Institut der Wirtschaftsprüfer - Hauptfachausschuss (HFA)
Aufsatz vom 24.09.2002 0568258

IDW-RS-FAIT-1 - IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)

(Stand: 24.09.2002) [1]

1. Vorbemerkungen

(1) Die Grundsätze ordnungsmäßiger Buchführung schreiben kein bestimmtes Buchführungsverfahren vor. Sie lassen jedes Verfahren - auch auf Informationstechnologie gestützte Systeme - zu, wenn dies die Anforderungen erfüllt, die durch die Grundsätze ordnungsmäßiger Buchführung an das Verfahren gestellt werden (§ 239 Abs. 4 HGB).

(2) Unter Informationstechnologie (IT) wird in dieser IDW Stellungnahme zur Rechnungslegung die Gesamtheit der im Unternehmen zur elektronischen Datenverarbeitung eingesetzten Hard- und Software verstanden.

(3) Diese IDW Stellungnahme zur Rechnungslegung konkretisiert die aus den §§ 238, 239 und 257 HGB resultierenden Anforderungen an die Führung der Handelsbücher mittels IT-gestützter Systeme und verdeutlicht die beim Einsatz von IT möglichen Risiken für die Einhaltung der Grundsätze ordnungsmäßiger Buchführung.

(4) Wirtschaftszweigspezifische und sonstige Besonderheiten, die im Einzelfall zu berücksichtigen sind, bleiben in dieser IDW Stellungnahme zur Rechnungslegung grundsätzlich außer Betracht.

(5) Die IDW Stellungnahme zur Rechnungslegung ersetzt Abschn. A. und B. der Stellungnahme FAMA 1/1987: Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung [2].

2. Das IT-System und der Einsatz von IT im Unternehmen

(6) Die gesetzlichen Vertreter haben die Verantwortung dafür, dass die Unternehmensziele in Übereinstimmung mit der von ihnen festgelegten Geschäftspolitik des Unternehmens im Rahmen der gesetzlichen Vorschriften erreicht werden. Soweit hierfür IT eingesetzt wird, haben sie geeignete Regelungen einzuführen, um die Risiken aus dem Einsatz von IT zu bewältigen.

(7) Der Einsatz von IT im Unternehmen erfolgt in Form eines IT-Systems, das zur Verarbeitung von Daten folgende Elemente beinhaltet:

- IT-gestützte Geschäftsprozesse
- IT-Anwendungen
- IT-Infrastruktur.

Das Zusammenwirken dieser Elemente wird durch das IT-Kontrollsystem bestimmt, das von dem IT-Umfeld und der IT-Organisation abhängt.

(8) Das IT-Kontrollsystem ist Bestandteil des internen Kontrollsystems (IKS). Es umfasst diejenigen Grundsätze, Verfahren und Maßnahmen (Regelungen), die zur Bewältigung der Risiken aus dem Einsatz von IT eingerichtet werden. Hierzu gehören Regelungen zur Steuerung des Einsatzes von IT im Unternehmen (internes Steuerungssystem) und Regelungen zur Überwachung der Einhaltung dieser Regelungen (internes Überwachungssystem) [3]

IT-Kontrollen sind Bestandteil des internen Überwachungssystems. Zu ihnen zählen die in IT-Anwendungen enthaltenen Eingabe-, Verarbeitungs- und Ausgabekontrollen sowie alle im IT-System vorgesehenen prozessintegrierten Kontrollen und organisatorischen Sicherungsmaßnahmen wie z.B. Zugriffskontrollen oder Netzwerkkontrollen auf der Ebene der IT-Infrastruktur. Darüber hinaus gehören zu den IT-Kontrollen auch solche Maßnahmen, die sich unabhängig von der jeweiligen IT-Anwendung als generelle Kontrollen auf das gesamte IT-System auswirken (z.B. Kontrollen der Entwicklung, Einführung und Änderung von IT-Anwendungen (Change-Management)).

Die prozessunabhängigen Überwachungsmaßnahmen werden im Wesentlichen durch die Interne Revision oder unmittelbare Überwachungsmaßnahmen der gesetzlichen Vertreter durchgeführt.

(9) Durch die IT-Organisation sind die Verantwortlichkeiten und Kompetenzen im Zusammenhang mit dem Einsatz von IT im Unternehmen geregelt. Sie umfasst einerseits Regelungen für die Entwicklung, Einführung und Änderung des IT-Systems sowie andererseits Regelungen für die Steuerung des Einsatzes eines IT-Systems.

(10) Das IT-Umfeld ist geprägt durch die Grundeinstellung, das Problembewusstsein und das Verhalten der gesetzlichen Vertreter und der Mitarbeiter in bezug auf den Einsatz von IT.

(11) IT-gestützte Geschäftsprozesse i.S.d. IDW Stellungnahme zur Rechnungslegung sind die betriebswirtschaftlich oder technisch zusammengehörigen Tätigkeiten von Unternehmen, zu deren Abwicklung IT eingesetzt wird.

(12) IT-Anwendungen sind sowohl eigenerstellte Software als auch von Dritten bezogene Software, die als Individual- oder Standardsoftware für die IT-gestützte Abwicklung von Geschäftsprozessen herangezogen werden. Sie können entweder eigenständig oder im Verbund mit anderen Softwareprogrammen oder auch als integrierte Softwarelösung eingesetzt werden.

(13) Die IT-Infrastruktur umfasst alle technischen Ressourcen und den IT-Betrieb. Zu den technischen Ressourcen zählen neben baulichen und räumlichen Einrichtungen eines Rechenzentrums bzw. eines Rechnerraums die Hardware, die Betriebssystemsoftware, die für den Aufbau von internen und externen Netzen erforderlichen Kommunikationseinrichtungen sowie technische Lösungen für die Abwicklung und Unterstützung des IT-Betriebs. Unter IT-Betrieb sind Regelungen und Maßnahmen im Zusammenhang mit dem Einsatz von IT-Anwendungen zu verstehen, die die Durchführung, Aufrechterhaltung und Sicherheit der Informationsverarbeitung gewährleisten.

(14) Die Elemente des IT-Systems sind rechnungslegungsrelevant, wenn sie dazu dienen, Daten über Geschäftsvorfälle oder betriebliche Aktivitäten zu verarbeiten, die entweder direkt in die IT-gestützte Rechnungslegung einfließen oder als Grundlage für Buchungen dem Rechnungslegungssystem in elektronischer Form zur Verfügung gestellt werden (rechnungslegungsrelevante Daten). Der Begriff der Rechnungslegung umfasst dabei die Buchführung, den Jahresabschluss und den Lagebericht bzw. auf Konzernebene den Konzernabschluss und den Konzernlagebericht [4].

Die Buchführung beinhaltet das Hauptbuch und die Nebenbücher und wird immer dann berührt, wenn Geschäftsvorfälle das Vermögen oder die Schulden beeinflussen, oder diese zur Bildung von Rechnungsabgrenzungsposten, zu Aufwendungen und Erträgen oder zu erläuterungs- bzw. berichtspflichtigen Vorgängen in Jahresabschluss und Lagebericht bzw. Konzernabschluss und -lagebericht führen. Darüber hinaus kann ein IT-System zur Erstellung des Jahres- oder Konzernabschlusses und zur Abfassung zahlenmäßiger Begründungen des Lage- oder Konzernlageberichts beitragen.

3. Der Einsatz von IT in der Rechnungslegung

(15) Die Bandbreite des IT-Einsatzes in Unternehmen reicht von der Unterstützung manueller Tätigkeiten (z.B. durch PC-Standardapplikationen) bis zu komplexen IT-Systemen, die als integrierte Systeme eine einheitliche Datenbasis zur Steuerung umfassender

Unternehmensaktivitäten verwenden und durch eine weitgehende Verknüpfung von operativen und rechnungslegungsbezogenen Funktionen gekennzeichnet sind (z.B. Enterprise Ressource Planning-Systeme).

(16) Insbesondere der Einsatz integrierter Softwarelösungen führt dazu, dass rechnungslegungsrelevante Daten über betriebliche Aktivitäten direkt (ohne manuelle Eingaben) in das Rechnungslegungssystem, und damit in die IT-gestützte Rechnungslegung, Eingang finden.

(17) Die gesetzlichen Vertreter sind verantwortlich für die Erfüllung der gesetzlichen Ordnungsmäßigkeitsanforderungen, die bei der Gestaltung einer IT-gestützten Rechnungslegung zu erfüllen sind.

(18) Die Anforderungen der §§ 238, 239 und 257 HGB sind bei der Gestaltung einer IT-gestützten Rechnungslegung zu beachten. Im Einzelnen sind dies

- die Beachtung der Grundsätze ordnungsmäßiger Buchführung (§ 239 Abs. 4 HGB) und die Berücksichtigung der damit verbundenen Anforderungen an die Sicherheit IT-gestützter Rechnungslegung,
- die Nachvollziehbarkeit der Buchführungs- bzw. Rechnungslegungsverfahren (§ 238 Abs. 1 Satz 2 HGB),
- die Nachvollziehbarkeit der Abbildung der einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung (§ 238 Abs. 1 Satz 3 HGB),
- die Einhaltung der Aufbewahrungsvorschriften (§ 239 Abs. 4, § 257 HGB).

3.1. Sicherheitsanforderungen an rechnungslegungsrelevante Daten

(19) Voraussetzung für die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung ist neben der Gesetzesentsprechung des Rechnungslegungssystems die Sicherheit der verarbeiteten rechnungslegungsrelevanten Daten.

(20) Nur bei Vorliegen sicherer rechnungslegungsrelevanter Daten und IT-Systeme kann die Verlässlichkeit der in Buchführung, Jahresabschluss und Lagebericht enthaltenen Informationen gewährleistet werden [5].

(21) Hieraus folgt, dass die gesetzlichen Vertreter auch für die Einhaltung der Sicherheit der IT-Systeme und der rechnungslegungsrelevanten Daten verantwortlich sind. Dazu ist für das Unternehmen ein geeignetes Sicherheitskonzept zu entwickeln, einzuführen und aufrecht zu erhalten, das den erforderlichen Grad an Informationssicherheit gewährleistet.

(22) Das Sicherheitskonzept beinhaltet die Bewertung der Sicherheitsrisiken aus dem Einsatz von IT aus Sicht der gesetzlichen Vertreter und daraus abgeleitet die technologischen und organisatorischen Maßnahmen, um eine angemessene IT-Infrastruktur für die IT-Anwendungen zu gewährleisten sowie die ordnungsmäßige und sichere Abwicklung der IT-gestützten Geschäftsprozesse sicherzustellen.

(23) IT-Systeme haben daher die folgenden Sicherheitsanforderungen zu erfüllen:

- Vertraulichkeitverlangt, dass von Dritten erlangte Daten nicht unberechtigt weitergegeben oder veröffentlicht werden. Organisatorische und technische Maßnahmen - wie bspw. Verschlüsselungstechniken - umfassen u.a. Anweisungen zur Beschränkung der Übermittlung personenbezogener Daten an Dritte, die verschlüsselte Übermittlung von Daten an berechtigte Dritte, die eindeutige Identifizierung und

Verifizierung des Empfängers von Daten oder die Einhaltung von Löschfristen gespeicherter personenbezogener Daten.

- Integritätvon IT-Systemen ist gegeben, wenn die Daten und die IT-Infrastruktur sowie die IT-Anwendungen vollständig und richtig zur Verfügung stehen und vor Manipulation und ungewollten oder fehlerhaften Änderungen geschützt sind. Organisatorische Maßnahmen sind geeignete Test- und Freigabeverfahren. Technische Maßnahmen sind z.B. Firewalls und Virenscanner. Die Ordnungsmäßigkeit der IT-gestützten Rechnungslegung setzt voraus, dass neben den Daten und IT-Anwendungen auch die IT-Infrastruktur nur in einem festgelegten Zustand eingesetzt wird und nur autorisierte Änderungen zugelassen werden.
- Verfügbarkeitverlangt zum einen, dass das Unternehmen zur Aufrechterhaltung des Geschäftsbetriebs die ständige Verfügbarkeit der IT-Infrastruktur, der IT-Anwendungen sowie der Daten gewährleistet. Zum anderen müssen die IT-Infrastruktur, die IT-Anwendungen und Daten sowie die erforderliche IT-Organisation in angemessener Zeit funktionsfähig bereitstehen. Daher sind z.B. geeignete Back-up-Verfahren zur Notfallvorsorge einzurichten. Maßnahmen zur Sicherung der Verfügbarkeit sind erforderlich, um den Anforderungen nach Lesbarmachung der Buchführung gerecht zu werden.
- Autorisierungbedeutet, dass nur im Voraus festgelegte Personen auf Daten zugreifen können (autorisierte Personen) und dass nur sie die für das System definierten Rechte wahrnehmen können. Diese Rechte betreffen das Lesen, Anlegen, Ändern und Löschen von Daten oder die Administration eines IT-Systems. Dadurch soll ausschließlich die genehmigte Abbildung von Geschäftsvorfällen im System gewährleistet werden. Geeignete Verfahren hierfür sind physische und logische Zugriffsschutzmaßnahmen (z.B. Passwortschutz). Organisatorische Regelungen und technische Systeme zum Zugriffsschutz sind die Voraussetzung zur Umsetzung der erforderlichen Funktionstrennungen. Neben Identitätskarten werden zukünftig biometrische Zugriffsgenehmigungsverfahren an Bedeutung gewinnen.
- Authentizitätist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist. Dies kann bspw. über Berechtigungsverfahren geschehen. Beim elektronischen Datenaustausch bieten sich für eine Identifizierung des Partners bspw. digitale Signatur- oder passwortgestützte Identifikationsverfahren an.
- Unter Verbindlichkeitwird die Eigenschaft von IT-gestützten Verfahren verstanden, gewollte Rechtsfolgen bindend herbeizuführen. Transaktionen dürfen durch den Veranlasser nicht abstreitbar sein, weil beispielsweise der Geschäftsvorfall nicht gewollt ist.

(24) Maßnahmen zur Gewährleistung der Vertraulichkeit unterstützen auch die Einhaltung anderer Rechtsnormen, die keinen unmittelbaren Rechnungslegungsbezug haben, wie bspw. das Bundesdatenschutzgesetz (BDSG) oder die Telekommunikations-Datenschutzverordnung (TDSV).

Das BDSG hat die Aufgabe, durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken. Gegenstand der mit dem Gesetz beabsichtigten Schutzmaßnahmen ist das Informations- und Kommunikations-System der Unternehmungen. Die Einhaltung des BDSG ist im Rahmen des Sicherheitskonzeptes zu gewährleisten und durch den Datenschutzbeauftragten zu überwachen.

Obwohl die Maßnahmen zum Schutz personenbezogener Daten und zur Vertraulichkeit sehr eng miteinander verbunden sind, führt die Erfüllung der Sicherheitsanforderungen an rechnungslegungsrelevante Daten nicht automatisch zur Erfüllung der Anforderungen an den Schutz personenbezogener Daten. Dies gilt insbesondere für Sicherungsmaßnahmen des BDSG für Daten, die nicht rechnungslegungsrelevant sind (z.B. Nichtkundendateien). Die Beurteilung der Einhaltung datenschutzrechtlicher Bestimmungen durch den Abschlussprüfer kann Gegenstand einer gesonderten Beauftragung sein. Insbesondere bei WebTrust-Prüfungen [6] werden die zu den Bereichen Datenschutz und Datensicherheit vom Unternehmen im Internet gemachten Angaben zur Abwicklung des elektronischen Geschäftsverkehrs auf ihre Einhaltung hin überprüft.

3.2. Grundsätze ordnungsmäßiger Buchführung

3.2.1. Allgemeine Grundsätze

(25) Die Grundsätze ordnungsmäßiger Buchführung bei IT-gestützter Rechnungslegung sind nur erfüllt, wenn das Rechnungslegungssystem die Einhaltung der folgenden allgemeinen Ordnungsmäßigkeitskriterien bei der Erfassung, Verarbeitung, Ausgabe und Aufbewahrung der rechnungslegungsrelevanten Daten über die Geschäftsvorfälle sicherstellt [7]:

- Vollständigkeit (§ 239 Abs. 2 HGB)
- Richtigkeit (§ 239 Abs. 2 HGB)
- Zeitgerechtheit (§ 239 Abs. 2 HGB)
- Ordnung (§ 239 Abs. 2 HGB)
- Nachvollziehbarkeit (§ 238 Abs. 1 Satz 2 HGB)
- Unveränderlichkeit (§ 239 Abs. 3 HGB).

(26) Der Grundsatz der Vollständigkeit betrifft die lückenlose Erfassung aller rechnungslegungsrelevanten Geschäftsvorfälle (vgl. Tz. 14). Der Grundsatz der Vollständigkeit umfasst auch, dass ein und derselbe Geschäftsvorfall nicht mehrfach gebucht wird.

Jeder Geschäftsvorfall ist grundsätzlich einzeln zu erfassen. Zusammengefasste oder verdichtete Buchungen sind zulässig, sofern sie nachvollziehbar in ihre Einzelpositionen aufgegliedert werden können. Die Vollständigkeit der erfassten Buchungen muss während der Verarbeitung und für die Dauer der Aufbewahrungsfrist (§ 257 HGB) nachweisbar erhalten bleiben.

(27) Nach dem Grundsatz der Richtigkeit haben die Belege und Bücher die Geschäftsvorfälle inhaltlich zutreffend abzubilden. Die Geschäftsvorfälle müssen in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften abgebildet werden.

(28) Die Zeitgerechtheit der Buchführung betrifft die Zuordnung der Geschäftsvorfälle zu Buchungsperioden sowie die Zeitnähe der Buchungen. Jeder Geschäftsvorfall ist der Buchungsperiode zuzuordnen, in der er angefallen ist. Zwingend ist die Zuordnung zum jeweiligen Geschäftsjahr oder zu einer nach Gesetz, Satzung oder Rechnungslegungszweck vorgeschriebenen kürzeren Rechnungsperiode.

Geschäftsvorfälle sind zeitnah, d.h. möglichst unmittelbar nach Entstehung des Geschäftsvorfalls zu erfassen. Bei zeitlichen Abständen zwischen der Entstehung eines

Geschäftsvorfalls und seiner Erfassung sind geeignete Maßnahmen zur Sicherung der Vollständigkeit zu treffen.

(29) Die Buchführungspflicht kann durch vollständigen Ausdruck der Buchungen oder durch deren Speicherung in Kombination mit einer ständigen Ausdruckbereitschaft erfüllt werden.

(30) Das Buchführungsverfahren muss gewährleisten, dass die Buchungen sowohl in zeitlicher Ordnung (Journalfunktion) als auch in sachlicher Ordnung (Kontenfunktion) dargestellt werden können. Die Buchungen bzw. die einzelnen Geschäftsvorfälle müssen innerhalb angemessener Zeit festgestellt und optisch lesbar gemacht werden können.

(31) Ein sachverständiger Dritter muss nach dem Grundsatz der Nachvollziehbarkeit in der Lage sein, sich in angemessener Zeit einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens zu verschaffen. Die Abwicklung des einzelnen Geschäftsvorfalls sowie des angewandten Buchführungs- bzw. Rechnungslegungsverfahrens müssen nachvollziehbar sein. Die hieraus resultierende Prüfbarkeit muss über die Dauer der Aufbewahrungsfrist gegeben sein. Dies gilt auch für die zum Verständnis der Buchführung erforderliche Dokumentation.

(32) Nach dem Buchungszeitpunkt darf entsprechend dem Grundsatz der Unveränderlichkeit eine Eintragung oder Aufzeichnung nicht so verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist (§ 239 Abs. 3 HGB). Daher sind spätere Eintragungen oder Aufzeichnungen ausschließlich so vorzunehmen, dass sowohl der ursprüngliche Inhalt als auch die Tatsache, dass Veränderungen vorgenommen wurden, in einer für einen sachverständigen Dritten in angemessener Zeit nachvollziehbaren Form erkennbar bleiben.

Bei programmgenerierten bzw. programmgesteuerten Buchungen (automatisierte Belege bzw. Dauerbelege) sind Änderungen an den der Buchung zu Grunde liegenden Generierungs- und Steuerungsdaten ebenfalls aufzuzeichnen. Dies betrifft insbesondere die Protokollierung von Änderungen in rechnungslegungsrelevanten Einstellungen oder die Parametrisierung der Software und die Aufzeichnung von Änderungen an Stammdaten.

3.2.2. Belegfunktion

(33) Die in § 238 Abs. 1 HGB geforderte Nachvollziehbarkeit der Buchführung vom Urbeleg zum Abschluss und vice versa setzt voraus, dass jede Buchung und ihre Berechtigung durch einen Beleg nachgewiesen wird (Grundsatz der Belegbarkeit). Die Belegfunktion verlangt, dass jede Buchung vollständig durch einen Beleg nachgewiesen ist oder nachgewiesen werden kann. Sie ist die Grundvoraussetzung für die Beweiskraft der Buchführung. Über die Belegfunktion wird der Nachweis der zutreffenden Abbildung der internen und externen Geschäftsvorfälle im Rechnungswesen geführt.

(34) Bei IT-gestützten Prozessen kann und soll der Nachweis oft nicht durch konventionelle Belege erbracht werden. Dies betrifft zum Beispiel Buchungen von Materialverbräuchen, die bei Lagerentnahmen automatisch generiert werden oder Fakturiersätze, die von Programmen durch Multiplikation von Preisen mit aus der Betriebsdatenerfassung entnommenen Mengen gebildet werden (z.B. Gas- und Stromverbrauch bei Versorgungsunternehmen, Billing-Systeme bei Telekommunikationsunternehmen).

(35) Auch in diesen Fällen muss der mit dem Grundsatz der Belegbarkeit verfolgte Zweck eingehalten werden. Bei IT-gestützten automatisierten Rechnungslegungsverfahren (z.B. Abschreibungen, maschinelle Bewertung von Halb- und Fertigfabrikaten) wird die Belegfunktion über den verfahrensmäßigen Nachweis des Zusammenhangs zwischen dem

einzelnen Geschäftsvorfall und seiner Buchung oder durch Sammelbelege nebst Einzelnachweis erfüllt. Der verfahrensmäßige Nachweis ist in solchen Fällen regelmäßig durch die folgenden Funktionen zu führen:

- Dokumentation der programminternen Vorschriften zur Generierung der Buchungen
- Nachweis, dass die in der Dokumentation enthaltenen Vorschriften einem autorisierten Änderungsverfahren unterlegen haben (u.a. Zugriffsschutz, Versionsführung, Test- und Freigabeverfahren)
- Nachweis der Anwendung des genehmigten Verfahrens sowie
- Nachweis der tatsächlichen Durchführung der einzelnen Buchungen.

(36) Die Realisierung der Belegfunktion ist durch die Gestaltung der Geschäftsprozesse beeinflusst. Ein Geschäftsvorfall ist zumindest mit folgenden Angaben zu erfassen:

- hinreichende Erläuterung des Vorgangs (Buchungstext oder -schlüssel)
- Buchungsbetrag bzw. Mengen- und Wertangaben, aus denen sich der zu buchende Betrag ergibt
- Zeitpunkt des Geschäftsvorfalls (Belegdatum, Bestimmung der Buchungsperiode)
- Bestätigung (Autorisierung) durch den Buchführungspflichtigen.

(37) Zu welchem Zeitpunkt ein Geschäftsvorfall als gebucht gilt, ist auch abhängig von einer in der Unternehmensorganisation festgelegten Entscheidung des Buchführungspflichtigen. Geschäftsvorfälle gelten als gebucht, wenn sie autorisiert und nach einem Ordnungsprinzip vollständig, richtig, zeitgerecht und verarbeitungsfähig erfasst und gespeichert sind. Hierzu sind die Angaben zum Geschäftsvorfall zu ergänzen um

- die Kontierung (Konto und Gegenkonto),
- das Ordnungskriterium (Belegnummer),
- das Buchungsdatum (Kennzeichnung des Zeitpunkts der Buchung).

(38) Beim Einsatz von - der Finanzbuchführung vorgelagerten - IT-Anwendungen (z.B. Logistiksysteme, Leistungsabrechnungsverfahren) können Geschäftsvorfälle bereits dann als gebucht gelten, wenn sie - mit allen erforderlichen Angaben erfasst und gespeichert werden. Voraussetzung hierfür ist, dass die vorgelagerten IT-Anwendungen die Anforderung des § 239 Abs. 3 HGB sicherstellen, d.h. dass die Unveränderlichkeit der Eintragung der Aufzeichnung in der Weise gewährleistet wird, dass der ursprüngliche Inhalt feststellbar bleibt. Weiterhin muss die vorgelagerte IT-Anwendung in ihrer Wirkung auf die Buchführung von den gesetzlichen Vertretern autorisiert sein.

(39) Buchungstexte oder Vorgangsbezeichnungen können in abgekürzter verständlicher Form oder durch Schlüssel bezeichnet werden, wenn anhand eines Schlüsselverzeichnisses in angemessener Zeit eine Übersetzung möglich ist.

(40) Die Autorisierung (Freigabe) der Buchung kann abhängig von der Entstehung des Belegs auf unterschiedliche Weise dokumentiert werden.

- Bei konventionellen Papierbelegen bzw. Erfassungsformularen ergibt sich die Autorisierung aus Unterschriften oder Handzeichen.
- Automatisch mit der Erfassung erstellte Belege (z.B. telefonisch angenommene Bestellungen) werden durch die Benutzeridentifikation des verantwortlichen Mitarbeiters in Verbindung mit einem entsprechend ausgestalteten Zugriffsberechtigungsverfahren freigegeben.

- Automatisch mit der Erfassung durch den Kunden gespeicherte Daten (z.B. elektronische Zahlungsaufträge, Bestellungen über Internet-basierte Anwendungen) können z.B. durch ein entsprechendes Signaturverfahren autorisiert werden.
- Bei per Datenfernübertragung gesendeten oder empfangenen Belegen ist ebenfalls ein entsprechendes Autorisierungsverfahren festzulegen. Neben weltweit standardisierten Datenfernübertragungsverfahren (S.W.I.F.T., EDI, EDIFACT) sind auch einzelvertragliche Festlegungen zwischen Vertragspartnern möglich.
- Bei programmintern generierten Buchungen erfolgt die Autorisierung der Buchung durch die IT-Anwendung. Aus der Verfahrensdokumentation müssen die Regeln für Generierung und Kontrolle der maschinellen Buchungen eindeutig erkennbar sein. Die freigegebenen Programme müssen gegen unautorisierte und undokumentierte Änderungen geschützt sein.

3.2.3. Journalfunktion

(41) Die Journalfunktion verlangt, dass alle buchungspflichtigen Geschäftsvorfälle möglichst bald nach ihrer Entstehung vollständig und verständlich in zeitlicher Reihenfolge aufgezeichnet werden (Journal). Während durch die Erfüllung der Belegfunktion die Existenz und Verarbeitungsberechtigung eines Geschäftsvorfalls nachgewiesen werden muss, hat die Journalfunktion den Nachweis der tatsächlichen und zeitgerechten Verarbeitung der Geschäftsvorfälle zum Gegenstand.

(42) Die Erfüllung der Journalfunktion kann in bestimmten Fällen durch eine auswertbare Speicherung (Einzelnachweis) der Buchungen in der Buchführung vorgelagerten IT-Anwendungen mit Übertragung von Summenbuchungen erfolgen. Bei diesen vorgelagerten IT-Anwendungen (vgl. Tz. 37) ist Voraussetzung für die Erfüllung der Journalfunktion, dass auch für die vorgelagerten IT-Anwendungen die Ordnungsmäßigkeitsanforderungen an die Buchführung eingehalten werden. Dazu ist neben der Dokumentation des Verfahrens ein Kontroll- und Abstimmungsverfahren erforderlich, mit dem die Identität der in der vorgelagerten IT-Anwendung gespeicherten Buchungen mit den in Haupt- und Nebenbüchern vorhandenen Buchungen gewährleistet und nachgewiesen werden kann.

(43) Die Journalfunktion ist nur erfüllt, wenn die gespeicherten Aufzeichnungen gegen Veränderung oder Löschung geschützt sind. Sofern Belege in Zwischendateien erfasst werden, um nach Kontrolle Erfassungskorrekturen vornehmen zu können, sind die erstellten Listen als Erfassungsprotokolle und nicht als Journale einzustufen, da die abschließende Autorisierung der Geschäftsvorfälle noch aussteht.

(44) Im Journal sind - ggf. über eine entsprechende Verweistechnik - die Geschäftsvorfälle mit allen für die Erfüllung der Belegfunktion erforderlichen Angaben nachzuweisen.

(45) Die Sicherung der Journale über die gesetzlich vorgeschriebene Aufbewahrungsfrist kann durch eine Protokollierung auf Papier oder auf maschinell lesbaren Datenträgern erfüllt werden. Sofern das Journal in ausgedruckter Form aufbewahrt wird, muss die Vollständigkeit der Druckliste z.B. über fortlaufende Seitennummern bzw. Summenvorträge nachweisbar sein. Bei der Aufbewahrung auf Datenträgern ist zu beachten, dass das zu Grunde liegende Verfahren die Lesbarkeit über den gesamten Aufbewahrungszeitraum gewährleisten muss.

3.2.4. Kontenfunktion

(46) Die Kontenfunktion verlangt, dass die im Journal in zeitlicher Reihenfolge aufgezeichneten Geschäftsvorfälle auch in sachlicher Ordnung auf Konten abgebildet werden. Bei computergestützten Buchführungsverfahren werden Journal- und Kontenfunktion in der Regel gemeinsam wahrgenommen, indem bereits bei der erstmaligen Erfassung des Geschäftsvorfalls alle für die sachliche Zuordnung notwendigen Angaben erfasst werden. Diese Funktionen werden bei integrierter Software z.B. durch maschinelle Kontenfindungsverfahren unterstützt.(47) Zur Erfüllung der Kontenfunktion sind die Geschäftsvorfälle getrennt nach Sach- und Personenkonten mit folgenden Angaben darzustellen:

- Kontenbezeichnung
- Kennzeichnung der Buchungen
- Summen und Salden nach Soll und Haben
- Buchungsdatum
- Belegdatum
- Gegenkonto
- Belegverweis
- Buchungstext bzw. dessen Verschlüsselung.

(48) Beim Ausdruck der Konten muss die Vollständigkeit der Kontoblätter z.B. über fortlaufende Seitennummern je Konto oder Summenvorträge nachweisbar sein.

(49) Die Kontenfunktion kann auch durch Führung von Haupt- und Nebenbüchern in unterschiedlichen IT-Anwendungen erfüllt werden. Ausprägungen von Nebenbüchern sind z.B. die Führung von Forderungen und Verbindlichkeiten in Kontokorrentsystemen oder Abrechnungssysteme mit eigener Führung von Personenkonten, z.B. Systeme für Verbrauchsabrechnungen. IT-Anwendungen, die Nebenbücher enthalten, müssen Funktionen zur ordnungsgemäßen Kontenpflege beinhalten. Hierbei handelt es sich z.B. um

- die Kennzeichnung von offenen und ausgeglichenen Forderungen und Verbindlichkeiten (Auszifferungsverfahren)
- die Auswertung von nicht ausgeglichenen Forderungen und Verbindlichkeiten in Offene Posten-Listen.

(50) Bei der Buchung verdichteter Zahlen muss ein Nachweis der in den verdichteten Zahlen enthaltenen Einzelposten möglich sein.

(51) In der Hauptbuchführung werden bei der Führung von Nebenbüchern in der Regel nur die Salden der Nebenbuchkonten geführt. Durch Kontroll- und Abstimmverfahren in Verbindung mit einer entsprechenden Verfahrensdokumentation muss daher der Nachweis der richtigen und vollständigen Übertragung der fortgeschriebenen Salden vom Nebenbuch in das Hauptbuch erbracht werden.

3.2.5. Dokumentation

(52) Auch in einer IT-gestützten Rechnungslegung muss die Buchführung einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens vermitteln (§ 238 Abs. 1 Satz 2 HGB) und müssen sich die Geschäftsvorfälle in ihrer Entstehung und Abwicklung verfolgen lassen (§ 238 Abs. 1 Satz 3 HGB).

(53) Voraussetzung für die Nachvollziehbarkeit des Buchführungs- bzw. Rechnungslegungsverfahrens ist eine ordnungsgemäße Verfahrensdokumentation, die die Beschreibung aller zum Verständnis der Rechnungslegung erforderlichen Verfahrensbestandteile enthalten muss. Die Beurteilung der Ordnungsmäßigkeit - insbesondere komplexer Verfahren - ist für einen sachverständigen Dritten nur dann möglich, wenn ihm neben den Eingabedaten und Verarbeitungsergebnissen auch eine aussagefähige, der Komplexität entsprechend detaillierte Dokumentation zur Verfügung steht. Der Aufbau und die Pflege der zum Verständnis der Rechnungslegung erforderlichen Dokumentation sind Voraussetzung für die Erfüllung der Grundsätze ordnungsmäßiger Buchführung.

(54) Die Verfahrensdokumentation in einer IT-gestützten Rechnungslegung besteht aus der Anwenderdokumentation und der technischen Systemdokumentation sowie der Betriebsdokumentation.

(55) Die Anwenderdokumentation muss alle Informationen enthalten, die für eine sachgerechte Bedienung einer IT-Anwendung erforderlich sind. Neben einer allgemeinen Beschreibung der durch die IT-Anwendung abgedeckten Aufgabenbereiche sowie einer Erläuterung der Beziehungen zwischen einzelnen Anwendungsmodulen sind Art und Bedeutung der verwendeten Eingabefelder, die programminterne Verarbeitung (insbesondere maschinelle Verarbeitungsregeln) und die Vorschriften zur Erstellung von Auswertungen anzugeben.

(56) Bei Einsatz von Standardsoftware ist die vom Produkthersteller gelieferte Dokumentation um die Beschreibung der anwendungsspezifischen Anpassungen und die Dokumentation des eingerichteten internen Kontrollsystems des Anwenders (z.B. Parametrisierungen, Verwendung der Eingabefelder, Schlüsselsystematiken) zu ergänzen.

(57) Die technische Systemdokumentation enthält eine technische Darstellung der IT-Anwendung. Sie ist Grundlage für die Einrichtung eines sicheren und geordneten IT-Betriebs sowie für die Wartung der IT-Anwendung durch den Programmersteller. Art und Umfang der technischen Dokumentation sind abhängig von der Komplexität der IT-Anwendung. Die Dokumentationstechnik und formale Gestaltung der technischen Dokumentation liegen im Ermessen des Programmerstellers.

Die Dokumentation muss in einer Weise zur Verfügung gestellt werden, die einem sachverständigen Dritten den Nachvollzug der programminternen Verarbeitung, insbesondere der Verarbeitungsfunktionen und -regeln, in angemessener Zeit ohne Kenntnis der Programmiersprache erlaubt.

Angesichts der Vielzahl von Programmiersprachen ist eine nur auf den Programm-Quellcode gestützte Dokumentation zur Sicherstellung der Nachvollziehbarkeit des Buchführungs- bzw. Rechnungslegungsverfahrens nicht ausreichend.

(58) Die technische Systemdokumentation soll über folgende Bereiche informieren:

- Aufgabenstellung der IT-Anwendung im Kontext der eingesetzten Module
- Datenorganisation und Datenstrukturen (Datensatzaufbau bzw. Tabellenaufbau bei Datenbanken)
- veränderbare Tabelleninhalte, die bei der Erzeugung einer Buchung herangezogen werden
- programmierte Verarbeitungsregeln einschließlich der implementierten Eingabe- und Verarbeitungskontrollen

- programminterne Fehlerbehandlungsverfahren
- Schlüsselverzeichnisse
- Schnittstellen zu anderen Systemen.

(59) Die Betriebsdokumentation dient der Dokumentation der ordnungsgemäßen Anwendung des Verfahrens. Dies betrifft u.a.

- Datensicherungsverfahren,
- Verarbeitungsnachweise (Verarbeitungs- und Abstimmprotokolle),
- Art und Inhalt des Freigabeverfahrens für neue und geänderte Programme,
- Auflistung der verfügbaren Programme mit Versionsnachweisen.

3.2.6. Aufbewahrungspflichten

(60) Um die Aufbewahrung der Buchführungsunterlagen über die gesetzlich vorgesehenen Zeiträume zu gewährleisten, müssen sowohl die Anforderungen an die Art der Aufbewahrungsmedien (Original, Datenträger) beachtet, als auch die technischen Voraussetzungen für die Gewährleistung der jederzeitigen Lesbarmachung erfüllt sein (§§ 257, 261 i.V.m. § 239 Abs. 4 Satz 2 HGB).

(61) Journale, Konten, Belege und Abschlüsse sind gemäß § 257 HGB für einen Zeitraum von 10 Jahren aufzubewahren. Zu den aufbewahrungspflichtigen Unterlagen zählen nach § 257 Abs. 1 Nr. 1 HGB auch die zum Verständnis der Buchführung erforderlichen Unterlagen.

(62) Zu den zum Verständnis der Buchführung erforderlichen Unterlagen zählen bei Individualsoftware neben der Anwenderdokumentation der Programm-Quellcode, der in maschinenlesbarer Form aufzubewahren ist, und die technische Systemdokumentation soweit die entsprechenden Programme rechnungslegungsrelevant und somit für die Erfüllung der Beleg-, Journal- oder Kontenfunktion von Bedeutung sind.

(63) Bei Einsatz von Standardsoftware liegen dem Anwender im Regelfall keine Programm-Quellcodes und ggf. auch keine technische Systemdokumentation vor. Hier sind in jedem Fall die mit der Standardsoftware ausgelieferten Programmbeschreibungen, aus denen der Leistungsumfang der Software hervorgeht, aufzubewahren. Ferner sollte der Anwender mit dem Softwarelieferanten vereinbaren, dass er oder ein neutraler Dritter während der Dauer der Aufbewahrungsfrist Zugriff auf die technische Systemdokumentation oder die Programm-Quellcodes hat.

(64) Unternehmensspezifische Einstellungen und Anpassungen, Parametrisierungen und Änderungen in Tabellen und Stammdaten, die für die Verarbeitung aufzeichnungspflichtiger Geschäftsvorfälle erforderlich sind, zählen zu den zum Verständnis der Buchführung erforderlichen Unterlagen und unterliegen daher ebenfalls der Aufbewahrungsfrist von 10 Jahren.

(65) Systemprotokolle oder sonstige technische Aufzeichnungen (z.B. Logs) sind ausnahmsweise dann zum Verständnis der Buchführung erforderlich und damit 10 Jahre aufzubewahren, wenn zur Ordnungsmäßigkeitsbeurteilung erforderliche Informationen ausschließlich diesen Unterlagen entnommen werden können. In anderen Fällen ist, unbeschadet anderer Vorschriften zur Aufbewahrungsdauer, in der Regel eine Aufbewahrung bis zur Beendigung der Abschlussprüfung erforderlich.

(66) Bei der Auslagerung von IT-Systemen und -Anwendungen muss der Servicegeber vertraglich verpflichtet werden, die für die Erfüllung der Buchführungspflichten des Servicenehmers erforderlichen Unterlagen aufzubewahren und auf Verlangen auszuhändigen. Hierzu zählen u.a. die Dokumentation der Programmablaufsteuerung (Job-Prozeduren) und die Dokumentation von Änderungen.

(67) Neben der Aufbewahrung der Buchführungsunterlagen im Original gestattet § 257 Abs. 3 HGB die Speicherung auf einem Bild- oder sonstigen Datenträger, sofern empfangene Handelsbriefe und Buchungsbelege bildlich und alle anderen aufbewahrungspflichtigen Unterlagen (Handelsbücher, Inventare, Lageberichte, Arbeitsanweisungen und sonstige Organisationsunterlagen, abgesandte Handelsbriefe) inhaltlich wiedergegeben werden können. Eröffnungsbilanzen, Jahres- und Konzernabschlüsse müssen im Original aufbewahrt werden.

(68) Der Begriff "bildliche Wiedergabe" bedeutet, dass eine vollständige Übereinstimmung zwischen Original und Wiedergabe bestehen muss. Dabei ist im Einzelfall zu würdigen, ob oder inwieweit die farbliche Gestaltung im Interesse der Beweiskraft zu dokumentieren ist. Die Anforderungen zur Dokumentation elektronisch empfangener Handelsbriefe sind in der IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce (IDW RS FAIT 2), Tz. 40 ff. [8] dargestellt.

(69) Typische Archivierungsverfahren sind die optische Archivierung (Mikrofilm), die elektronische Archivierung (Speicherung von Daten in digitalisierter Form auf magnetischen Datenträgern) und die digital optische Archivierung (Speicherung eines optischen Abbilds auf elektronischen Medien).

(70) Die technischen Verfahren zur Archivierung sind abhängig von der Art und Weise, wie die aufzubewahrenden Unterlagen gespeichert werden. Dabei ist zu unterscheiden zwischen sog. kodierten Dokumenten (CI = Coded Information) und nicht kodierten Dokumenten (NCI = Non Coded Information). CI-Dokumente können durch IT direkt ausgewertet werden und beinhalten z.B. auf elektronischem Wege empfangene Handelsbriefe oder ausdruckfähige Dateien. NCI-Dokumente bestehen aus analogen Informationsträgern (Papier), die in ihrer Ursprungsform durch IT nicht direkt auswertbar sind, sondern vor der Speicherung z.B. mittels Scannern digitalisiert werden müssen. Ergebnis ist eine digitalisierte Abbildung (Bitmap oder Image), welches am Bildschirm angezeigt und ausgedruckt werden kann. Um ein Image gezielt aufzufinden, muss es mit einem Index versehen werden, der getrennt vom Dokument gespeichert werden muss.

(71) CI-Dokumente können somit unmittelbar gespeichert werden und lassen sich darüber hinaus auch inhaltlich auswerten (z.B. durch Suche nach Kontonummern in einer archivierten Datei mit Kontoauszügen). Typische Ausprägung dieser Archivierungsverfahren ist das COLD (Computer Output on Laser Disk)-Verfahren. Der zusätzliche Ausdruck eines CI-Dokumentes erhöht nicht dessen Beweiskraft. Vielmehr ist die Erfüllung der Belegfunktion durch das Archivierungsverfahren selbst sicherzustellen. Elektronisch empfangene Handelsbriefe (z.B. EDI, S.W.I.F.T-Verfahren oder Kommunikation oder Transaktionen im E-Commerce) sind in dem empfangenen Format im Sinne eines Urbelegs zu archivieren.

(72) Für die Beurteilung der handelsrechtlichen Zulässigkeit eines NCI-Archivierungsverfahrens ist die Unterscheidung zwischen Brutto- und Netto-Imaging von Bedeutung. Beim Brutto-Imaging wird das vollständige Abbild gespeichert. Dieses Verfahren ist somit für Eingangs- und Ausgangsbelege geeignet. Beim Netto-Imaging werden auf einem Beleg (z.B. Briefkopf) wiederkehrende Informationen ausgefiltert und nicht jedes Mal mit

abgespeichert. Das Verfahren eignet sich daher für die Archivierung von standardisierten Eingangs- oder Ausgangsbelegen, sofern sichergestellt ist, dass das Netto-Image zum Zeitpunkt der Wiedergabe mit den ausgefilterten Informationen kombiniert werden kann.

(73) Gängige Verfahren zur Archivierung auf Bild- und Datenträgern sind Mikrofilmverfahren und Systeme zur optischen Archivierung auf einmal beschreibbaren Wechselmedien. Die Verwendung dieser Verfahren ist zulässig, wenn ihr Einsatz den Grundsätzen ordnungsmäßiger Buchführung entspricht. Die Unveränderbarkeit der digitalisierten Dokumente ist zur Sicherstellung der Beweiskraft der Buchführung durch aufeinander abgestimmte technische (z.B. Speichermedien ohne Änderungsmöglichkeit) und organisatorische (z.B. Zugriffsschutz- und Sicherungsverfahren) Maßnahmen sowie die sachgerechte Implementierung von Dokumenten-Management-Systemen im Rahmen der vorhandenen Unternehmensorganisation zu gewährleisten.

(74) Zu den damit in Zusammenhang stehenden technischen und organisatorischen Anforderungen zählen die

- Unveränderbarkeit eines digitalisierten Dokumentes,
- Sicherung der Dateien,
- organisatorische Regelungen zum Digitalisierungsverfahren, zur Kontrolle der Vollständigkeit und Wiedergabequalität sowie
- Indizierungsverfahren, die eine eindeutige Zuordnung des digitalen Dokuments zum Geschäftsvorfall erlauben.

(75) Das optische Archivierungsverfahren muss so gestaltet sein, dass die Lesbarkeit der Datenträger über die Aufbewahrungsfrist sichergestellt ist. Dies gilt auch bei Verfahrenswechseln, bei dem die Speichermedien in ein neues EDV-Verfahren übernommen werden müssen.

4. Die Einrichtung eines IT-Systems mit Rechnungslegungsbezug

(76) Um die Unternehmensziele zu erreichen und die erkannten Risiken zu bewältigen, stimmen die gesetzlichen Vertreter ihre IT-Strategie mit der Unternehmensstrategie ab, damit ein angemessenes IT-Kontrollsystem eingerichtet werden kann. Die IT-Strategie ist weiter abhängig von der Komplexität und Diversifikation der Geschäftstätigkeit und der Organisationsstruktur des Unternehmens. Sie schließt die Bewertung der IT-Risiken aus der Geschäftstätigkeit ein, die sich auf die Rechnungslegung auswirken können.

IT-Risiken können für Unternehmen, deren Geschäftstätigkeit weitgehend von IT abhängt, bestandsgefährdend sein. Sie müssen deshalb im Risikofrüherkennungssystem festgestellt, analysiert, bewertet und an die verantwortlichen Personen weitergeleitet werden [9].

Bei der Einrichtung eines IT-Systems sind die Anforderungen der Grundsätze ordnungsmäßiger Buchführung an eine ordnungsmäßige IT-gestützte Rechnungslegung für alle Elemente des IT-Systems sicherzustellen (vgl. Tz. 6).

4.1. IT-Umfeld und IT-Organisation

(77) Voraussetzungen für ein geeignetes IT-Umfeld sind eine angemessene Grundeinstellung zum Einsatz von IT und ein Problembewusstsein für mögliche Risiken aus dem IT-Einsatz bei den gesetzlichen Vertretern und den Mitarbeitern. Zu einem geeigneten IT-Umfeld gehört

auch das Bewusstsein für Sicherheit in der Unternehmensorganisation. Dieses ist zugleich eine wesentliche Bedingung für die angemessene Umsetzung des Sicherheitskonzepts.

(78) Die Überwachung der Umsetzung der IT-Strategie durch die Implementierung eines angemessenen und wirksamen IT-Kontrollsystems ist Aufgabe der gesetzlichen Vertreter.

Die Anforderungen an die Gestaltung der IT-Organisation betreffen die Aufbau- und Ablauforganisation. Die Aufbauorganisation regelt die Einordnung des IT-Bereichs in die Organisationsstruktur des Gesamtunternehmens und den Aufbau des IT-Bereichs selbst. Geregelt werden die Verantwortlichkeiten und Kompetenzen im Zusammenhang mit dem IT-Einsatz.

Die Ablauforganisation regelt sowohl die Organisation der Entwicklung, Einführung und Änderung als auch die Steuerung des Einsatzes von IT-Anwendungen. Auch im Rahmen des IT-Betriebs müssen Aufgaben, Kompetenzen und Verantwortlichkeiten der IT-Mitarbeiter klar definiert sein. Übliche Instrumente hierfür sind Prozess- und Funktionsbeschreibungen oder Organisationshandbücher.

(79) Eine funktionale Trennung sollte sowohl innerhalb des IT-Bereichs (Entwicklung und IT-Betrieb) als auch zu anderen Abteilungen des Unternehmens bestehen. Ist eine solche Funktionstrennung aufgrund der personellen Ausstattung nicht möglich, z.B. bei Personalidentität von Fach- und IT-Aufgaben, müssen zusätzliche Überwachungsmaßnahmen durch die gesetzlichen Vertreter eingerichtet werden.

4.2. IT-Infrastruktur

(80) Die technischen Ressourcen und die Verfahren für einen sicheren und geordneten IT-Betrieb sollen insbesondere die Integrität und Verfügbarkeit der IT auf der Grundlage des Sicherheitskonzepts gewährleisten.

(81) Das Sicherheitskonzept muss in Übereinstimmung mit der IT-Strategie und der IT-Organisation stehen und eine Bewertung der spezifischen Sicherheitsrisiken des Unternehmens enthalten. Ein solches Sicherheitskonzept wird durch Ausführungsanweisungen etwa im Bereich des IT-Betriebs, des Netzbetriebs und der Administration sowie bei der Gestaltung von Zugriffsschutzverfahren konkretisiert.

(82) Die aus dem Sicherheitskonzept abgeleiteten Sicherungsmaßnahmen umfassen physische Sicherungsmaßnahmen und logische Zugriffskontrollen, Datensicherungs- und Auslagerungsverfahren.

(83) Physische Sicherungsmaßnahmen dienen dem Schutz der Hardware sowie der Programme und Daten vor Verlust, Zerstörung und unberechtigter Veränderung. Hierzu zählen bauliche Maßnahmen, Zugangskontrollen, Feuerschutzmaßnahmen und Maßnahmen zur Sicherung der Stromversorgung, die zur Sicherung der Funktionsfähigkeit der IT erforderlich sind.

(84) Durch logische Zugriffskontrollen z.B. unter Verwendung von Benutzer-ID und Passwörtern ist die Identität der Benutzer von IT-Systemen eindeutig festzustellen, um damit nicht autorisierte Zugriffe zu verhindern. Mitarbeitern sind nur die Berechtigungen zu erteilen, die zur Wahrnehmung ihrer Aufgaben erforderlich sind.

In organisatorischen Grundsätzen sind die Einrichtung, Änderung und Entziehung sowie die Sperrung von Berechtigungen, die Protokollierung aller Aktivitäten im Bereich der

Berechtigungsverwaltung, die Gestaltung des Passwortes z.B. hinsichtlich Mindestlänge und Ablaufdatum und die Festlegung von aufgabenbezogenen Berechtigungsprofilen festzulegen.

(85) Datensicherungs- und Auslagerungsverfahren müssen so ausgestaltet sein, dass die jederzeitige Verfügbarkeit und Lesbarkeit der Daten sichergestellt ist. Geeignete Verfahren sind hinreichend gestaffelte Tages-, Monats- und Jahressicherungen, die Inventarisierung aller Sicherungsmedien einschließlich der Führung von Datenträgerverzeichnissen sowie die Auslagerung wichtiger Sicherungsbestände außerhalb des Rechnerbereichs.

Ein nachvollziehbar dokumentiertes Datensicherungssystem setzt voraus, dass über die gesicherten Daten und Programme systematische Verzeichnisse geführt werden, die eine geordnete Aufbewahrung und Auffindbarkeit sicherstellen.

(86) Die Durchführung regelmäßiger Datensicherungen ist im allgemeinen Voraussetzung für

- die Rekonstruktion historischer Bestände (Programme und Daten) und
- die Rekonstruktion aktueller Software- und Datenbestände bei Funktionsstörungen der Hardware.

Im Rahmen des Datensicherungsverfahrens für die Wiederherstellbarkeit des IT-Systems sind die Zahl bzw. die regelmäßige Wiederkehr der Sicherungen (Generationenkonzept), die verwendeten Sicherungsmedien und die Art der Aufbewahrung der Sicherungen festzulegen.

(87) Der IT-Betrieb umfasst sowohl Verfahren für einen geordneten Regelbetrieb von IT-Anwendungen als auch Verfahren für den Notbetrieb. Der geordnete Regelbetrieb von IT-Anwendungen setzt dokumentierte Verfahrensabläufe für die Arbeitsvorbereitung, die Programmeinsatzplanung, den Betrieb von IT-Anwendungen und Netzwerken und für die Arbeitsnachbereitung voraus. In diesem Zusammenhang sind der Einsatz von Programmversionen, die Verarbeitungsreihenfolge und der Zugriff auf Dateien und Datenbanken zu regeln. Die Verfahren für den Notbetrieb umfassen organisatorische Regelungen zur Wiederherstellung der Betriebsbereitschaft und reichen von Maßnahmen bei Systemstörungen (Wiederanlaufkonzepte) bis hin zu Konzepten bei einem vollständigen Ausfall des IT-Systems (Katastrophenfall-Konzept).

(88) Die jederzeitige Verfügbarkeit des IT-Systems ist eine wesentliche Voraussetzung für die Aufrechterhaltung des Geschäftsbetriebs. Deshalb sind Vorkehrungen für einen Notbetrieb zu treffen. Ein Ausfall wesentlicher IT-Anwendungen ohne kurzfristige Ausweichmöglichkeit kann materielle und immaterielle Vermögensschäden nach sich ziehen und stellt einen wesentlichen Mangel der Buchführung dar.

(89) Die Maßnahmen zur Sicherung der Betriebsbereitschaft lassen sich unterscheiden in Maßnahmen, die sich auf den kurzfristigen Ersatz einzelner Systemkomponenten richten und so genannte Katastrophenfall-Szenarien, die bei einem vollständigen Ausfall der gesamten IT eines Unternehmens (z.B. aufgrund von Feuer-, Wasser-, Erdbebenschäden oder Gewaltanschlägen) einen Wiederanlauf ermöglichen sollen.

(90) Um den Ausfall einzelner Systemkomponenten zu kompensieren, werden in der Regel fehlertolerante Systeme in Verbindung mit einer in Teilen redundanten Auslegung wichtiger Systemkomponenten eingesetzt. Typische Beispiele sind gespiegelte Server oder Festplattentechnologien, bei denen das jeweilige Backup-System die Aufgaben des ausgefallenen Systems übernimmt.

(91) Katastrophenfall-Szenarien reichen von räumlich entfernten Rechenzentren, die (gegenseitig) die vollständige Rechenlast übernehmen können, über Backup-Rechner

innerhalb oder außerhalb des Unternehmens bis zu Servicevereinbarungen zwischen Unternehmen und speziellen Backup-Dienstleistern oder Hardware-Herstellern und -Lieferanten. Die Entscheidung des Unternehmens für ein spezifisches Szenario wird maßgeblich von der Abhängigkeit des Unternehmens von der Verfügbarkeit der IT-Anwendungen und der Art der eingesetzten IT-Infrastruktur bestimmt. Die Maßnahmen zum Notbetrieb bzw. zum Wiederanlauf sind entsprechend dem Sicherheitskonzept festzulegen, zu dokumentieren (Notfall- / Katastrophenhandbuch) und an die betroffenen Mitarbeiter zu kommunizieren. Die Wirksamkeit der umgesetzten Maßnahmen ist in regelmäßigen Zeitabständen zu trainieren und zu testen.

(92) Sofern ein Unternehmen bei der hierfür erforderlichen Analyse der Risikosituation zu dem Ergebnis kommt, dass die Geschäftstätigkeit für einen begrenzten Zeitraum allein mit manueller Abwicklung fortgeführt werden kann, kann nach wirtschaftlicher Betrachtung unter Umständen auf entsprechende Maßnahmen verzichtet werden. In jedem Fall ist eine Datensicherung erforderlich, aus der die Programme und Datenbestände wieder aufgebaut und in angemessener Zeit lesbar gemacht werden können.

4.3. IT-Anwendungen

(93) Anforderungen an die Ordnungsmäßigkeit von IT-Anwendungen richten sich auf die Erfüllung der verfahrensbezogenen Anforderungen der Grundsätze ordnungsmäßiger Buchführung hinsichtlich der Erfüllung der Beleg-, Journal- und Kontenfunktion, die Erfüllung der Anforderungen an die Softwaresicherheit sowie die Anforderungen an die rechnungslegungsrelevanten Verarbeitungsregeln. Zu den einzelnen Sicherheits- und Ordnungsmäßigkeitsanforderungen wird auf Tz. 19 ff. und 24 ff. verwiesen. Es muss ferner gewährleistet sein, dass die in der IT-Strategie formulierten Anforderungen an die Funktionalität der IT-Anwendungen eingehalten werden.

(94) Neben der Einführung von anwendungsbezogenen Überwachungsmaßnahmen ist durch generelle Kontrollen die Ordnungsmäßigkeit von IT-Anwendungen sicherzustellen.

(95) Zu den anwendungsbezogenen IT-Kontrollen zählen insbesondere die Eingabe-, Verarbeitungs- und Ausgabekontrollen.

- Eingabekontrollen sollen bereits zum Zeitpunkt der Erfassung die Richtigkeit und Vollständigkeit der in IT-Anwendungen übernommenen Daten sicherstellen. Sie reichen von feldbezogenen Kontrollen (z.B. Datumskontrollen, Muss- / Kann-Feldsteuerung) bis zu komplexen Kontrollstrukturen unter Verwendung von Stammdaten (z.B. bei der Kontrolle der Zulässigkeit bestimmter Soll- / Haben-Kontenkombinationen).
- Verarbeitungskontrollen sollen gewährleisten, dass die Daten den Verarbeitungsprozess vollständig und richtig durchlaufen. Beispiele hierfür sind Abstimmkontrollen wie Kontrollnummern und Satzzähler in Batchprozeduren. Darüber hinaus sollen mit Verarbeitungskontrollen Fehler im Ablauf erkannt und geeignete Korrekturmaßnahmen ausgelöst werden. Dies betrifft etwa Recoverymaßnahmen nach Abbruch einer Verarbeitung aufgrund fehlerhafter oder fehlender Dateien.
- Ausgabekontrollen sollen die vollständige und richtige Erstellung und Verteilung von Verarbeitungsergebnissen in lesbarer Form sichern und betreffen z.B. die sachgerechte Aufbereitung von Reports aus Datenbanken oder Schnittstellen für die Übergabe von Dateien an andere IT-Anwendungen.

(96) Generelle Kontrollen sind in den folgenden Bereichen erforderlich:

- Entwicklung von Individualsoftware
- Auswahl, Beschaffung und Einführung von Standardsoftware
- Test- und Freigabeverfahren und
- Verfahren zur Änderung von IT-Anwendungen (Change-Management).

(97) Individualsoftware kann entweder durch eigene Mitarbeiter (Eigenentwicklung) oder im Auftrag des Unternehmens durch Dritte (Fremdentwicklung) erstellt werden. Die Softwareentwicklung sollte bspw. auf Machbarkeitsstudien und dokumentierten Grob- und Feinkonzepten bzw. vergleichbaren Konzepten beruhen, in denen die Anforderungen an die Ordnungsmäßigkeit und Sicherheit der Rechnungslegung sowie Anforderungen an die weitere Funktionalität der Software berücksichtigt sind.

(98) Um bei der Softwareentwicklung den Anforderungen einer ordnungsmäßigen Rechnungslegung gerecht zu werden, sind folgende Maßnahmen erforderlich

- die Gestaltung eines der Art und Größe des Entwicklungsvorhabens angemessenen Projektmanagements,
- die Einhaltung der von den gesetzlichen Vertretern vorgegebenen Richtlinien zum Qualitätsmanagement,
- Normierungen und Namenskonventionen für die Programmierung und die Dokumentation,
- ausreichende Toolunterstützung für das Design und die Realisierung von IT-Anwendungen.

(99) Die Auswahl und Beschaffung von Standardsoftware muss bei komplexen Systemen auf der Basis von festgelegten Anforderungen an die IT-Anwendung und die zu Grunde liegende IT-Infrastruktur vorgenommen werden. Anforderungen der Fachabteilungen sind grundsätzlich zu berücksichtigen und in den Pflichtenheften festzulegen.

(100) Die Implementierung von Standardsoftware ist in der Regel mit unternehmensspezifischen Anpassungen und Einstellungen (Customizing) verbunden. Diese dienen der konkreten Ausgestaltung der Standardsoftware in der Rechnungslegung des Unternehmens und unterliegen den Anforderungen der Ordnungsmäßigkeit und Sicherheit.

(101) Bei der Einführung oder wesentlichen Änderung von IT-Anwendungen müssen meist Altdaten (Steuerungs-, Stamm- und Bewegungsdaten) aus den abgelösten Anwendungssystemen übernommen werden (Migration). Zur Sicherstellung einer ordnungsgemäßen Softwareeinführung bedarf es ebenfalls eines geeigneten Projektmanagements.

(102) Voraussetzung für ein angemessenes Test- und Freigabeverfahren ist die Trennung von Entwicklungs- und Testsystem von dem produktiv eingesetzten System (für den laufenden Geschäftsbetrieb eingesetztes System). Das Verfahren zur technischen Übergabe von Programmen muss gewährleisten, dass nur autorisierte und freigegebene Programme aus den Entwicklungs- bzw. Testbibliotheken in die Produktionsbibliotheken eingestellt werden können.

(103) Die erforderlichen Funktions- und Integrationstests sollten in einer separaten Testumgebung durchgeführt werden. Testgegenstand, Art und Umfang der Testfälle und die Dokumentation und Archivierung der Testergebnisse sind festzulegen. Die Freigabe der IT-Anwendung für den produktiven Einsatz (laufender Geschäftsbetrieb) hat durch einen formalen Vorgang der Akzeptierung der Testergebnisse und der Systemgestaltung durch die

Unternehmensleitung bzw. - soweit die Verantwortung delegiert wurde - durch die verantwortliche Projektleitung zu erfolgen.

(104) Voraussetzung für die Freigabe sind sowohl die erfolgreich getesteten Verarbeitungsfunktionen und -regeln der IT-Anwendung als auch das Vorliegen angemessener aktueller Anwender- und Verfahrensdokumentationen sowie die Funktionsfähigkeit von Schnittstellenprozessen zu vor- und nachgelagerten Anwendungen.

(105) Änderungen an IT-Anwendungen sind nur auf der Basis eines geregelten Verfahrens vorzunehmen. Auch für Änderungen sind festgelegte Anforderungen an Programmierung, Dokumentation und Tests zu beachten.

Voraussetzung für die ordnungsgemäße Integration von Änderungen in das Gesamtsystem ist die Einführung eines geeigneten Change- und Konfigurationsmanagements, das Verfahren zur Installation und Überwachung von Änderungen innerhalb von definierten Releasekonzepten oder Versionsführungen beinhaltet.

4.4. IT-gestützte Geschäftsprozesse

(106) Die Gestaltung von IT-gestützten Geschäftsprozessen (Geschäftsprozessmodellierung) kann auf Basis einer funktional ausgerichteten oder auf Basis einer geschäftsprozessorientierten Organisation erfolgen.

Bei einer funktional ausgerichteten Unternehmensorganisation stehen bei der Einrichtung des IT-Kontrollsystems die betrieblichen Funktionen des Unternehmens (z.B. Einkauf, Verkauf, Materialwirtschaft) und damit eine funktionsbereichsbezogene Ausrichtung der IT-Kontrollen im Vordergrund (z.B. bei der Ausgestaltung eines Transaktionsfreigabeverfahrens (Vier-Augen-Prinzip) oder bei der Ausgestaltung des Berechtigungskonzeptes).

Bei geschäftsprozessorientierten Unternehmensorganisationen werden die gleichen IT-Kontrollen eingesetzt, allerdings erfolgt eine funktionsbereichsübergreifende Ausrichtung des Kontrollumfangs. Dies betrifft etwa die Gestaltung eines Freigabeverfahrens für Transaktionen innerhalb eines Prozesses unter Beachtung der manuellen und maschinellen Kontrollen sowie der Abstimmverfahren oder die Gestaltung von Transaktionsberechtigungen für den gesamten Geschäftsprozess.

(107) Vor diesem Hintergrund ist es für die Einrichtung eines angemessenen IT-Kontrollsystems von entscheidender Bedeutung, dass bei einer funktionsbereichsbezogenen Ausgestaltung der IT-Kontrollen die Sicherheit und Ordnungsmäßigkeit der rechnungslegungsrelevanten Daten über den gesamten IT-gestützten Geschäftsprozess hinweg gewährleistet werden.

(108) Insbesondere komplexe IT-gestützte Geschäftsprozesse können mit ihren Teilprozessen mehrere funktionale Bereiche im Unternehmen mit nicht integrierten Bestandteilen von IT-Anwendungen bzw. der IT-Infrastruktur betreffen. Eine auf den jeweiligen funktionalen Bereich ausgerichtete Analyse der Sicherheits- und Ordnungsmäßigkeitsrisiken und damit eine auf den Funktionsbereich isoliert ausgerichtete Implementierung des IT-Kontrollsystems birgt die Gefahr, dass Risiken aus dem geschäftsprozessbedingten Datenaustausch zwischen den Teilsystemen unberücksichtigt bleiben. Bspw. kann das Risiko darin bestehen, dass keine Aufzeichnungen darüber vorliegen, welche Daten in welchen Programmen bzw. Programmteilen in den vor- bzw. nachgelagerten IT-Teilsystemen verarbeitet wurden und wie auf welche Daten durch Anwender der anderen Funktionsbereiche zugegriffen werden kann.

(109) Damit im Zusammenhang kann auch eine mangelnde Berücksichtigung der systemtechnischen Zusammenhänge stehen. Sie beinhaltet die Gefahr, dass bspw. Zugriffsrechte, Datensicherungsmaßnahmen etc. lediglich bezüglich der einzelnen IT-Teilsysteme wirksam sind und damit hinsichtlich des Teilprozesses, jedoch nicht hinsichtlich des Gesamtprozesses. Zugriffsschutz- oder Datensicherungsverfahren, die auf eine einzelne im Geschäftsprozess integrierte IT-Anwendung durch Manipulation in den vor- oder nachgelagerten IT-Teilsystemen reagieren, könnten gezielt umgangen werden.

4.5. Überwachung des IT-Kontrollsystems

(110) Unter Überwachung des IT-Kontrollsystems ist die Beurteilung der Wirksamkeit des IT-Kontrollsystems im Zeitablauf durch Mitarbeiter des Unternehmens zu verstehen. Dabei ist zu beurteilen, ob das IT-Kontrollsystem sowohl angemessen ist als auch kontinuierlich funktioniert. Darüber hinaus haben die gesetzlichen Vertreter dafür Sorge zu tragen, dass festgestellte Mängel im IT-Kontrollsystem abgestellt werden.

(111) Ein wesentliches Element des internen Überwachungssystems stellt die Überwachungstätigkeit im besonderen Auftrag der gesetzlichen Vertreter dar ("High-Level-Controls"). Sie beinhaltet im Einzelfall Aktivitäten, die durch die gesetzlichen Vertreter selbst ergriffen bzw. beauftragt werden und eine Beurteilung erlauben, ob die Strategien (Unternehmensstrategie und IT-Strategie), die daraus abgeleiteten Grundsätze, Verfahren und Maßnahmen (Regelungen) in Übereinstimmung mit den Unternehmenszielen umgesetzt wurden, ob das eingerichtete Kontrollsystem angemessen und wirksam ist und ob die umgesetzten Maßnahmen die Erreichung der Unternehmensziele sicherstellen. Typische Beispiele für diese Kontrollen sind die Durchsicht von Fehler- und Ausnahmeberichten im Hinblick auf die Beeinträchtigung kritischer Erfolgsfaktoren, die Durchführung von Benchmarks oder die regelmäßige Analyse der internen Dienstleistungsqualität.

(112) In zahlreichen Unternehmen wird neben prozessintegrierten Überwachungsmaßnahmen das IT-Kontrollsystem von der internen Revision überwacht. Zu den Aufgaben der internen Revision zählt die Beurteilung der Wirksamkeit des eingerichteten IT-Kontrollsystems sowie die Überwachung der Einhaltung der Regelungen und Anforderungen der gesetzlichen Vertreter und der Ordnungsmäßigkeit z.B. durch eine regelmäßige Überwachung sensitiver IT-gestützter Geschäftsprozesse [10].

4.6. IT-Outsourcing

(113) IT-Outsourcing kann sich von der Datenerfassung und -speicherung bis zur vollständigen Verarbeitung von Transaktionen und damit der Abwicklung komplexer Geschäftsprozesse erstrecken.

Ausprägung der Auslagerung (IT-Outsourcing) von Prozessen und Funktionen auf Provider und andere externe Dienstleister sind u.a.:

- Übertragung von Rechenzentrums-Dienstleistungen
- Einschaltung von Providern z.B. bei Geschäftsprozessen, die das Internet nutzen sowie
- Administration von (Standard-) Software durch externe Dienstleister.

(114) Wenn die gesetzlichen Vertreter eines Unternehmens betriebliche Funktionen auf ein anderes Unternehmen auslagern (einschließlich IT-gestützter Funktionen), müssen sie die hieraus entstehenden Auswirkungen auf das interne Kontrollsystem des Unternehmens

beachten. Sofern im Rahmen des Outsourcing die Ausführung von Geschäftsvorfällen und / oder die Datenverarbeitung von einem damit beauftragten Dienstleistungsunternehmen wahrgenommen werden, verbleibt die Verantwortung für die Einhaltung der Ordnungsmäßigkeits- und Sicherheitsanforderungen bei den gesetzlichen Vertretern.

(115) Es kann zwischen solchen Dienstleistungsunternehmen, die ausschließlich die Erfassung und buchmäßige Verarbeitung von Geschäftsvorfällen übernehmen, und solchen, die bestimmte Geschäfte im Auftrag des Unternehmens in eigener Verantwortung ausführen, unterschieden werden. Im erstgenannten Fall kann die Einrichtung organisatorischer Regelungen beim Unternehmen ausreichend sein, um mögliche mit der Auslagerung verbundene Fehler zu erkennen. Im zweiten Fall muss sich das Unternehmen die Ordnungsmäßigkeit des internen Kontrollsystems des Dienstleistungsunternehmens nachweisen lassen oder sich Einsichtsrechte vertraglich einräumen lassen. Für den Fall nicht vertragskonformer Leistungserbringung müssen Einwirkungsmöglichkeiten bis hin zur kurzfristigen Auflösung des Vertrags bestehen.

Fußnoten:

[1] Verabschiedet vom Hauptfachausschuss (HFA) am 24.09.2002.

[2] WPg 1988, S. 1 ff.

[3] Vgl. IDW Prüfungsstandard: Das interne Kontrollsystem im Rahmen der Abschlussprüfung (IDW PS 260), Tz. 5, 6; in: WPg 2001, S. 821 ff.

[4] Vgl. IDW Prüfungsstandard: Grundsätze für die ordnungsmäßige Erteilung von Bestätigungsvermerken bei Abschlussprüfungen (IDW PS 400), Tz. 2; in: WPg 1999, S. 641 ff.

[5] Vgl. IDW Prüfungsstandard: Ziele und allgemeine Grundsätze der Durchführung von Abschlussprüfungen (IDW PS 200), Tz. 8; in: WPg 2000, S. 706 ff.

[6] Vgl. IDW Prüfungsstandard: Die Durchführung von WebTrust-Prüfungen (IDW PS 890); in: WPg 2001, S. 458 ff.

[7] Vgl. auch Aussagen in der Rechnungslegung in: IDW Prüfungsstandard: Prüfungsnachweise im Rahmen der Abschlussprüfung (IDW PS 300), Tz. 7; in: WPg 2001, S. 898 ff.

[8] WPg 2003, S. 1258 ff.

[9] Vgl. IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340), Tz. 4; in: WPg 1999, S. 658 ff.

[10] Vgl. IDW Prüfungsstandard: Interne Revision und Abschlussprüfung (IDW PS 321); in: WPg 2002, S. 686 ff.

Normen:

HGB:239 HGB:239/2 HGB:239/3 HGB:239/4 HGB:238/1/2 HGB:257 HGB:261