

Software-Zertifizierung nach IDW PS 880

Dr. Mathias Philipp
KPMG Mannheim

ABSTRACT

Der Beitrag unterscheidet zunächst zwischen prozeß- und produktorientierten Software-Zertifizierungsmethoden. Es erfolgt eine Einordnung dieser Methoden in die Revisionstheorie. Es werden kurz die häufig in der Praxis anzutreffenden Ansätze der Software-Zertifizierung nach der Software-Prüfungsrichtlinie RAL-GZ 901 der Gütegemeinschaft Software e.V. (entspricht DIN 66 285) und nach ISO 9000 dargestellt (Kapitel 1). In Kapitel 2 wird der Prüfungsstandard IDW PS 880 „Erteilung und Verwendung von Softwarebescheinigungen“ des Instituts der Wirtschaftsprüfer ausführlich dargestellt. In Kapitel 3 erfolgt eine abschließende Würdigung des IDW PS 880.

ABSTRACT

This paper first distinguishes between process- and product-oriented software certification methods. These methods are then related to audit theory. Chapter 1 briefly describes the standards often used in practice to certify software according to RAL-GZ 901 of Gütegemeinschaft Software e.V. (corresponding to DIN 66 285) and ISO 9000. In chapter 2 the auditing standard IDW PS 880 "Issue and use of software certifications" of the German Institute of Auditors (Institut der Wirtschaftsprüfer) is presented in detail. Chapter 3 offers concluding remarks on the advantages of the auditing standard IDW PS 880.

KEYWORDS: Softwarezertifizierung, Softwaretestat, ISO 9000, Softwarequalität, Prospektprüfung

1 PROZESS- UND PRODUKTORIENTIERTE SOFTWARE-ZERTIFIZIERUNG

1.1 Prozeßorientierte Software-Zertifizierung

Bei der prozeßorientierten Software-Zertifizierung wird die Aufbau- und Ablauforganisation des „Produktionsprozesses“ der Softwareerzeugung beurteilt. Es wird das System der Softwareproduktion betrachtet. Entspricht dieses System bestimmten formalen Anforderungen, wird auf die Güte der Produktionsergebnisse „Software“ geschlossen. Ein Normenwerk für eine solche Prozeßzertifizierung liefert ISO 9000 [Mell97]. „Für die Entwicklung, Lieferung und Wartung von Software existiert seit 1991 ein Leitfaden ISO 9000-3, der seit Juni 1992 als DIN ISO 9000 Teil 3: Leitfaden für die Anwendung von ISO 9001 auf die Entwicklung, Lieferung und Wartung von Software verfügbar ist [DIN92b].“ [Grie93, 579]

Insbesondere in Kapitel 5 „Qualitätssicherungssystem - Lebenszyklustätigkeiten“ von ISO 9000-Teil 3 werden Software-Lebenszyklusorientierte Qualitätssicherungsmaßnahmen beschrieben. Diese beschreiben in 10 Unterkapiteln die vorzusehenden Maßnahmen in den Phasen Vertragsüberprüfung, Festlegung der Forderungen des Auftraggebers, Planung der Entwicklung, Planung der Qualitätssicherung, Design und Implementierung, Testen und Validierung, Annahme, Vervielfältigung, Lieferung und Installation sowie Wartung.

Zu beachten ist, daß keine Prüfung eines konkreten Softwareproduktes anhand von Software-Qualitätsmerkmalen erfolgt, da ISO 9000 allgemein keine Qualitätseigenschaften und damit insbesondere auch keine Software-Qualitätseigenschaften definiert.

1.2 Produktorientierte Software-Zertifizierung

Bei der produktorientierten Software-Zertifizierung werden konkrete Qualitätseigenschaften von der Software gefordert. Diese Eigenschaften müssen zunächst unabhängig vom Softwareherstellungsprozess gegeben sein. Da aber Eigenschaften wie beispielsweise Wartbarkeit oder Portabilität in der Regel nur bei einer bestimmten Qualität des Herstellungsprozesses erreicht werden können, sind über Produkteigenschaften auch Rückschlüsse auf den Herstellungsprozess möglich; oder vice versa wie dies bei der prozeßorientierten Software-Zertifizierung geschieht [Abs. 1.1].

Als Beispiel für eine produktorientierte Software-Zertifizierung soll die sogenannte „Prospektprüfung“ nach RAL-GZ 901 gegeben werden [RAL901, Schm88]. Ziel von RAL-GZ 901 ist die vollständige Übereinstimmung des Softwareproduktes mit der Produktbeschreibung. „Die Güte- und Prüfbestimmungen sollen sicherstellen, daß die geprüfte Software samt Dokumentation mit den Herstellerangaben laut Produktbeschreibung übereinstimmen [sic!]. ... Nicht geprüft werden die Sicherheitstechnik und der Datenschutz ...“ [Schu98, 798]. Eigenschaften wie etwa Wartbarkeit oder Zuverlässigkeit werden nur dann in die Prüfung miteinbezogen, wenn sie in der Produktbeschreibung aufgeführt werden.

1.3 Revisionsmethodische Einordnung der Zertifizierungsansätze

Revisionsmethodisch handelt es sich bei der prozeßorientierten Software-Zertifizierung um eine sogenannte „Systemprüfung“ (Abbildung 1). Das System der Softwareherstellung wird beurteilt, um mit diesem Urteil auf die Qualität des Ergebnisses „Software“ zu schließen. Bei der produktorientierten Software-Zertifizierung handelt es sich um eine „ergebnisorientierte Prüfung“. Das System der Softwareherstellung wird als Black-Box behandelt. Was beurteilt wird, ist ausschließlich das Ergebnis; in diesem Fall das Softwareprodukt.

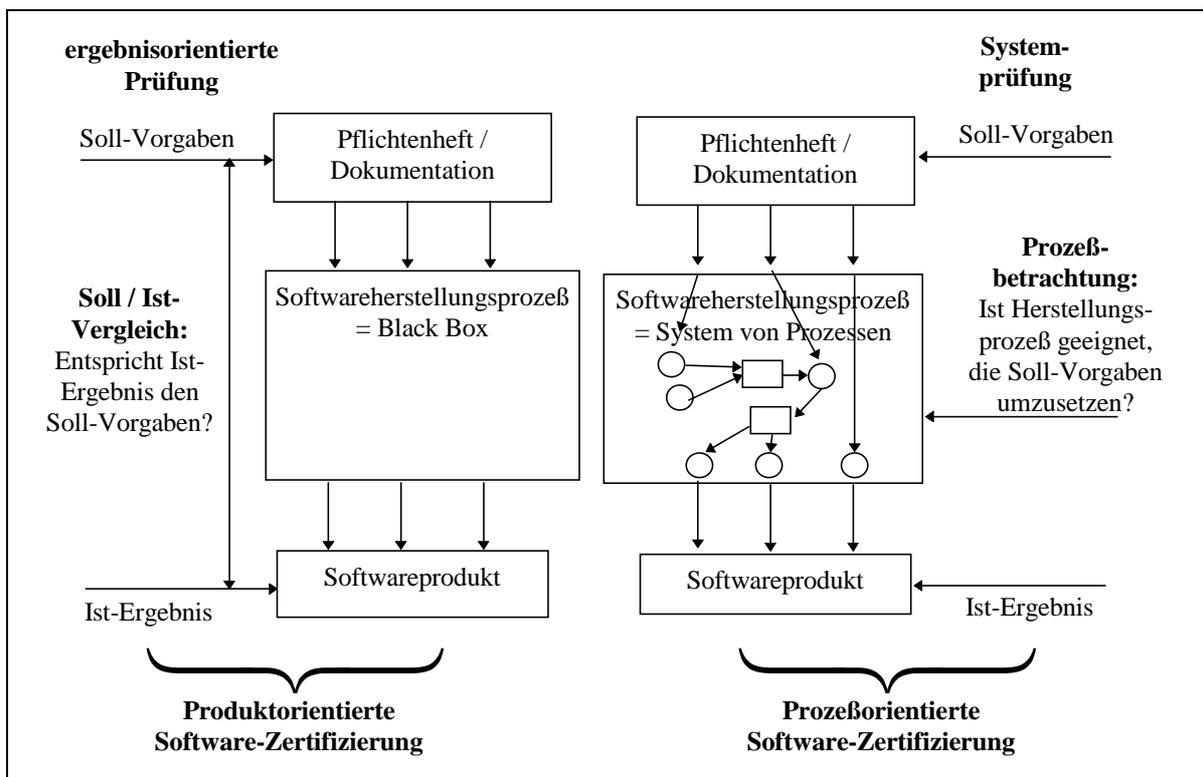


Abbildung 1: Systemprüfung und ergebnisorientierter Prüfungsansatz

In der Revisionstheorie wurden unter dem Begriff „systemorientierte Prüfung“ Ansätze entwickelt, die eine Hintereinanderschaltung der beiden Ansätze „Systemprüfung“ und „ergebnisorientierte Prüfung“

vorsehen: In Abhängigkeit von den Ergebnissen der Systemprüfung werden die ergebnisorientierten Prüfungshandlungen intensiviert oder verringert [vgl. Phil99, Kap. 5.3.2]. Werden beispielsweise bei der Systemprüfung bestimmte Schwächen im Herstellungsprozeß identifiziert, wird die Anzahl der Testfälle erhöht, die genau auf diesen Schwachpunkt abzielen (Erhöhung der ergebnisorientierten Prüfungshandlungen). Entsprechend kommt es zu einer Verringerung der Testfälle, falls den Herstellungsprozeß ein ausgereifter Qualitätssicherungsprozeß begleitet.

Wie in Abschnitt 1.2 angedeutet, ist grundsätzlich auch eine umgekehrte Vorgehensweise denkbar. Aufbauend auf ergebnisorientiert entdeckten Qualitätsmängeln werden die Ursachen hierfür im Herstellungsprozeß lokalisiert. Diese Vorgehensweise kann jedoch bei punktuellen und meist unter Zeitdruck stattfindenden Zertifizierungen oft nicht realisiert werden. Vielmehr sollte es Teil des Qualitätsmanagements beim Softwarehersteller sein.

2 ZERTIFIZIERUNG NACH IDW PS 880

In IDW PS 880 definiert das Institut der Wirtschaftsprüfer einen Prüfungsstandard für die Erteilung und Verwendung von Softwarebescheinigungen. Der Prüfungsstandard ist produktorientiert, da die Erfüllung konkreter Eigenschaften gefordert wird, die sich an der Erfüllung des unbestimmten Rechtsbegriffs „Grundsätze ordnungsmäßiger Buchführung“ (GoB) ausrichten. Unter Einbeziehung von Fachgutachten 1/1988 „Grundsätze ordnungsmäßiger Durchführung von Abschlußprüfungen“ [FG1/88] und dessen Ausstrahlung auf alle Tätigkeiten eines Wirtschaftsprüfers sowie den fachlichen Stellungnahmen zur Prüfung der ordnungsmäßigen Anwendung von Software [FAMA93] ist der (Software-) Prüfer jedoch gehalten, prüfungsmethodisch systemorientiert im Sinne von Abschnitt 1.3 vorzugehen. Neben dieser berufsständisch formalen Argumentation ist diese Prüfungsmethode auch aus Wirtschaftlichkeitsüberlegungen heraus geboten.

2.1 Prüfungsgegenstand, Geltungsbereich und Aussagekraft

IDW PS 880 „zeigt die Anforderungen auf, die bei der Prüfung von Softwareprodukten und der Erteilung von Bescheinigungen zu Softwareprodukten zu beachten sind, wenn diese für die Ordnungsmäßigkeit der Rechnungslegung von Bedeutung sind“ [PS880, 597]. Prüfungsgegenstand ist damit die Beurteilung der Einhaltung der Grundsätze ordnungsmäßiger Buchführung. Wie in [Phil98, Phil96] hergeleitet, unterliegen nahezu alle betrieblichen Informationssysteme den Ordnungsmäßigkeitsanforderungen des Handels- und Steuerrechts und sind damit für die Rechnungslegung von Bedeutung. Das Bundesministerium der Finanzen begründet dies in den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme [GoBS95] im wesentlichen damit, daß durch Informationssysteme auch außerhalb des eigentlichen Buchhaltungsbereichs rechnungslegungsrelevante Daten erfaßt, erzeugt, bearbeitet oder übermittelt werden: „In einem DV-gestützten Buchführungssystem sind auch solche Prozesse zu berücksichtigen, in denen außerhalb des eigentlichen Buchhaltungsbereiches buchführungsrelevante Daten erfaßt, erzeugt, bearbeitet und / oder übermittelt werden.“ [GoBS95: Tz.1.1] Die GoBS spezifizieren die GoB, falls die Buchführung DV-gestützt erfolgt.

Insgesamt bleibt somit festzuhalten, daß im betrieblichen Anwendungsumfeld kaum Software zu finden sein wird, die nicht unter den Anwendungsbereich der GoBS und damit der GoB fällt. Daraus folgt, daß der Prüfungsstandard IDW PS 880 auf nahezu jede betriebswirtschaftliche Software angewendet werden kann und sollte.

Die Aussagekraft einer Software-Zertifizierung nach IDW PS 880 läßt sich am besten aus der Formulierung des Prüfungsergebnisses ableiten: „Die von mir/uns geprüfte rechnungslegungsrelevante Software (Release/Version-Nr. ..., über deren Prüfung ich/wir mit Datum vom ... einen Bericht erstattet habe(n), ermöglicht bei sachgerechter Anwendung eine den Grundsätzen ordnungsmäßiger Buchführung entsprechende Rechnungslegung.“ [PS880, 603] Die häufig in der Praxis vertretene Meinung, daß zertifizierte Software in der betrieblichen Anwendungspraxis nicht mehr zu prüfen sei, ist damit nicht richtig, da die Zertifizierung nicht die sachgerechte Anwendung der Software miteinschließt. Anforderungen an die sachgerechte Anwendung der Software sind in [FAMA93, GoBS95] sowie deren Umsetzung im Informationssystem-Lebenszyklus in [Phil98] beschrieben.

Beispielsweise beinhaltet dies ein ordnungsmäßiges Customizing oder ein adäquates Berechtigungs- und Sicherheitskonzept [vgl. PhHo99].

2.2 Vorarbeiten

Zunächst sieht der IDW PS 880 eine Bestandsaufnahme des Zertifizierungsobjektes sowie der Zertifizierungsumgebung vor. Es ist genau festzuhalten, um welche Version (Releasestand, Puplevel, HotPacket) es sich bei der zu zertifizierenden Anwendungssoftware handelt. In der gleichen Weise ist die Testumgebung (Hardware, Betriebssystem, Netzwerksoftware, Datenbanksystem) zu erfassen. Soll die Anwendungssoftware beispielsweise für mehrere Betriebssysteme zertifiziert werden, sind entsprechend mehrere Testumgebungen zu beschreiben.

Im weiteren werden bei der Zertifizierung die Bereiche der Abbildung 2 geprüft.

2.3 Verarbeitungsfunktionen

Es sind die Verarbeitungsfunktionen festzustellen, die mindestens notwendig sind, um die handels- und steuerrechtlichen Ordnungsmäßigkeitsanforderungen zu erfüllen. Wie in [Phil98, Phil96] hergeleitet, sind allgemein folgende Ordnungsmäßigkeitsanforderungen zu erfüllen (vgl. Abbildung 3):

- (i) Die Nachvollziehbarkeit des Verfahrens, das durch die Verarbeitungsfunktionen realisiert wird.
- (ii) Die Nachvollziehbarkeit der Geschäftsvorfälle.
- (iii) Ordnungsmäßige Anwendung der Verarbeitungsverfahren.

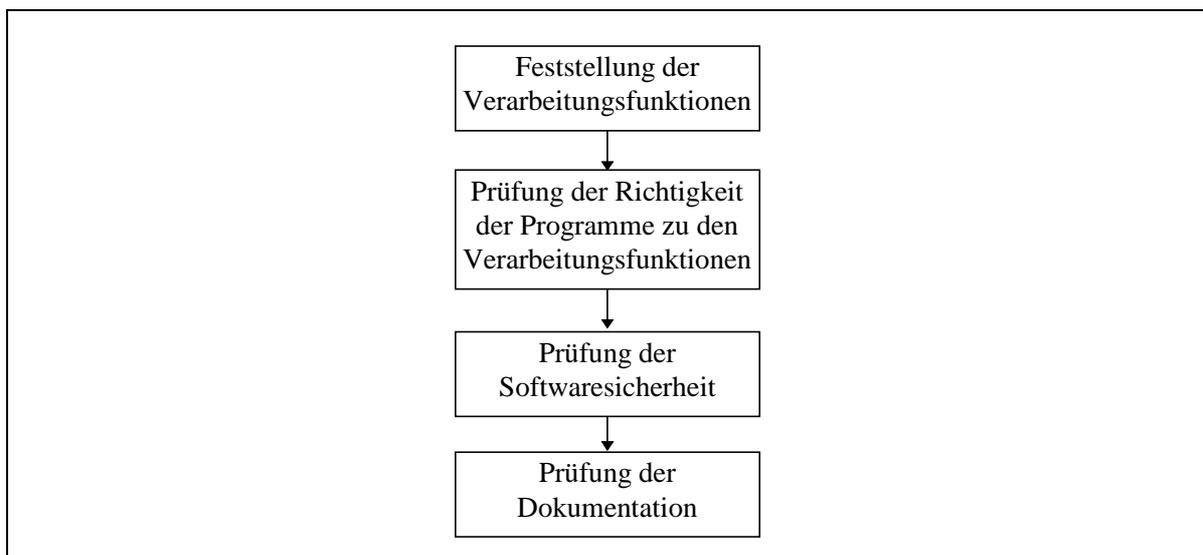


Abbildung 2: Ablauf der Software-Zertifizierung nach IDW PS 880

In [GoBS95] wird dargestellt, wie diese Ordnungsmäßigkeitsanforderungen umzusetzen sind. Es wird ausführlich auf die sogenannte Beleg-, Journal- und Kontenfunktion als Grundlage zur Erfüllung von (ii) eingegangen. Zur Sicherstellung von (iii) wird die Einrichtung eines Internen Kontrollsystems sowie das Vorhandensein einer Anwenderdokumentation gefordert. Für (i) ist eine Systemdokumentation erforderlich.

Da gemäß [GoBS95, Tz.9] die Erfüllung dieser Ordnungsmäßigkeitsanforderungen durch den Anwender nachzuweisen ist, muß der Softwarehersteller Funktionen bereitstellen, die es dem Anwender ermöglichen, diese Anforderungen umzusetzen. Der IDW PS 880 geht deshalb ausführlich

auf die notwendigen Funktionalitäten zur Erfüllung der Beleg-, Journal- und Kontenfunktion sowie auf Sicherheits- und Dokumentationsanforderungen ein.

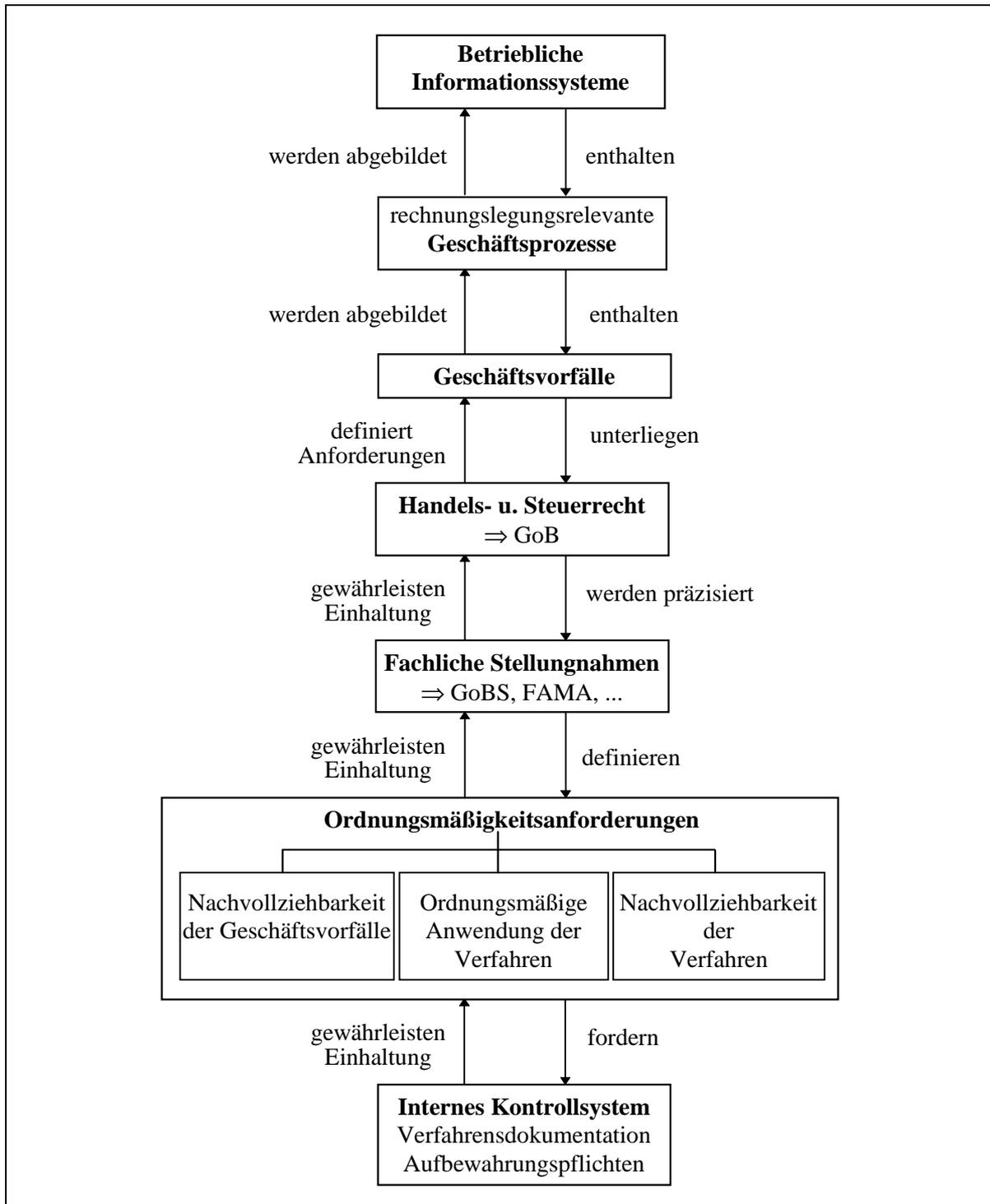


Abbildung 3: Ordnungsmäßigkeitsanforderungen an betriebliche Informationssysteme, in Anlehnung an [Phil98, 314].

Es sind somit zunächst die in der Software zur Verfügung gestellten Verarbeitungsfunktionen aufzunehmen und es ist zu beurteilen, ob diese überhaupt geeignet sind, die Ordnungsmäßigkeits-

anforderungen umzusetzen. Die Beurteilung erfolgt auf Basis der System- und Anwenderdokumentation [vgl. Kap. 2.5].

Anschließend ist die richtige programmtechnische Umsetzung der Verarbeitungsfunktionen zu prüfen. Dazu kann gemäß IDW PS 880 in starkem Umfang auf die Testdatenbank des Herstellers zurückgegriffen werden. Die Durchführung von durch den Prüfer erstellten Testfällen ist darüber hinaus verpflichtend. Insgesamt müssen die Testfälle „die wesentlichen, in der Dokumentation beschriebenen Funktionen abdecken und die für die Arbeitsaufgabe repräsentativen Kombinationen von Funktionen berücksichtigen.“ [PS880] Testfälle sollen auch fehlerhafte Datenkombinationen enthalten, um zu prüfen, ob diese vom System abgewiesen oder korrigiert werden.

Da in der Regel (integrierte) Softwarepakete aus verschiedenen Modulen bestehen, sind darüber hinaus Testfälle zu berücksichtigen, die die korrekte Zusammenarbeit der verschiedenen Module prüfen (Integrationstests).

Eine Prüfung der Verarbeitungsfunktionen anhand der Quellprogramme ist gemäß IDW PS 880 nur in Ausnahmefällen als Ergänzung zu obigen Tests erforderlich.

2.4 Softwaresicherheit

In [Phil99] wird gezeigt, daß Anwender neben dem deutschen Recht [insbes. GoBS] auch nach internationalen Normen verpflichtet sind, ein Internes Kontrollsystem einzurichten. Auf der Ebene der zu zertifizierenden Software betrifft dies

- die Einrichtung eines differenzierten Zugriffsschutzes,
- die Unterstützung von Datensicherungsmaßnahmen und
- Recovery-Möglichkeiten (Wiederanlaufverfahren).

Der Zugriffsschutz soll insbesondere eine Funktionstrennung von unter Kontrollaspekten unvereinbaren Tätigkeiten ermöglichen und hat sich, soweit möglich, auf die Betriebssystem-, Datenbank- und Netzwerkebene zu erstrecken. Insgesamt werden aber keine höheren Anforderungen gestellt, als nach dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik [BSI98] vorgesehen [vgl. Petz99].

2.5 Dokumentation

Das Vorhandensein einer aussagefähigen Verfahrensdokumentation ist eine wesentliche Voraussetzung für die Nachvollziehbarkeit und damit Prüfbarkeit der Software und stellt eine Grundlage für die sachgerechte Anwendung der Software beim Anwender dar [PS880, 601]. In IDW PS 880 wird unterschieden zwischen System- und Anwenderdokumentation. Bezüglich Umfang und Gestaltung der Dokumentation bestehen grundsätzlich keine Vorschriften. Jedoch werden die in [FAMA93] und [GoBS95] aufgestellten Mindestanforderungen in IDW PS 880 übernommen sowie generelle Anforderungen wie Aktualität, Vollständigkeit, Fehlerfreiheit, Verständlichkeit und Übersichtlichkeit formuliert.

„Eine nicht vorliegende Dokumentation oder eine nur unzureichende Dokumentation stellt einen schwerwiegenden Mangel dar und hat die Versagung der Softwarebescheinigung zur Folge.“ [PS880, 602]

2.6 Software-Zertifikat und Nutzung für Werbezwecke

Das Software-Zertifikat besteht aus einem Bericht, der im wesentlichen aus folgenden Teilen besteht:

2.7 Folgezertifizierungen

Bei Folgeversionen sind lediglich die geänderten Softwareteile und deren Auswirkung auf die bereits zertifizierte Software zu prüfen.

3 RESÜMEE

Es wurde gezeigt, daß der IDW PS 880 auf nahezu jede betriebswirtschaftliche Anwendungssoftware angewendet kann (Abschn. 2.1). Des weiteren deckt dieser Zertifizierungsstandard ein breiteres Prüfungsspektrum ab als beispielsweise die Prüfung nach RAL-GZ 901. IDW PS 880 ist ein produktorientierter Prüfungsstandard, in dem aber die Überlegungen einer prozeßorientierten Prüfung z.B. nach ISO 9000-3 enthalten sind. Auch wenn sich der IDW PS 880 zunächst an rechnungslegungsrelevante Software richtet, kann dieser Prüfungsstandard auch als Orientierung für nicht-rechnungslegungsrelevante Software herangezogen werden.

AUTOR UND BIOGRAPHIE

Dr. Mathias Philipp, wohnhaft in Haardtstraße 18, 68163 Mannheim, studierte bis 1992 an der Universität Mannheim Wirtschaftsinformatik. Von 1992 bis 1997 arbeitete er als wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsinformatik (Professor Müller) der Johann Wolfgang Goethe-Universität, Frankfurt a.M. Das Thema seiner Doktorarbeit lautet „Analyse und Konfiguration betrieblicher Abläufe unter Revisionsaspekten“ [Phil99]. Von 1994 bis 1998 arbeitete er auch als freiberuflicher IT-Auditor und IT-Consultant für die KPMG Deutsche Treuhand-Gesellschaft AG Wirtschaftsprüfungsgesellschaft, Mannheim. Das Berufsexamen zum Certified Information Systems Auditor (CISA) legte er vor der amerikanischen Information Systems Audit and Control Association (ISACA) 1995 ab. Seit 1998 ist er als Prokurist und Manager bei KPMG Mannheim im Angestelltenverhältnis tätig. Er ist dort Leiter der Abteilung „Information Risk Management“. Darüber hinaus ist er als Autor zahlreicher Fachartikel und als Fachreferent bekannt.

e-mail: mphilipp@mphilipp.de
<http://www.mphilipp.de>

LITERATUR

- [Acke98] Acken, Jan van: Testate - Nutzen oder Augenwischerei, in: ReVision 1/1998, S. 52-53
- [BSI98] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch, 1998; <http://www.bsi.de/gshb/>
- [DIN92b] Deutsches Institut für Normung e.V. (Hrsg.): DIN ISO 9000 Teil 3 - Leitfaden für die Anwendung von ISO 9001 auf die Entwicklung, Lieferung und Wartung von Software, Berlin, 1992
- [FAMA93] Fachausschuß für moderne Abrechnungssysteme (FAMA) 1/1987: Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung, i.d.F. 11/1993, in: FN-IDW 11/1993, S. 462-476
- [FG1/88] IDW (Hrsg.): Fachgutachten 1/1988 - Grundsätze ordnungsmäßiger Durchführung von Abschlußprüfungen, in: Die Wirtschaftsprüfung, 1-2/1989, S. 9-19
- [GoBS95] Schreiben des Bundesministeriums der Finanzen vom 7. November 1995: Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), in: Bundessteuerblatt 1995, Teil 1, Nr. 18, S. 738-747; <http://www.wiwi.uni-frankfurt.de/~mphilipp/papers/gobs.doc>
- [Grie93] Griese Joachim: Der Beitrag von ISO 9000 zur Software-Qualitätssicherung, in: Wirtschaftsinformatik, 6/1993, S. 575-585
- [Koch85] Koch, Bernd: Das Software-Testat - Probleme bei der Prüfung von Buchhaltungssoftware, in: Die Wirtschaftsprüfung 24/1985, S. 645-652
- [Mell97] Mellis, Werner: Softwarequalität und Softwarequalitätsmanagement, in: Lexikon der Wirtschaftsinformatik, P. Mertens (Hrsg.), 2. Aufl., Berlin, 1997, S. 369-370
- [Petz99] Petzel, Erhard: SAP-Sicherheit und IT-Grundschutz, in: ReVision 1/1999, S. 5-9

- [PhHo99] Philipp, Mathias; Horschler, Marcus: Projektbegleitende Prüfung von Migrationsprojekten: Rechtliche Grundlagen und Umsetzung bei einer SAP R/3-Migration, in: 3. GI-Fachtagung Management und Controlling von IV-Projekten, Glashütten (Taunus), März 1999, S. 92-102; http://www.wiwi.uni-frankfurt.de/~mphilipp/papers/gi_migra.pdf
- [Phil96] Philipp, Mathias: Aus Handels- und Steuerrecht abgeleitete Anforderungen an Geschäftsprozessmodelle und Workflow-Managementsysteme, in: EMISA 1995 - Requirement Engineering für Informationssysteme, A. Oberweis (Hrsg.), Karlsruhe, 1995, S. 47-54; <http://www.wiwi.uni-frankfurt.de/~mphilipp/papers/emisa96.pdf>
- [Phil98] Philipp, Mathias: Ordnungsmäßige Informationssysteme im Zeitablauf - Umsetzung der GoBS im Informationssystem-Lebenszyklus, in: Wirtschaftsinformatik 4/1998, S. 312-317; http://www.wiwi.uni-frankfurt.de/~mphilipp/papers/wi4_98.pdf oder <http://www.wirtschaftsinformatik.de/wi/preprints.htm>
- [Phil99] Philipp, Mathias: Analyse und Konfiguration betrieblicher Abläufe unter Revisionsaspekten, Frankfurt, Univ., Diss., 1999; erscheint in: Hamburg: Ottokar Schreiber, 1999 http://www.wiwi.uni-frankfurt.de/~mphilipp/papers/abstract_diss.pdf sowie <http://www.mphilipp.de/papers/disspraesent.zip>
- [PS880] IDW-Prüfungsstandard - Erteilung und Verwendung von Softwarebescheinigungen (IDW PS 880), in: FN-IDW 12/1998, S. 597-604
- [RAL901] RAL Deutsches Institut für Gütesicherung und Kennzeichnung (Hrsg.): Güte- und Prüfbestimmungen Software, Berlin 1985; siehe auch <http://www.ral.de/RALg68.htm>
- [Schm88] Schmidt, Klaus P.: Rahmenprüfplan für Software: Formblätter und Anleitung für Prüfungen von Software nach den Güte- und Prüfbestimmungen Software RAL-GZ 901 und der Vornorm DIN 66 285 „Anwendungssoftware, Prüfungsgrundsätze“, Sankt Augustin: Arbeitspapier 312 der GMD, 1988
- [Schu98] Schuppenhauer, Rainer: Grundsätze für eine ordnungsmäßige Datenverarbeitung (GoDV) - Handbuch der DV-Revision, 5. Aufl., Düsseldorf, 1998