahl eines Komplett-PC fertigt, ausliefert und in Rechnung stellt. Fehlende Teile werden über den Einkauf bei einem Lieferanten beschafft. Alle notwendigen Stammsätze (Kunde, Lieferant, Materialien, Stückliste, Arbeitsplatz und -plan etc.) und Belege können von den Lernenden selbst im System angelegt werden. Die Vorgehensweise hierzu ist in insgesamt zwölf aufeinander aufbauenden Fallstudien detailliert dargestellt. Ein separates Kapitel umfasst eine Einführung in die Bedienung und die Menüführung der Software.

Alle Fallstudien werden durch die intensive Beschreibung des jeweils notwendigen SAP®-Hintergrundwissens vorbereitet und begleitet. Dieses Hintergrundwissen wurde thematisch bewusst breit angelegt und bezieht sich nicht nur auf die einzelnen Fallstudien, sondern beschreibt auch davon unabhängig einzelne Module und Komponenten in übersichtlicher Weise. Zahlreiche Abbildungen erleichtern das Verständnis für die komplexe Software.

Das Buch dient der SAP® R/3®-Schulung und Ausbildung. Es liefert insbesondere Seminaranbietern und Hochschulen eine handlungsorientierte, qualitativ hochwertige Arbeitsunterlage und basiert auf dem SAP® Release IDES 4.7 Enterprise.

Herausgegeben von Deloitte
Schriftleitung: Michael Cluse und Jörg Engels

Basel II

Handbuch zur praktischen Umsetzung des neuen Bankenaufsichtsrechts

Erich Schmidt Verlag,
629 S., ISBN 3 503 08346 4
Subskriptionspreis gültig bis 31. März 2005: 79,90 €
Ladenpreis ab 01.04.2005: 98,00 €

Die weitläufig als "Basel II" bezeichnete Überarbeitung der Eigenkapitalanforderungen für Kreditinstitute stellt nicht nur die Finanzdienstleistungsbranche vor große Aufgaben. Durch das veränderte Umfeld können sich auch die Kreditnehmer diesem Thema nicht entziehen.

Das Regelwerk ist mit über 800 Paragraphen gleichermaßen umfangreich wie komplex. Noch immer besteht bei vielen Regelungen Interpretationsbedarf.

Das vorliegende Handbuch leistet Hilfestellung bei der Umsetzung der neuen Anforderungen. In mehr als 30 Beiträgen werden die neuen aufsichtrechtlichen Bestimmungen erläutert und ihre Auswirkungen für die Praxis handhabbar analysiert. Der Autorenkreis setzt sich zusammen aus hochkarätigen Praktikern, die ihre Erfahrung mit der Umsetzung von Basel II einbringen. Mitarbeiter der Prüfungs- und Beratungsgesellschaft Deloitte arbeiten schwerpunktmäßig die Veränderungen des Aufsichtsrechts auf.

In eigenständigen Beiträgen beschreiben diese Praktiker die Besonderheiten für Spezialkreditinstitute und Kreditnehmer, so dass alle Bereiche der Baseler Vereinbarung umfassend abgedeckt werden.

Schwerpunkte
- Kreditrisikomessverfahren unter Basel II
- Kreditrisikounterlegung
- Messung und Steuerung der operationellen Risiken
- Banksteuerung unter Basel II
- Branchenspezifische Aspekte der Kreditinstitute und Finanzdienstleister

Die Säulen II und III: Aufsichtliche Überprüfung und Marktdisziplin

---

Hrsg. International Group of Controlling (IGC)

Controller-Wörterbuch

Die zentralen Begriffe der Controllerarbeit mit ausführlichen Erläuterungen

Deutsch - Englisch, Englisch - Deutsch

Schäffer-Poeschel Verlag,
570 S., ISBN 3-7910-2405-1
29,95 €

Das Controller-Wörterbuch gibt die zentralen Fachbegriffe des praxisorientierten Wissensstandes in Deutsch-Englisch und Englisch-Deutsch wieder. Das Wörterbuch ist in der jeweiligen Sprache alphabetisch aufgebaut, dabei reicht das Spektrum der Begriffe von A wie Abgrenzungen (accruals and dererrals) bis Z wie Ziel (objektive/target). Die Begriffe werden nicht nur in die jeweilige Sprache übersetzt, vielmehr erfolgen ausführliche inhaltliche Erläuterungen, deren Verständnis durch zahlreiche graphische Darstellungen unterstützt wird. Die nunmehr 3. Auflage wurde überarbeitet und neu um die wichtigsten Begriffe aus dem Bereich der elektronischen Datenverarbeitung ergänzt; dabei erfolgte die Auswahl aus der Sicht des Controllers.

Zielsetzung dieses zweisprachigen Controller-Wörterbuches ist es, zu einem einheitlichen Gebrauch des Controller-Fachvokabulars beizutragen. Es soll Praktikern und Studierenden im Bereich Controlling als Nachschlagewerk für die zentralen Controlling-Begriffe dienen.

Herausgeber: IGC (International Group of Controlling) Die IGC ist eine Interessengemeinschaft für die Aus- und Weiterbildung sowie Forschung und Entwicklung auf dem Gebiet des Controlling; zwischenzeitlich gehören der IGC 27 Mitgliedsorganisationen im deutschsprachigen Bereich sowie in den osteuropäischen Ländern an. Sie dient u.a. als Plattform für die Abstimmung und Weiterentwicklung einer übereinstimmend getragenen Controlling-Konzeption sowie einer einheitlichen Controlling-Terminologie.

Peter Münch

Technisch-organisatorischer Datenschutz

2. überarbeitete und erweiterte Auflage 2005

Datakontext Fachverlag,
428 S., ISBN 3-89577-358-1
49,00 €

Nichts entwickelt sich gegenwärtig so schnell wie die Informationstechnik und die damit verbundenen Sicherheitsrisiken - so hat der Autor im März 2003 die Erstauflage seines Buches eingeleitet. Die Einzigartigkeit dieser Fachlektüre und die gewählte Darstellungsform haben durchweg positive Kritik erfahren; in dem von der Aufsichtsbehörde Baden-Württemberg im September 2004 herausgegebenen Merkblatt "Der betriebliche Beauftragte für den Datenschutz" wird der Titel "Technisch-organisatorischer Datenschutz" neben anderen, mehr datenschutzrechtlich orientierten Schriften, als Basisliteratur für Datenschutzbeauftragte angegeben.

Die Einzigartigkeit dieser Fachlektüre und die gewählte Darstellungsform haben durchweg positive Kritik erfahren...

Die zweite aktualisierte und erweiterte Auflage trägt neuen Herausforderungen im technischen und organisatorischen Datenschutz Rechnung, wie u.a. der SPAM-, RFID- oder USB-Stick-Problematik Rechnung, berücksichtigt neue gesetzliche Regelungen und deren Auswirkungen und setzt sich mit neueren Tendenzen wie technikorientierter Datenschutz auseinander. Das Verhältnis des sich immer umfassender etablierenden IT-Sicherheitsbeauftragten zum Datenschutzbeauftragten wird vertieft. Die auf der beigefügten CD vorhandenen Arbeitshilfen wurden aktualisiert und deutlich erweitert. ✜

ABO-Bestellung für ReVision

Ein Abo von ReVision beinhaltet folgende Verlagsdienstleistungen:

- Supplement für SAP R/3® Revisoren
- IBS-Prüfmanual
- Zugriffsfreigabe auf umfassende Informationen unter **www.revision-hamburg.de** mit allen jeweils erschienenen ReVisions-Beiträgen und Zusatzinformationen, abrufbar und selektierbar
- Zusendung vertiefender Hinweise und Unterlagen zu Beiträgen auf Anfrage

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

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

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

Bestell-Fax

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

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

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

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

Konto-Nr.: _____ BLZ: _____

Bank: _____ Kontoinhaber: _____

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

Name: _____ Vorname: _____

Firma: _____ Telefon: _____

Abteilung: _____ eMail: _____

Straße: _____ PLZ/Ort: _____

Ort, Datum: _____ Unterschrift: _____