Testat nach OPDV-Stellungnahme Nr. 1/2006 - Ergebnis der Risikobewertung - ArciSoft 3 Archiv- und Lagersoftware

(**Abschlussergebnis**)

Dokumentversion 3.7 vom 06.03.2009 18:31

Dieses Testat ist nur gültig, wenn es komplett weitergegeben wird, also alle Seiten vom Deckblatt bis zur Unterschriftenseite enthält.
Unvollständig weitergegebene Dokumente sind ungültig!

INFORMATIKZENTRUM DER SPARKASSEN-ORGANISATION GMBH

Inhaltsverzeichnis

Versionsführung dieses Dokumentes:

Wer	Wann/ Version	Was
Hr. König	V090305 V3.6	▪ Berücksichtigung der bereitgestellten Unterlagen ab [100]
Hr. König	V090306 V3.7	▪ Berücksichtigung der nachgelieferten Unterlagen ab [103]

1 Vorwort und Zusammenfassung

Die in den letzten Jahren eingeführten Internet-basierten Infrastrukturen, wie sie bspw. die auf Browsern basierenden Client- und Serverarchitekturen erfordern, eröffnen den Anwendern die komfortable Abwicklung von Transaktionen ohne komplexe Softwareinstallation auf den Arbeitsplatzsystemen. Zugleich bringen die neuen Technologien neue Risikopotentiale mit sich, die mit immer sorgfältigerer Planung, Umsetzung und Überprüfung der IT-Anwendungen und Infrastrukturen einzugrenzen sind.

Dies sicherzustellen ist Aufgabe des jeweiligen Projektmanagements, der beteiligten Fachabteilungen sowie der Innenrevision. Mit der Stellungnahme OPDV 1/2006 liegen Regularien für die Freigabe eines Systems vor. Soweit es sich um fremd entwickelte, komplexe Systeme handelt, wird der Aufwand hierfür jedoch zunehmend größer. Wenn der Einsatz des Systems dann noch bei mehreren Betreibern vorgesehen ist, dann bietet es sich an, die Freigabe in eine Programmfreigabe und eine Einsatzfreigabe aufzuspalten.

- Im Rahmen der **Programmfreigabe** sind die fachliche Eignung entsprechend den Anforderungen des Fachkonzepts, die sachgerechte Umsetzung in der Programmierung innerhalb eines geordneten Programmentwicklungsverfahrens, der erfolgreiche Test von Verarbeitungsfunktionen und -regeln innerhalb der Anwendung (ggf. einschl. Schnittstellen) sowie das Vorliegen einer aktuellen Verfahrensdokumentation zu beurteilen.
  Unter besonderen Umständen können Umfang und Intensität der Qualitätssicherungsmaßnahmen einer Programmfreigabe reduziert werden, ggf. sogar ganz unterbleiben. Dies kann der Fall sein
  - bei Betriebssystemen und betriebssystemnaher Software
  - bei Programmen von IT-Dienstleistern, die sich dazu verpflichtet haben, ihr Programmeinsatzverfahren nach Maßgabe dieser Stellungnahme auszurichten, und gewährleisten, dass die Einhaltung dieser Verpflichtung regelmäßig geprüft wird
  - bei typischerweise nicht bankfachlicher Standard-Software (z. B. Bürosoftware), wenn die Funktionsfähigkeit aufgrund der Vertrauenswürdigkeit in die Qualität der Softwareentwicklung der Herstellerfirma unterstellt werden kann, z. B. aufgrund des hohen Verbreitungs- und Bekanntheitsgrads
  - wenn die Programmfreigabe eines vertrauenswürdigen Dritten (z. B. DSGV, SIZ, andere Sparkasse oder IT-Dienstleister als Vertreter) i. S. dieser

[1] z. B. IDW PS 880, ISO-Normen

[2] z. B. Prüfungsstellen, BSI, Wirtschaftsprüfungsgesellschaft , TÜV-IT

Stellungnahme vorliegt und eine unveränderte Programmversion eingesetzt wird

- beim Vorliegen eines qualifizierten Softwaretestats[3] von einer anerkannten Prüfungseinrichtung[4] und dem Einsatz einer unveränderten Version des Programms. Entsprechende Nachweise sind nachvollziehbar zu dokumentieren.

- Gegenstand der **Einsatzfreigabe** ist die Untersuchung der organisatorischen und technischen Prozesse des Anwenders, die den Einsatz innerhalb der vorhandenen Umgebung bestimmen, sowie die Gewährleistung der Funktionsfähigkeit von Schnittstellenprozessen zu vor- und nachgelagerten Anwendungen und der Belastbarkeit im Echtbetrieb.
  Besonderer Aufmerksamkeit bedürfen die Einbindung in das Interne Kontrollsystem und die Parametrisierung des neuen Programms sowie die Ergebnisse von Integrationstests.
  Voraussetzung für die durchzuführende Beurteilung sind das Vorliegen vollständiger und aktueller Programm- und Hardwareübersichten sowie angemessene Verfahren in den Bereichen Beschaffung und Change-Management.

Im Verlauf der Prüfung kam auch die *Checkliste Prüfungen nach OPDV 1/2006* des SIZ zum Einsatz. Diese Liste baut auf der Stellungnahme Nr. 1/2006 des Fachausschusses OPDV auf und berücksichtigt die Praktiken und Erfahrungen mit DV-Projekten innerhalb der Sparkassen-Finanzgruppe. Dieses Testat ist somit eine thematisch umfassende und unabhängige Analyse des Entwicklungs-, Qualitätssicherungsprozesses sowie des Praxiseinsatzes, der dem Freigabeverfahren nach OPDV 1/2006 unterliegt. Das Testat berücksichtigt insbesondere auch Aspekte des Projektmanagements, der IT-Qualität, der Softwareentwicklung sowie der IT-Sicherheit.

1.1 Benutzung / Zweck des Dokumentes

Kursive Texte kennzeichnen Originalzitate aus anderen Dokumenten oder Vorgaben.

1.2 Prüfgegenstand

1.2.1 Identifizierung

Im Rahmen der hier dokumentierten Prüfung ist die erstellte IT-Anwendung *ArciSoft 3 Archiv- und Lagersoftware* und deren Herstellungsprozess bei der SoulTek GbR[5] zu untersuchen und zu bewerten [IDW PS 880, Tz2].

[3] z. B. IDW PS 880, ISO-Normen

[4] z. B. Prüfungsstellen, BSI, Wirtschaftsprüfungsgesellschaft , TÜV-IT

[5] Nachfolgend mit Hersteller abgekürzt.

1.2.2 Produktbeschreibung und -abgrenzung

Gegenstand der Prüfung ist ein Softwaresystem namens *ArciSoft 3 Archiv- und Lagersoftware*. *ArciSoft 3 Archiv- und Lagersoftware* ist eine Lagerverwaltungssoftware.

[103, S. 4]: *Bei der Software handelt es sich um eine datenbankgestützte Web-Anwendung auf der Basis von MS-Windows 2000, XP und Vista oder MS-Windows 2003/2005 Server. Als Datenbanken kommen wahlweise MS-Access 2003 oder MS-SQL Server 2005, bei Bedarf auch andere Systeme zum Einsatz. Je nach Anforderung kann ArciSoft als Einzelplatz- oder Netzwerk-System installiert werden.*

Die Kernfunktionalität [ISO/IEC 9126] der *ArciSoft 3 Archiv- und Lagersoftware*-Anwendung besteht laut Pflichtenheft [100] aus:

> *ArciSoft vereinfacht die Verwaltung Ihrer Akten und Dokumente.*
>
> *Das Programm ist die ideale Lösung für Papierarchive in Banken und öffentlichen Verwaltungen, Unternehmen, Krankenhäusern, sowie konventionellen Archiven aller Art.*
>
> *ArciSoft sorgt für Ordnung im Inventar, denn es merkt sich, wer wann welches Objekt ausgeliehen hat. Der Status aller Akten und Dokumente ist jederzeit nachvollziehbar. Ein integriertes Barcodemodul identifiziert Akten und Mitarbeiter ohne manuelle Eingabe.*

Der Flyer [102] konkretisiert die Funktionen mit:

Die ArciSoft Leistungen im Überblick:

- > Netzwerkunterstützung
- > Akten- und Dokumentenverwaltung
- > Aktenrecherche
- > Suchfunktionen
- > Stammdatenverwaltung
- > Barcodeunterstützung
- > Labeldruck
- > Historien
- > Aussonderungsliste
- > Reservierungsmodul
- > Reports und Statistiken
- > E-Mail-Benachrichtigungs-System

1.3 Ziel der Prüfung

Das Ziel der Prüfung ist die Bewertung, ob ArciSoft als Kategorie-C entsprechend OPDV-Stellungnahme Nr. 1/2006 eingestuft werden kann.

1.4 Voraussetzungen der Prüfung

Für den vorliegenden Prüfbericht ist Folgendes vorausgesetzt:

- Prüfer erfüllen die persönlichen, fachlichen und formalen Voraussetzungen für die Durchführung der Prüfung nach OPDV 1/2006.
- Das IT-System bzw. IT-Produkt unterliegt den Regelungen der OPDV 1/2006.

- Grundsätzlich haben die Betreiber wie auch der Prüfer das Vertrauen in den Hersteller, dass er seine Kompetenzen nach bestem Wissen und Gewissen einsetzt. Damit mögliche Fehler vermieden oder zumindest erkannt und beseitigt werden können, gewährte der Hersteller dem Prüfer einen umfassenden und detaillierten Einblick in seine internen Abläufe. Dies beinhaltet seine Prozesse, Verfahren, Methoden und Dokumente. Hierdurch wird das Vertrauen in die Produkte des Herstellers gestärkt. Die Offenlegung dieser betriebsinternen Informationen erfolgt im wechselseitigen Vertrauen auf die Einhaltung üblicher Vertraulichkeitsregelungen. In den Prüfbericht fließen ausschließlich Informationen, die für die Analyse und Bewertung nach OPDV 1/2006 erforderlich sind.

1.5 Projektbeteiligte

Hersteller und Lieferant

Hersteller und Lieferant von *ArciSoft 3 Archiv- und Lagersoftware* ist die SoulTek GbR.

Betreiber

Hinweis: Die erforderliche Betreiberfreigabe seitens der Rechenzentren ist nicht Gegenstand dieses Berichts.

Abnahmen

Seitens der Rechenzentren und der Projektsparkassen liegen dem SIZ keine Abnahmeschreiben vor.

Prüfinstitut

Die Prüfung wurde durchgeführt von Herrn König, Mitarbeiter des Informatikzentrums der Sparkassenorganisation GmbH (SIZ), Bonn.

2 Details zur Risikoklassifizierung

Die Risikokategorie für die gesamte Anwendung ergibt sich aus dem Maximum der potenziellen Auswirkungen. Es müssen alle fünf folgenden Abschnitte berücksichtigt werden [28,9].

Die folgende Tabelle benennt Unternehmensinteressen und verweist auf jeweils die spezifischen Risiken, durch die dieses Interesse gefährdet wird. Auf die Details wird dann in den folgenden Abschnitten eingegangen.

Unternehmensinteresse[6]	**Gefährdendes Risiko und Verweis auf konkrete Ausprägungen**[7]
Effizienz [ISO/IEC 9126]	Suchzeiten nach Akten sollen reduziert werden, ein spezielles Risiko ist hier aber nicht erkennbar, denn in Summe reduziert fast jede Dokumentation bei umfangreichen Beständen die Suche.

[6] Unternehmensinteressen sind im „COBIT-Würfel“ [COBIT4.0, S.26] :, [COBIT4.1, S.25]:als Unternehmensanforderung beschrieben.

[7] Entsprechend [GAIT, Prinzip1] muss die übergeordnete Analyse von Risiken durchgeführt werden, bevor die in den Unterabschnitten im Rahmen der Analyse auszufüllenden Listen potenzieller Risiken bearbeitet werden.

Unternehmens-interesse[6]	**Gefährdendes Risiko und Verweis auf konkrete Ausprägungen**[7]
Vertraulichkeit	Zugriffsberechtigungen sind in der IT-Anwendung vertraulich zu behandeln, dies ist aber eine allgemein gültige Forderung und daher kein spezifisches Thema dieser Anwendung. Der Inhalt der archivierten Unterlagen unterliegt ggf. auch strengerer Geheimhaltung. Die Unterlagen selbst werden aber nicht durch die IT-Anwendung archiviert, sondern lediglich Verweise auf die Position dieser Unterlagen. Die Berechtigungsprüfung beim Zugriff von Benutzern auf reale Akten muss ggf. durch die ausliefernden Stellen wahrgenommen werden.
Integrität	Auch wenn eine Dokumentation vor vielen Integritätsproblemen schützen kann, so erreicht auch dieser Schutz keine 100%. Der Archivar ist für eine sinnvolle Einteilung seines Lagers und für Integritätsprüfungen verantwortlich. Diese Tätigkeiten gehören zum Tagesgeschäft eines Archivars und werden durch die Software unterstützt.
Compliance / Einhaltung rechtlicher Erfordernisse	Archivierungsfristen sind u. a. auch gesetzlich vorgegeben, darüber hinaus bestehen für viele Aktentypen weiter reichende Archivierungsanforderungen aus rechtlichen Aspekten wie z. B. Nachweisen. Aspekte hierzu finden sich im Abschnitt *2.4 Einhaltung gesetzlicher oder bankaufsichtsrechtlicher Vorschriften*.

Vor einer detaillierteren Betrachtung der Risiken muss formal auch auf folgende Aussage aus der OPDV-Stellungnahme Nr. 1/2006 [OPDV1/2006, 3.2.] hingewiesen werden:

Unter besonderen Umständen können Umfang und Intensität der Qualitätssicherungsmaßnahmen einer Programmfreigabe reduziert werden, ggf. sogar ganz unterbleiben. Dies kann der Fall sein

- *[...]*
- *bei typischerweise nicht bankfachlicher Standard-Software (z. B. Bürosoftware), wenn die Funktionsfähigkeit aufgrund der Vertrauenswürdigkeit in die Qualität der Softwareentwicklung der Herstellerfirma unterstellt werden kann, z. B. aufgrund des hohen Verbreitungs- und Bekanntheitsgrads*

Bei ArciSoft handelt es sich um eine *nicht bankfachliche Standard-Software*.

***ArciSoft 3 Archiv- und Lagersoftware* stellt nach der in diesem Dokument beschriebenen Risikobeurteilung eine IT-Anwendung mit vernachlässigbarem Risiko dar und entspricht dabei den Vorgaben der Risikostufe C der OPDV-Stellungnahme Nr. 1/2006.**

2.1 Wirtschaftliche Auswirkungen bzw. Auswirkungen auf geschäftspolitische Entscheidungen

Das Pflichtenheft [100, 2.2.1] stellt fest: *Wirtschaftliche Auswirkungen bzw. Auswirkungen auf geschäftspolitische Entscheidungen – in der Software werden keine wirtschaftlichen Daten verarbeitet, diese wirkt sich somit nicht negativ auf geschäftspolitische Entscheidungen*

aus. Sie schafft keine Abhängigkeit der wirtschaftlichen Geschäftsprozesse von den Programmergebnissen. Dieser Aussage schließt sich das SIZ an.

2.2 Auswirkungen auf die Kundenbeziehung

Das Pflichtenheft [100, 2.2.2] stellt hierzu fest: *Auswirkungen auf die Kundenbeziehung - die Software wird nicht im Kunden- und Beratungsbereich, sondern allein im internen Archivierungs- und Lagerbereich eingesetzt. Sie kann sich somit nicht negativ, wie z.B. durch fehlerhafte Beratungsergebnisse auswirken. Es werden keine kundenbezogenen Personaldaten gespeichert und verarbeitet, so dass das BDSG hierzu nicht berührt wird. Mitarbeiternamen und E-Mailadressen stehen nur dem verantwortlichen Administrator zur Verfügung, dessen Zugang passwortgeschützt ist*. Dieser Aussage schließt sich das SIZ an.

2.3 Auswirkungen auf das Sicherheitsniveau

Das Pflichtenheft [100, 2.2.3] stellt hierzu fest: *Auswirkungen auf das Sicherheitsniveau des Unternehmens – die Software eröffnet keine neuen Sicherheitslücken: Sie erfordert keine Installation und bewirkt keine Veränderung der Registrierungsdateien. Die Kommunikation der Clients mit dem Webserver erfolgt allein über das HTTPS-Protokoll. Die Daten werden per SSL verschlüsselt*.

Die IT-Anwendung unterliegt darüber hinaus folgenden Beurteilungskriterien zu Auswirkungen auf das Sicherheitsniveau:

- ArciSoft beinhaltet eine eigene Benutzerverwaltung [101, S13], die an die beim einsetzenden Institut bestehende Benutzerverwaltung anzubinden ist.
- Die notwendige Verfügbarkeit [IIR2, 20 Datenverarbeitungsrisiken: Verfügbarkeit] von *ArciSoft 3 Archiv- und Lagersoftware* und der darüber durchgeführte Zugriff auf Akten wird durch das SIZ mit „muss mehrmals täglich verfügbar sein“ bewertet. Die Sicherstellung dieser Verfügbarkeit obliegt in dieser IT-Anwendung allein dem Archivar, bzw. dem technischen Betreiber, die sich bei technischen Fragen an den Hersteller wenden können. In der Produktbeschreibung [103, S.3] weist der Hersteller darauf hin, dass „*Die Zuverlässigkeit der Software ist unter anderem damit belegt, dass von den ArciSoft-Betreibern, die das Programm seit Jahren einsetzen, kein Ausfall gemeldet wurde*“. Aus Sicht des SIZ ist diese Aussage nur für den Normalbetrieb, nicht aber für Notfälle (d. h. extern veranlasste Störungen des Betriebes, siehe Notfallkonzept) ausreichend, hier sind durch das einsetzende Institut entsprechende Konzepte zu erarbeiten, die auch dann einen Zugriff auf Akten ermöglichen, wenn aus notfalltechnischen Gründen die IT-Anwendung nicht betriebsbereit ist. Auf diese Aspekte wird weder im Flyer[102] noch in der Beschreibung [102] noch im Pflichtenheft [100] hingewiesen.

2.4 Einhaltung gesetzlicher oder bankaufsichtsrechtlicher Vorschriften

Das Pflichtenheft [100, 2.2.4] stellt hierzu fest: *Einhaltung von gesetzlichen, bankaufsichtsrechtlichen oder sonstigen relevanten Vorschriften – In der Software werden Artikeldaten und Verwahrfristen verwaltet, die von dem Archivar definiert und gepflegt werden. Somit ist die Einhaltung der gesetzlichen Vorgaben durch seine Prüfung gewährleistet. Die Software berührt sonst keine relevanten Vorschriften. Reportfunktionen liefern nur programminterne Berichte über Ausleihanfragen, Ausleihen und Berichte zur Kassation*.

Die IT-Anwendung unterliegt dabei insbesondere folgenden detaillierteren Beurteilungskriterien zu Auswirkungen auf die Einhaltung von gesetzlichen und sonstigen relevanten Vorschriften:

- Aufbewahrungsfristen werden sowohl durch gesetzliche oder normative Vorgaben als auch durch rechtliche Notwendigkeiten definiert. Die IT-Anwendung erwartet vom Bedienen die korrekte Übersetzung in eine einzugebende Anzahl von Jahren für institutsspezifische Aktengruppen.
- Bei der Einlagerung von Akten muss deren unterlagenspezifische Zuordnung zu einer Aktenkategorie manuell erfolgen und aus dieser Festlegung wird der spezifische Entsorgungszeitpunkt ermittelt. Auch hier findet keine automatische Kontrolle statt.
- Das BDSG kennt auch sehr kurze Entsorgungspflichten bei Kundendaten, die nicht zu Transaktionen werden, z. B. bei Nachfragen eines Interessenten. Die Produktbeschreibung [103, S.3] weist darauf hin, dass dieser Sachverhalt durch die IT-Anwendung nicht unterstützt wird.

Andere Auswirkungen auf gesetzliche oder andere relevante Vorgaben werden nicht gesehen. Insgesamt werden dabei diese Auswirkungen durch die IT-Anwendung vom SIZ als nicht relevant bewertet.

2.5 Datenüberstellung in autorisierte Programme

Das Pflichtenheft [100, 2.2.5] stellt dazu fest: *Bedeutung der Daten bei der Überstellung in autorisierte Programme – es werden keine Daten aus anderen Programmen gelesen oder in andere Programme überstellt*. Aus Sicht des SIZ hat damit der Hersteller keine Erlaubnis zur Verwendung potenziell existierender Übernahmemaßnahmen erteilt.

3 Literaturverzeichnis (inkl. Angaben zum geprüften Projekt)

Im Testierungsprojekt wurden u. a. folgende Artefakte[8] vollständig berücksichtigt, im Dokument selbst werden weitere Referenzen durch eckige Klammern gekennzeichnet und dabei jeweils die verständliche Kurzbezeichnung des Dokumentes angegeben, z. B. [HGB, §238]:

[1] Anforderungen der SI vom 22.3.2006 an eine IT-Anwendung
[2] Arbeitshilfe für die Beurteilung von Qualitätseigenschaften bei Fremdsoftware (Erstveröffentlichung: Fachmitteilungen Nr. 7 vom 31. 3. 1999 durch den Fachausschuss OPDV, Anm. d. Red.)
[3] DIN ISO/IEC 12119 „Software-Erzeugnisse, Qualitätsanforderungen und Prüfbestimmungen"

[8] Berücksichtigte Artefakte (SW-Teile und Dokumente) werden in den Testierungsdokumenten mit abkürzender Notation der Quelle hier mit [<lit-nr>] bezeichnet, wenn dieses Artefakt im Literaturverzeichnis auftaucht. Konkrete Inhalte innerhalb dieser Quelle werden dabei möglichst auch detaillierter angegeben:
[<lit-nr>, <Abschnitt>] Der Abschnitt kann dabei auch aus der Abschnittsnummer gebildet werden
[<lit-nr>, S.<Seitennummer>] Als Seitenangabe im Dokument
[<lit-nr>, XYZ] wenn XYZ in der speziellen Dokumentenform eine Stelle eindeutig kennzeichnet, bei Tabellenkalkulationsprogrammen z. B. die Zellennummern.
Für allgemein bekannte Literaturhinweise wird statt der numerischen Angabe auch die abkürzende Bezeichnung im Text verwendet, auch wenn dieses Schriftstück nicht im Literaturverzeichnis auftaucht.

[4] Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) - Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995, veröffentlicht im BStBl. 1995, Teil I, S.738ff.
[5] BMF-Schreiben vom 7. November 1995 zu den GoBS
[6] FAMA 1/1987
[7] Verlautbarung OPDV 1991
[8] TÜViT im Rahmen der Überarbeitung der Checkliste für das Projekt TRAVIC Jan 2005
[9] „Arbeitsanweisung DV09 Softwareeinsatz und Anwendungsentwicklung V01 vom 15.1.2004“ der Stadtsparkasse Augsburg
[10] „Schutzbedarfsfeststellung für IT-Anwendungen“ der Stadtsparkasse Wuppertal (Sp 860 033…) einschließlich dazugehörender Beispielfragen
[11] Definierte Einsatzbedingungen von der Konzernrevision der Deutschen Sparkassen Leasing AG & Co. KG
[12] „UHB-Sicherheitsmanagement-> IT-Sicherheitsmanagement-> Arbeitsanweisung – Freigabe von Anwendungen“ der Sparkasse Nürnberg
[13] WS IT-Revision Kiel vom 10.5.2004 der Sparkassenakademie Schleswig-Holstein
[14] Datenbanktitel: Handbuch DV-Prüfung/IR (vom FA OPDV, Anm. d. Red.)
Datenbankname: HB-DVPK.NSF
Freigabedatum: Freigabe mit Stand 10/99 erfolgte am 11.10.99
[15] Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954), neu gefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), geändert durch § 13 Abs. 1 des Gesetzes vom 5. September 2005 (BGBl. I S.2722) sowie durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970) Aktualisierte, nicht amtliche Fassung Stand: 26.08.2006
[16] AE-Modell des SIZ
[17] Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung (OPDV); Stellungnahme Nr. 1/2006; Anforderungen an einen ordnungsgemäßen Programmeinsatz; Stand Juli 2006
[18] BITKOM Publikation „Compliance in IT-Outsourcing-Projekten - LEITFADEN zur Umsetzung rechtlicher Rahmenbedingungen“ (siehe)
[19] [= FAIT1] IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1); (Stand: 24.09.2002): Verabschiedet vom Hauptfachausschuss (HFA) am 24.09.2002
[20] [= IIR2] Deutsches Institut für Interne Revision (IIR) - IIR Revisionsstandard Nr. 2 - Prüfung des Risikomanagements durch die Interne Revision
[= IIR-QA] Leitfaden QA ©2007, download unter http://www.iir-ev.de/deutsch/iir/-berufsgrundlagen/QALeitfaden08.pdf
[21] [= FAIT2] Entwurf IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW ERS FAIT 2) (Stand: 01.07.2002)
[22] [= GPSG] Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz - GPSG) GPSG - Ausfertigungsdatum: 06.01.2004
[23] [= COBIT4.0] COBIT 4.0, deutsche Ausgabe der KPMG in der Version vom 14.5.2007
[24] [= COBIT4.1] COBIT 4.1, IT Governance Institute - 3701 Algonquin Road, Suite 1010 - Rolling Meadows, IL 60008 USA - Phone: +1.847.590.7491 - Fax: +1.847.253.1443 - E-mail: info@itgi.org - Web site: www.itgi.org, Ausgabe 2007
[25] [=SITB] Sicherer IT-Betrieb, Version 4.1 vom 3.11.2005; Herausgeber SIZ
[26] IT-Revision, Schriftlicher Lehrgang in 10 Lektionen, Management Circle Edition, 1. Auflage (2007)
[27] Fachtagung IT-Revision: Impulse für die tägliche Arbeit, Sparkassenakademie Bonn 30.10.07
[28] SVN Prüfungsstellen, Checkliste für IT-Prüfungen, CL Softwarebeschaffung.doc

[29] BaFin Rundschreiben vom 30.10.2007, Rundschreiben 5/2007 (BA), Mindestanforderungen an das Risikomanagement (MaRisk)

[30] BSI: Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären – Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen

[31] [=DGCK] Deutscher Corporate Governance Kodex (in der Fassung vom 14. Juni 2007) der Regierungskommission Deutscher Corporate Governance Kodex

[32] [=GAIT] "The GAIT Principles" (Stand 2. Jan. 2007) und "The GAIT Methodology" (Stand Jan. 2007)

[33] [=GS-KAT] IT-Grundschutz-Kataloge, deutsch: Stand 2006 - 8. Ergänzungslieferung

[34] [=IDW EPS 850] Entwurf IDW Prüfungsstandard: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie (IDW EPS 850) (Stand: 19.09.2007)

[35] [=HGrG] Gesetz über die Grundsätze des Haushaltsrechts des Bundes und der Länder (Haushaltsgrundsätzegesetz - HGrG) zuletzt geändert 31. Oktober 2006

[36] [=ISACA] der Berufsverband der EDV-Revisoren und IT-Sicherheitsmanager, ISACA Germany Chapter e. V., Eichenstrasse 7, 46535 Dinslaken hat als Berufsverband der IT-Revisoren und IT-Sicherheitsmanager Berufsstandards herausgegeben (http://www.isaca.de/grundlagen_standards_dl.php):
[ISACA-S1] = IS AUDITING STANDARD „AUDIT-CHARTA",
[ISACA-S2] = „UNABHÄNGIGKEIT",
[ISACA-S3] = „BERUFSETHIK UND STANDARDS",
[ISACA-S4] = „FACHKOMPETENZ",
[ISACA-S5] = „PLANUNG",
[ISACA-S6] = „AUSFÜHRUNG DER REVISIONSARBEITEN",
[ISACA-S7] = „BERICHTERSTATTUNG",
[ISACA-S8] = „NACHSCHAU",
[ISACA-R] = „IS Verfahren zur Risikobewertung" und
[ISACA-B] = „#060.020.092: Internet Banking"

[37] [=SOX] The Sarbanes-Oxley Act 2002

[38] [=COSO-Z-SPC] : COSO-Leitfaden zur Internen Kontrolle der Finanzberichterstattung bei kleineren Aktiengesellschaften (2006), Zusammenfassung. Download unter: http://www.coso.org/Publications/erm_sb/SB_Executive_Summary_German.pdf

[39] REVISIONSSYMPOSIUM NEUE ZIELE - NEUE WEGE FÜR DIE INTERNE REVISION 23. und 24. April 2008 in Bad Homburg v. d. Höhe
Vortrag: Auslagerungen von Geschäftsbereichen im Fokus der Internen Revision; Dr. Josef Kokert, Bundesanstalt für Finanzdienstleistungen

[40] REVISIONSSYMPOSIUM, Vortrag: Prüfung des Datenschutzes Einhaltung der Vorgaben des BDSG und Funktionsfähigkeit des Datenschutzmanagements als Vorbereitung für § 44 KWG-Prüfungen der BaFin
Dipl.-Ökonom Peter Krammig, Leiter Revision Deutsche Leasing AG, Bad Homburg v. d. Höhe und Dipl. Kfm. Christof Rietzke (CISA), Bereichsleiter und Prokurist S-Consit, Bad Oldesloe

[41] REVISIONSSYMPOSIUM, Vortrag: MiFID - (Markets in Financial Instruments Directive) Neue Prüfungserfordernisse für die Interne Revision? © Walter Ullrich + Matthias Korinth, Haspa

[42] Kongress: Testing & Finance 2008, 2.+3. Juni 2008, Frankfurt mit geschlossenem VÖB-Service-Kongres
//BATH//: Graham Bath, Performance Testing as a Life-Cycle activity
//KAZMEIER//: Rechtsanwältin Dana Kazmeier, VÖB-Service GmbH, Praxis des IT-Rechts VÖB-Service-DLK

[43] [=UVV-KASSEN] hier: BGV C9 - Kassen - Berufsgenossenschaftliche Vorschriften (BGV) (vormals VBG 120) (10/1988; 01/1997; 03/2002), Stand 21.05.2008.

[100] Pflichtenheft, Version 1.0, Datum 9.2.2009
03.03.2009 17:00 245.782 Pflichtenheft_MBS_ArciSoft_V1-0.pdf

[101] ArciSoft 3, Archiv-Software - Beschreibung
http://dc-ltd.de/produkte/arcisoft/ArciSoftA4.pdf

[102] ArciSoft 3 Flyer
http://www.soultek.de/produkte/arcisoft/ArciSoft_Flyer.pdf

[103] ArciSoft 3, Archiv-Software – Beschreibung
(enthält im Gegensatz zu [101] auf S. 3 den Hinweis, dass Dokumente mit kurzen Archivierungsfristen nicht durch die IT-Anwendung behandelt werden können)

4 INDEX

5 Unterschrift

Bonn, Freitag, 6. März 2009	Dipl. Inform. Bernhard König (Prüfer)	Gerald Schmidhuber (Qualitätssicherung des vorliegenden Testates, siehe Änderungshistorie)