

## **Entwurf IDW Prüfungsstandard: Abschlußprüfung bei Einsatz von Informationstechnologie (IDW EPS 330)**

(Stand: 03.07.2001)<sup>1</sup>

*Der Fachausschuß für Informationstechnologie (FAIT) des IDW hat den nachfolgenden Entwurf eines IDW Prüfungsstandards verabschiedet.*

*Eventuelle Änderungs- oder Ergänzungsvorschläge zu dem Entwurf werden schriftlich an die Geschäftsstelle des IDW, Postfach 32 05 80, 40420 Düsseldorf, bis zum 03.01.2002 erbeten.*

*Der Entwurf steht bis zu seiner endgültigen Verabschiedung als IDW Prüfungsstandard im Internet (<http://www.idw.de>) unter der Rubrik Verlautbarungen als Download-Angebot zur Verfügung.*

1.	Vorbemerkungen.....	2
2.	Ziele und Umfang von IT-Systemprüfungen.....	3
2.1.	Risiken aus dem Einsatz von IT.....	5
2.2.	Vorgehensweise bei der IT-Systemprüfung.....	9
2.3.	Besonderheiten des risikoorientierten Prüfungsansatzes bei IT-Systemprüfungen .....	13
3.	Durchführung von IT-Systemprüfungen .....	13
3.1.	Auftragsannahme und Prüfungsplanung .....	13
3.2.	Erhebung von Informationen .....	14
3.3.	Prüfung des IT-Umfelds und der IT-Organisation .....	16
3.4.	Prüfung der IT-Infrastruktur .....	16
3.4.1.	Physische Sicherungsmaßnahmen.....	16
3.4.2.	Logische Zugriffskontrollen .....	17
3.4.3.	Datensicherungs- und Auslagerungsverfahren .....	17
3.4.4.	Maßnahmen für den Regel- und Notbetrieb.....	18
3.4.5.	Sicherung der Betriebsbereitschaft .....	19
3.5.	Prüfung der IT-Anwendungen.....	20
3.5.1.	Programmfunktionen.....	20
3.5.2.	Auswahl-, Entwicklungs- und Änderungsprozeß.....	21
3.5.3.	Implementierung .....	22
3.6.	Prüfung IT-gestützter Geschäftsprozesse .....	23
3.7.	Prüfung des IT-Überwachungssystems .....	23
3.8.	Prüfung des IT-Outsourcing.....	24
4.	IT-gestützte Prüfungstechniken.....	24
4.1.	Einsatzbereiche .....	25

---

<sup>1</sup> Verabschiedet vom Fachausschuß für Informationstechnologie (FAIT) als Entwurf am 03.07.2001.

4.1.1. Einsatz im Rahmen der IT-Systemprüfung .....	26
4.1.2. Aussagebezogene Prüfungshandlungen .....	27
4.2. IT-gestützte Prüfungsdurchführung .....	27
4.3. Verwendung des IT-Systems des Unternehmens für Prüfungszwecke .....	28
4.4. Besonderheiten bei Einsatz IT-gestützter Prüfungstechniken .....	29
5. Dokumentation und Berichterstattung .....	30
6. Übereinstimmung mit ISA.....	30

## 1. Vorbemerkungen

- (1) Das Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) legt in diesem *IDW Prüfungsstandard* die Berufsauffassung dar, nach der Wirtschaftsprüfer unbeschadet ihrer Eigenverantwortlichkeit im Rahmen von Abschlußprüfungen IT-Systemprüfungen durchführen.
- (2) Der *IDW Prüfungsstandard* betrifft Abschlußprüfungen, d.h. Prüfungen von Jahres-, Konzern- und Zwischenabschlüssen i.S.d. *IDW Prüfungsstandards: Ziele und allgemeine Grundsätze der Durchführung von Abschlußprüfungen (IDW PS 200)*<sup>2</sup>, Tz. 5).
- (3) Wirtschaftszweigspezifische (z.B. bei der Prüfung von Kreditinstituten, Versicherungsunternehmen) und sonstige Besonderheiten, die im Einzelfall zusätzlich zu berücksichtigen sind, bleiben in diesem *IDW Prüfungsstandard* außer Betracht.
- (4) Für Prüfungen mit einem abweichenden Prüfungsgegenstand oder Prüfungen, die Abschlußprüfungen nach Art und Umfang nicht entsprechen, ist im Einzelfall zu entscheiden, inwieweit die Grundsätze dieses *IDW Prüfungsstandards* Anwendung finden. Erweiterte und spezielle Anforderungen an IT-Systemprüfungen, die über die für Abschlußprüfungen geltenden Anforderungen hinausgehen, sind in der *Stellungnahme HFA 4/1997: Projektbegleitende Prüfung EDV-gestützter Systeme*<sup>3</sup> und dem *IDW Prüfungsstandard: Erteilung und Verwendung von Softwarebescheinigungen (IDW PS 880)*<sup>4</sup> dargestellt.
- (5) Der *IDW Prüfungsstandard* entspricht dem International Standard on Auditing (ISA) 401 „Auditing in a Computer Information Systems Environment“<sup>5</sup> unter Berücksichtigung neuer Entwicklungen. Der *IDW Prüfungsstandard* beinhaltet zudem ergänzende Anforderungen, die sich aus der deutschen Rechtslage und Berufsübung ergeben.

---

<sup>2</sup> WPg 2000, S. 706 ff.

<sup>3</sup> WPg 1997, S. 680 ff.

<sup>4</sup> WPg 1998, S. 1066 ff.

<sup>5</sup> IFAC Handbook 2000, Technical Pronouncements, New York 2000, S. 230 ff.

- (6) Dieser *IDW Prüfungsstandard* ersetzt die Abschn. C. und D. der *Stellungnahme FAMA 1/1987: Grundsätze ordnungsmäßiger Buchführung bei computergestützten Verfahren und deren Prüfung*.<sup>6</sup>
- (7) Zum Einsatz von IT im Unternehmen und der Einrichtung eines IT-Systems gelten die Regelungen der *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1)*.<sup>7</sup> Dieser *IDW Prüfungsstandard* basiert auf den allgemeinen Anforderungen an die Prüfung des internen Kontrollsystems durch den Abschlußprüfer (vgl. *IDW Prüfungsstandard: Das interne Kontrollsystem im Rahmen der Abschlußprüfung (IDW PS 260)*).<sup>8</sup>

## 2. Ziele und Umfang von IT-Systemprüfungen

- (8) Der Abschlußprüfer hat das IT-gestützte Rechnungslegungssystem daraufhin zu beurteilen, ob es den gesetzlichen Anforderungen – insbesondere den im *IDW ERS FAIT 1* dargestellten Ordnungsmäßigkeits- und Sicherheitsanforderungen – entspricht, um die nach § 322 Abs. 1 Satz 1 HGB i.V.m. § 317 Abs. 1 Satz 1 HGB und § 321 Abs. 2 Satz 2 HGB geforderten Prüfungsaussagen über die Ordnungsmäßigkeit der Buchführung treffen zu können (vgl. *IDW Prüfungsstandard: Grundsätze für die ordnungsmäßige Erteilung von Bestätigungsvermerken bei Abschlußprüfungen (IDW PS 400)*,<sup>9</sup> Tz. 42, 66; *IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Berichterstattung bei Abschlußprüfungen (IDW PS 450)*<sup>10</sup>, Tz. 60 ff.). Folglich hat der Abschlußprüfer das IT-System des Unternehmens insoweit zu prüfen, als dessen Elemente dazu dienen, Informationen über Geschäftsvorfälle abzubilden, die für die Rechnungslegung von Bedeutung sein können (rechnungslungsrelevant). Der Begriff der Rechnungslegung umfaßt dabei die Buchführung, den Jahresabschluß und den Lagebericht bzw. auf Konzernebene den Konzernabschluß und den Konzernlagebericht (vgl. *IDW PS 400*, Tz. 2).

---

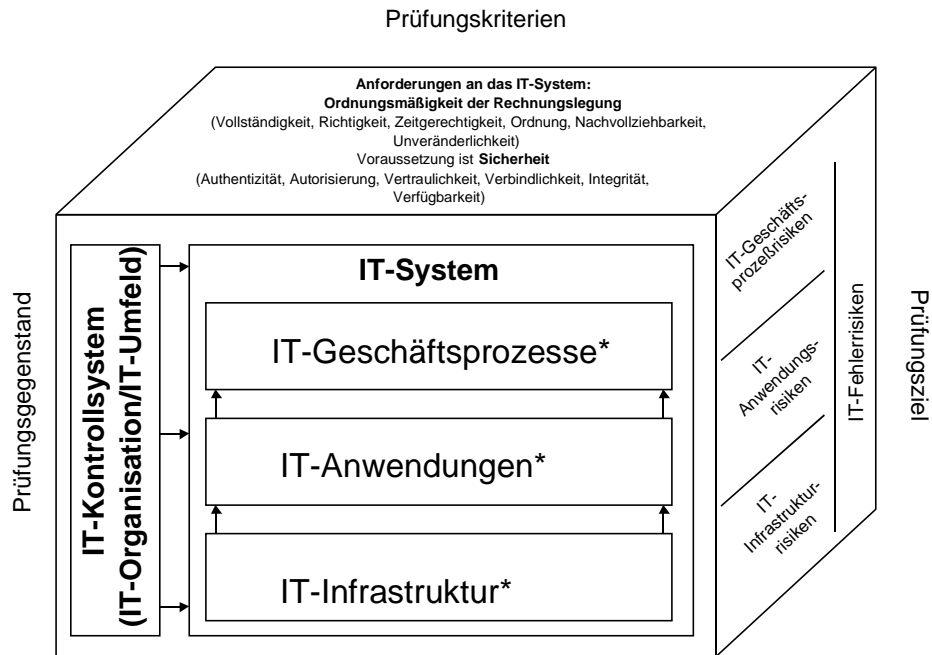
<sup>6</sup> WPg 1988, S. 1 ff.

<sup>7</sup> Liegt derzeit als *Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1)* vor, (WPg 2001, S. 512 ff.).

<sup>8</sup> WPg 2001, S. ■

<sup>9</sup> WPg 1999, S. 641 ff.

<sup>10</sup> WPg 1999, S. 601 ff.



\* soweit rechnungslegungsrelevant

Abbildung: IT-Systemprüfung

- (9) Die IT-Systemprüfung stellt damit einen Teilausschnitt aus der Prüfung des internen Kontrollsystems dar und wird nach den allgemeinen Grundsätzen für die Prüfung von internen Kontrollsystemen geplant und durchgeführt. Ziel der IT-Systemprüfung ist die Beurteilung der IT-Fehlerrisiken, d.h. des Risikos wesentlicher Fehler im IT-System, soweit diese rechnungslegungsrelevant sind (vgl. *IDW PS 260*, Tz. 23 ff.).

Da das IT-Kontrollsystem integraler Bestandteil des Internen Kontrollsystems eines Unternehmens ist, hat der Abschlußprüfer die aussagebezogenen Prüfungshandlungen (analytische Prüfungshandlungen sowie Einzelfallprüfungen) unter Berücksichtigung sowohl der Ergebnisse der Prüfung des IT-Kontrollsystems als auch des Internen Kontrollsystems in seiner Gesamtheit zu bemessen.

- (10) IT-Systemprüfungen erfordern spezielle, auf das IT-System bezogene Prüfungsmethoden. Prüfungsgegenstand sind die Prüfungsgebiete IT-Infrastruktur, IT-Anwendungen und IT-gestützte Geschäftsprozesse einschließlich des IT-Umfeldes und der IT-Organisation. Art und Umfang der IT-Systemprüfungen bestimmen sich auch aus
- der Wesentlichkeit des IT-Systems für die Rechnungslegung bzw. für die Beurteilung der Ordnungsmäßigkeit der Rechnungslegung und
  - der Komplexität des eingesetzten IT-Systems, die insbesondere von dem Grad der Integration in umfassende EDV-Lösungen abhängt.
- (11) Die IT-Systemprüfung kann sich grundsätzlich auf die Elemente des IT-Systems beschränken, die für die IT-gestützte Rechnungslegung von wesentlicher Bedeutung sein können.

- (12) Bei der Bemessung des Umfangs von IT-Systemprüfungen ist weiterhin die Komplexität der eingesetzten IT zu berücksichtigen. Bei IT-Anwendungen mit geringer Komplexität (z.B. PC-gestützte Buchführungssysteme) kann sich die IT-Systemprüfung auf ausgewählte Funktionalitäten wie bspw. Funktionalitäten zur Generierung automatischer Buchungen beschränken, wenn die hinreichende Sicherheit der Prüfungsaussagen (vgl. *IDW PS 200*, Tz. 24 ff.) durch aussagebezogene Prüfungshandlungen bzw. Plausibilisierungshandlungen erlangt werden kann. Bei komplexen IT-Systemen ist eine umfassende IT-Systemprüfung stets erforderlich, weil eine Beurteilung der Ordnungsmäßigkeit und Sicherheit der IT-gestützten Rechnungslegung ohne Berücksichtigung der programmierten rechnungslegungsrelevanten Abläufe nicht möglich ist.
- (13) Neben der Aufnahme des IT-Systems im Unternehmen muß sich der Abschlußprüfer auch einen Überblick über ausgelagerte Bestandteile des IT-Systems verschaffen. Die Prüfung von Unternehmen mit einem eigenständigen Rechenzentrumsbetrieb im Unternehmen erfordert eine andere Vorgehensweise als die Prüfung von Unternehmen, deren IT-System ganz oder teilweise ausgelagert ist. Die Verantwortlichkeit des Abschlußprüfers erstreckt sich in jedem Fall auf das gesamte rechnungslegungsrelevante IT-System.
- (14) IT-Systemprüfungen können als ex-post-Prüfungen, nach Modifikation, Neueinführung oder Erweiterungen wesentlicher rechnungslegungsrelevanter IT-Anwendungen erfolgen. Im Interesse einer frühzeitigen Berücksichtigung von Ordnungsmäßigkeits- und Sicherheitsanforderungen empfiehlt sich die projektbegleitende Prüfung EDV-gestützter Systeme (vgl. *Stellungnahme HFA 4/1997*). In der Regel wird es sich anbieten, IT-Systemprüfungen bereits im Vorfeld der Jahresabschlußprüfung durchzuführen.

## 2.1. Risiken aus dem Einsatz von IT

- (15) Das Unternehmen führt Risikobeurteilungen zum Einsatz von IT im Unternehmen durch, um Risiken festzustellen und zu analysieren, die die Entwicklung des Unternehmens beeinträchtigen (vgl. *IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340)*<sup>11</sup>) oder der Erreichung der Unternehmensziele entgegenstehen können. Hierzu zählen auch die Risiken, die zu wesentlichen Fehlern in der Rechnungslegung führen können. Das Verfahren und die Ergebnisse der Risikobeurteilungen des Unternehmens im Bereich Rechnungslegung stellen den Ausgangspunkt für die Risikobeurteilungen im Rahmen der risikoorientierten Prüfungsplanung des Abschlußprüfers dar (vgl. *IDW PS 260*, Tz. 48).
- (16) Die mit der konkreten Ausgestaltung des IT-Systems einhergehenden Risiken für wesentliche Fehler in der Rechnungslegung werden als IT-Fehlerrisiken bezeichnet. IT-Fehlerrisiken setzen sich aus den inhärenten

---

<sup>11</sup> WPg 1999, S. 658 ff.

Risiken und den Kontrollrisiken zusammen, die durch den Abschlußprüfer nicht beeinflussbar sind (vgl. *IDW PS 260*, Tz. 23 ff.). Eine separate Beurteilung von inhärenten IT-Risiken und IT-Kontrollrisiken kann allerdings in bestimmten Fällen aufgrund von Abhängigkeiten zwischen IT-Kontrollsystem und den inhärenten IT-Risiken zu einer falschen Beurteilung der Fehlerrisiken führen (vgl. *IDW PS 260*, Tz. 36).

(17) Inhärente IT-Risiken liegen dann vor, wenn durch den Einsatz eines IT-Systems Fehler auftreten können, die Auswirkungen auf die Ordnungsmäßigkeit der Rechnungslegung haben. Sie können sich im einzelnen auf die korrekte Ausgestaltung des Buchführungsverfahrens, auf die Richtigkeit der rechnungslegungsrelevanten Programmabläufe und Verarbeitungsregeln sowie auf die Sicherheit der rechnungslegungsrelevanten Daten und Informationen beziehen. Die Beurteilung der inhärenten Risiken ist auf Unternehmensebene und prüffeldspezifisch vorzunehmen.

(18) Bei der Beurteilung der inhärenten Risiken auf Unternehmensebene sind im Rahmen der Entwicklung einer Prüfungsstrategie insbesondere die folgenden IT-bezogenen Risikoindikatoren zu beachten:

- Risikoindikator "Abhängigkeit"

Die Abhängigkeit der Unternehmen von IT-Anwendungen und der IT-Infrastruktur hat, insbesondere durch die Vernetzung mit anderen Geschäftspartnern, Kreditinstituten, Behörden usw. stark zugenommen. Aufgrund des Automationsgrads und der Komplexität der IT-Systeme, die häufig ganze Prozeßketten unterstützen, sind die Unternehmen in hohem Maße auf die Funktionsfähigkeit und dauernde Betriebsbereitschaft der Systeme und das Fachwissen von Spezialisten angewiesen. Sensitive Daten, die ausschlaggebend für den Geschäftserfolg sind und in der Regel auch einen hohen Vermögenswert darstellen, werden überwiegend nur noch in IT-Systemen vorgehalten.

- Risikoindikator "Änderungen"

Wesentliche Risiken resultieren häufig aus größeren Änderungsprojekten im IT-Bereich, die durch die Einführung neuer Systeme und Technologien sowie Restrukturierungen bedingt sein können. Fehlgelaufene Projekte können wesentliche Kosten- und/oder Terminüberschreitungen sowie Mängel im Verfahrensablauf verursachen; dies gilt insbesondere bei unzureichenden Erfahrungen im Projektmanagement.

Auch die Risiken im Zusammenhang mit der Einführung von Standardsoftware werden häufig unterschätzt. Meist liegen keine fertigen Lösungen vor, weshalb ein komplexes und strukturiertes Anpassen (Customizing) der Software an die Anforderungen des Unternehmens erforderlich ist.

Die Änderungen im Unternehmensablauf werden häufig durch die Einführung neuer Technologien (z.B. Produktionsverfahren) bzw. Geschäftskonzepte, beispielsweise Konzepte für ein IT-gestütztes Beschaffungswesen

(e-Procurement), begleitet. Die IT-Auswirkungen solcher Änderungen sind anfänglich fremd und stellen hohe Anforderungen an die Anwender, die den Änderungen teilweise ablehnend gegenüberstehen.

- Risikoindikator “Know-how und Ressourcen”

Trotz der fortschreitenden Technik im IT-Bereich ist der Faktor “Mensch” für die Risikoanalyse unvermindert von Bedeutung. Wesentlich für den IT-Betrieb und die Geschäftsabwicklung ist aktuelles und spezifisches Fachwissen. Dies gilt nicht nur für die IT-Spezialisten in den IT-Abteilungen, sondern auch für die Anwender des eingesetzten IT-Systems. Auch Überlastungen im IT- und Anwenderbereich können erheblich zur Risikoerhöhung beitragen und durch unzureichende Pflege und Fehlbedienungen die Verlässlichkeit des IT-Systems beeinträchtigen.

- Risikoindikator “Geschäftliche Ausrichtung“

Wesentlich für die Risikobegrenzung ist die Ausrichtung der IT auf die Geschäftsstrategien und Prozeßanforderungen des Unternehmens. Geschäftsrisiken und IT-Risiken können dauerhaft nur auf ein sinnvolles Maß begrenzt werden, wenn die geschäftlichen Strategien des Unternehmens auch über eine adäquate IT-Strategie umgesetzt werden. Diese muß mittel- bis langfristig ausgerichtet, dokumentiert, von der Unternehmensleitung genehmigt sein und konkrete Maßnahmen beinhalten. Die geschäftlichen Anforderungen und die Anwenderbedürfnisse müssen klar definiert sein (z.B. über Fachkonzepte und Pflichtenhefte) und über IT-Funktionalitäten bzw. -Prozesse weitgehend abgedeckt werden. Zudem sind rechtliche Rahmenbedingungen – auch außerhalb des Handelsrechts – zu beachten (u.a. Anforderungen des Steuerrechts, Arbeits- und Umweltrechts, branchenabhängige Vorschriften, Vorgaben von Aufsichtsbehörden).

- (19) Im Rahmen der prüffeldspezifischen Beurteilung der inhärenten Risiken sind zur Entwicklung des Prüfungsprogramms u.a. folgende Aspekte von Bedeutung:

	<b>Abhängigkeit</b>	<b>Änderungen</b>	<b>Know-how/ Ressourcen</b>	<b>Geschäftliche Ausrichtung</b>
<b>IT-Umfeld</b>	Starke Dominanz der IT-Abteilung	Barrieren, Festhalten an bewährten Verfahren, ungenügende Unterstützung	Ungenügendes Bewußtsein für IT/Org-Themen	Unzureichende IT-Strategien und Planungen, unzureichendes Sicherheitskonzept
<b>IT-Organisation</b>	Unzureichende Organisation gefährdet Betrieb und Verfügbarkeit	Unzureichendes Projektmanagement, Zeit- und Kostenüberschreitungen	Fehlerhafte Aufgabenabwicklung	Ungenügende Anpassung der Richtlinien und Verfahren, Aufgaben und Kompetenzen
<b>IT-Geschäftsprozesse</b>	Abläufe sind weitgehend automatisiert bzw. komplex und damit fehleranfällig	Hohe Komplexität neuer Prozesse, fehlende Akzeptanz der Anwender	Unzureichende Unterstützung der Anwender	Langsame, ineffiziente und fehleranfällige Aufgabenabwicklung
<b>IT-Anwendungen</b>	Ausfälle gefährden Kernprozesse und Geschäftsabwicklung	Neue Funktionalität, Eingabe- und Bearbeitungsfehler	Fehlerhafte Anwendungsentwicklung/-betreuung	Geringe Unterstützung der Markt- und Benutzeranforderungen
<b>IT-Infrastruktur</b>	Unzureichende Gestaltung des Outsourcings erhöht Abhängigkeit von Dritten	Komplexe, neue Technologien, Sicherheitslücken	Veraltete Strukturen, unzureichende Pflege, Sicherheitslücken	Inhomogene IT-Plattform mit Insellösungen, unzureichende Sicherheit der Daten und Informationen

- (20) Die beispielhaft dargestellten Risikoindikatoren auf Unternehmens- und Prüffeldebene können das Entstehen von IT-Fehlerrisiken begründen, die sich als IT-Infrastruktur-, IT-Anwendungs- und IT-Geschäftsprozessrisiken konkretisieren:
- (21) *IT-Infrastrukturrisiken* bestehen darin, daß die für die Informationsverarbeitung notwendige IT-Infrastruktur nicht bzw. nicht in dem erforderlichen Maße zur Verfügung steht. Ursache kann die Anfälligkeit der Hardware für technische Störungen sein. Risiken der IT-Infrastruktur müssen durch ein auf das Bedürfnis des Unternehmens gerichtetes Sicherheitskonzept und die daraus abgeleiteten technischen und organisatorischen Kontrollen bewältigt werden.
- (22) *IT-Anwendungsrisiken* entstehen aus:
- fehlerhaften Funktionen in IT-Anwendungen

Diese betreffen sowohl Verarbeitungsfunktionen, die auf die Erfüllung der Journal-, Konten- und Belegfunktion gerichtet sind, als auch sonstige Programmabläufe und Verarbeitungsregeln, die rechnungslegungsrelevant sind.

- fehlenden oder nicht aktuellen Verfahrensregelungen und -beschreibungen
- unzureichend ausgeprägten Eingabe-, Verarbeitungs- und Ausgabekontrollen von Daten in IT-Anwendungen
- nicht ausreichenden Maßnahmen zur Gewährleistung der Softwaresicherheit im Zusammenhang mit der Sicherheitsinfrastruktur (unzureichende Zugriffsberechtigungskonzepte und Datensicherungs- und Wiederanlaufverfahren)

Daneben haben die jeweiligen Verfahren zur Auswahl, Entwicklung, Wartung und Freigabe von IT-Anwendungen Einfluß auf die IT-Fehlerrisiken.

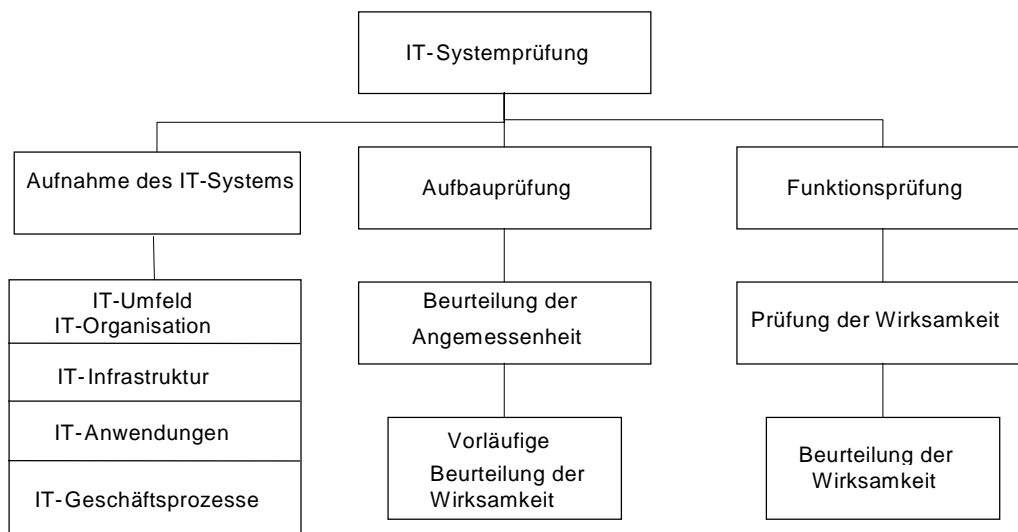
- (23) *IT-Geschäftsprozeßrisiken* entstehen, wenn sich Sicherheits- und Ordnungsmäßigkeitsanalysen nicht auf Geschäftsprozesse erstrecken, sondern nur auf die Kontrollelemente einer funktional ausgerichteten Organisation. Dabei können Risiken aus dem geschäftsprozeßbedingten Datenaustausch zwischen Teilsystemen, etwa unzureichende Transparenz der Datenflüsse, unzureichende Integration der Systeme oder mangelhafte Abstimm- und Kontrollverfahren in Schnittstellen zwischen Teilprozessen nicht erkannt werden. Es besteht die Gefahr, daß IT-Kontrollen bspw. Zugriffsrechte, Datensicherungsmaßnahmen, nur hinsichtlich der Teilprozesse, jedoch nicht hinsichtlich der Gesamtprozesse wirksam werden.
- (24) IT-Fehlerrisiken können auch aus der Kombination von IT-Infrastruktur-, IT-Geschäftsprozeß- und IT-Anwendungsrisiken entstehen und damit zu sachlich falschen Daten oder Verarbeitungsergebnissen und zu wesentlichen Fehlern in der Rechnungslegung führen.

## **2.2. Vorgehensweise bei der IT-Systemprüfung**

- (25) Der Abschlußprüfer hat die IT-Systemprüfung so zu planen und durchzuführen, daß er die IT-Fehlerrisiken des im Unternehmen eingesetzten IT-Systems zutreffend beurteilt.
- (26) Hierzu muß der Abschlußprüfer feststellen, ob das Unternehmen durch die Einrichtung eines wirksamen internen Kontrollsystems auf die festgestellten inhärenten Risiken des IT-Systems reagiert hat. Ein IT-Kontrollsystem ist aus Sicht des Abschlußprüfers dann wirksam, wenn es verhindert, daß inhärente Risiken des IT-Systems zu wesentlichen Fehlern in der Rechnungslegung führen.
- (27) Als wesentliche Voraussetzung für die Beurteilung des IT-Kontrollsystems hat der Abschlußprüfer die Angemessenheit der Bewertung der IT-Fehlerrisiken durch die Unternehmensleitung im Rahmen der Umsetzung der

IT-Strategie (vgl. *IDW ERS FAIT 1*, Tz. 72) und des Sicherheitskonzeptes (vgl. *IDW ERS FAIT 1*, Tz. 21) zu beurteilen.

- (28) Um zu verstehen, wie die Unternehmensleitung zur Risikobeurteilung kommt und wie sie über die Einrichtung eines IT-Kontrollsystems zur Begrenzung möglicher Auswirkungen dieser Risiken entscheidet, sind alle wesentlichen Regelungen zu untersuchen, die auf die Feststellung und Analyse von für die Rechnungslegung relevanten IT-Risiken gerichtet sind. Der Abschlußprüfer muß darüber hinaus nachvollziehen, wie die Unternehmensleitung sämtliche Risiken identifiziert, die sich auf die Ordnungsmäßigkeit und Verlässlichkeit der Rechnungslegung auswirken können, und wie deren Tragweite in bezug auf die Eintrittswahrscheinlichkeit und auf die quantitativen Auswirkungen beurteilt wird.
- (29) Zur Prüfung der Wirksamkeit des IT-Kontrollsystems sind folgende Prüfungsschritte in den im Rahmen der Prüfungsplanung festgelegten Prüfungsfeldern erforderlich:
- Aufnahme des IT-Systems als Basis der Kenntnisse des Abschlußprüfers über das IT-Kontrollsystem
  - Prüfung des Aufbaus des IT-Kontrollsystems (Aufbauprüfung)
  - Prüfung der Funktion des IT-Kontrollsystems (Funktionsprüfung).



- (30) Der Abschlußprüfer hat sich zunächst einen Überblick über das zur Rechnungslegung eingesetzte IT-System zu verschaffen. Soweit das identifizierte IT-Umfeld, die IT-Organisation, die IT-Infrastruktur, die IT-Anwendungen sowie die IT-gestützten Geschäftsprozesse relevant für die Rechnungslegung sein können, hat er die betreffenden Elemente des IT-Systems aufzunehmen. Zur Gewinnung von Informationen über das eingesetzte IT-System erhebt der Abschlußprüfer neben den Hardware- und Softwarekomponenten

auch die vorgesehenen IT-Kontrollen und damit den von der Unternehmensleitung angewiesenen Sollzustand des IT-Systems.

- (31) Die durch die Aufnahme des IT-Systems ermittelten Informationen und Kenntnisse über die IT-Systeme des Unternehmens sind Basis für die Aufbau- und Funktionsprüfung, wobei mittels der Aufbauprüfung zunächst eine vorläufige Beurteilung der Wirksamkeit des internen Kontrollsystems vorzunehmen ist. Zur abschließenden Beurteilung der Ordnungsmäßigkeit und Sicherheit der IT-gestützten Rechnungslegung sind die Ergebnisse der Aufbauprüfung durch Funktionsprüfungen zu ergänzen (vgl. *IDW PS 260*, Tz. 32).
- (32) Durch die Aufbauprüfung wird die Angemessenheit der personellen, organisatorischen und technischen Maßnahmen beurteilt, die das Unternehmen zur
- Schaffung eines geeigneten IT-Umfeldes,
  - Einführung einer geeigneten IT-Organisation,
  - Gewährleistung eines geordneten IT-Betriebs, insbesondere durch die Sicherung der Verfügbarkeit des IT-Systems,
  - Gewährleistung der Sicherheit, insbesondere durch die angemessene Umsetzung eines geeigneten IT-Sicherheitskonzeptes,
  - Einhaltung der erforderlichen Funktionalität der IT-Anwendungen,
  - Gewährleistung der Wirksamkeit der in den IT-Geschäftsprozessen enthaltenen Kontrollmaßnahmen sowie zur
  - Schaffung eines geeigneten Überwachungssystems
- getroffen hat. Als Ergebnis der Aufbauprüfung hat der Abschlußprüfer eine vorläufige Beurteilung der Wirksamkeit des IT-Systems einschließlich des Umfangs der IT-Fehlerrisiken vorzunehmen.
- (33) Ziel der Aufbauprüfung ist eine Beurteilung, ob das angewiesene IT-Kontrollsystem (Soll-Zustand) des Unternehmens unter Berücksichtigung der prüfungspezifischen inhärenten Risiken angemessen und im geplanten Umfang wirksam ist. Dabei unterstellt der Abschlußprüfer zunächst, daß die Kontrollen wie geplant durchgeführt und eingehalten werden. Prüfungsgegenstand sind sowohl die einzelnen IT-Kontrollen (z.B. Eingabe-, Ausgabe- und Verarbeitungskontrollen) als auch deren Zusammenwirken.
- (34) Typische Prüfungshandlungen im Rahmen von Aufbauprüfungen sind
- Durchsicht von Unterlagen,
  - Befragungen,
  - Beobachtung von Aktivitäten und Arbeitsabläufen.
- (35) Funktionsprüfungen werden in den Bereichen des IT-Systems durchgeführt, die vom Abschlußprüfer im Rahmen der Aufbauprüfung als angemessen beurteilt wurden. Ziel der Funktionsprüfung ist nunmehr die Beurteilung durch den Abschlußprüfer, ob die eingerichteten IT-Kontrollen wirksam sind und damit zur Begrenzung der IT-Fehlerrisiken (Tz. 16) beitragen.

- (36) Die im Ergebnis der Funktionsprüfungen getroffene abschließende Beurteilung der Wirksamkeit und kontinuierlichen Anwendung des IT-Kontrollsystems ist im Verlauf der Prüfung gegebenenfalls den gewonnenen Erkenntnissen anzupassen.
- (37) Neben den bereits für die Durchführung von Aufbauprüfungen genutzten Prüfungshandlungen kommen für Funktionsprüfungen weitere Prüfungstechniken in Betracht. Die Wirksamkeit von Kontrollen kann der Abschlußprüfer auch durch
- Plausibilitätsbeurteilungen,
  - Nachvollzug von Kontrollen in Form von Wiederholungen bzw. eigenen Kontrolltests oder
  - Verwendung von Unterlagen Dritter
- beurteilen.
- (38) Die Beurteilung der Wirksamkeit der IT-Organisation kann beispielsweise anhand des Vergleichs der Arbeitsergebnisse der jeweiligen IT-Organisation mit branchentypischen Ausgestaltungen oder mit Best-Practices vorgenommen werden. Weiterhin können Plausibilitätsbeurteilungen durch Verprobungen von kumulierten Verkehrszahlen oder Mengenströmen zwischen IT-Systemen oder deren Teilsystemen stattfinden.
- (39) Der Nachvollzug von IT-Kontrollen durch Wiederholungen oder Tests mit eigenen Testdaten kommt dann in Betracht, wenn durch das angewandte Verfahren die Reproduzierbarkeit der Ergebnisse nachgewiesen werden kann. Dabei kann der Abschlußprüfer die Ergebnisse von Kontrolltests in einem Testsystem nur dann auf das produktiv eingesetzte IT-System (Produktionssystem) übertragen, wenn durch ordnungsgemäße Freigabe- und ÜbergabeprozEDUREN die Identität beider IT-Anwendungen nachgewiesen werden kann.
- (40) Im Interesse einer wirksamen und wirtschaftlichen Prüfung ist abzuwägen, ob und inwieweit die Arbeiten der Internen Revision (vgl. *Entwurf IDW Prüfungsstandard: Interne Revision und Abschlußprüfung (IDW EPS 321)*<sup>12</sup>, Tz. 11 ff.), von anderen Mitarbeitern des Unternehmens oder von externen Sachverständigen bei der Festlegung der Prüfungshandlungen im Rahmen der Abschlußprüfungen zu berücksichtigen sind.
- So kann der Abschlußprüfer bspw. zur Beurteilung der Wirksamkeit von Backup-Regelungen auf die Testprotokolle des Unternehmens zurückgreifen, ohne erneute Backup-Übungen zu verlangen. Zur Beurteilung von IT-Anwendungen wird der Abschlußprüfer die Testfalldokumentation des Unternehmens würdigen und davon den Umfang eigener Kontrolltests abhängig machen.
- (41) Das Gesamturteil über das jeweilige Prüfungsfeld einer IT-Systemprüfung basiert zusammenfassend auf

---

<sup>12</sup> WPg 2001, S. 570 ff.

- den vom Abschlußprüfer erlangten Kenntnissen über das für die Rechnungslegung eingesetzte IT-System,
- einer vorläufigen Beurteilung des IT-Kontrollsystems auf der Basis der inhärenten Risiken verbunden mit der Einschätzung der Angemessenheit der vom Unternehmen eingerichteten Maßnahmen (Aufbauprüfung),
- der abschließenden Würdigung durch die Prüfung der Wirksamkeit der Maßnahmen i.S.e. ordnungsgemäßen und kontinuierlichen Anwendung (Funktionsprüfung) sowie
- der Prüfung der wesentlichen auf die Überwachung des IT-Kontrollsystems bezogenen Maßnahmen (z.B. Tätigkeit der Internen Revision).

### **2.3. Besonderheiten des risikoorientierten Prüfungsansatzes bei IT-Systemprüfungen**

- (42) Bei der Entscheidung über die Ausgestaltung des risikoorientierten Prüfungsansatzes ist die Aufbau- und Ablauforganisation des zu prüfenden Unternehmens ausschlaggebend. Grundsätzlich können funktional ausgerichtete und geschäftsprozeßorientierte Unternehmensorganisationen unterschieden werden. Ebenso kann der Prüfungsansatz funktional oder prozeßorientiert ausgerichtet werden. Sowohl die Anwendung des funktional als auch des prozeßorientierten Prüfungsansatzes muß eine Beurteilung des Risikos für das Auftreten wesentlicher Fehler in der Rechnungslegung ermöglichen.
- (43) Bei einer auf den jeweiligen funktionalen Bereich ausgerichteten Prüfung des IT-Kontrollsystems besteht die Gefahr, daß der geschäftsprozeßbedingte Datenaustausch unberücksichtigt bleibt und systemtechnische Zusammenhänge nur unzureichend berücksichtigt werden (vgl. *IDW ERS FAIT 1*, Tz. 105 f.). Dies kann dazu führen, daß das IT-Kontrollsystem hinsichtlich des funktional abgegrenzten IT-Teilsystems als wirksam beurteilt wird, jedoch bspw. durch Manipulationen in den vor- oder nachgelagerten IT-Teilsystemen gezielt umgangen werden kann.
- (44) Besonders gefährdet sind komplexe Geschäftsprozesse, die mit ihren Teilprozessen mehrere funktionale Bereiche im Unternehmen mit nicht integrierten Bestandteilen von IT-Anwendungen bzw. der IT-Infrastruktur betreffen. Hier ist sicherzustellen, daß der Datenfluß und die systemtechnischen Zusammenhänge zwischen den Teilsystemen hinreichend berücksichtigt werden.

## **3. Durchführung von IT-Systemprüfungen**

### **3.1. Auftragsannahme und Prüfungsplanung**

- (45) Vor der Auftragsannahme ist gewissenhaft zu prüfen, ob der Abschlußprüfer nach den Berufspflichten und nach der Berufsauffassung über die besonderen Kenntnisse und Erfahrungen verfügt, um eine im Rahmen der Abschlußprüfung vorzunehmende IT-Prüfung sachgerecht durchführen zu können

(vgl. *Stellungnahme VO 1/1995: Zur Qualitätssicherung in der Wirtschaftsprüferpraxis*<sup>13</sup>, Abschn. B. II.).

- (46) Hierzu müssen Abschlußprüfer und die im Rahmen der IT-Systemprüfung eingesetzten fachlichen Mitarbeiter die für ihre Tätigkeit ausreichenden Sachkenntnisse sowohl allgemein im Bereich der IT als auch über das vom Unternehmen eingesetzte IT-System besitzen (vgl. *IDW Prüfungsstandard: Kenntnisse über die Geschäftstätigkeit sowie das wirtschaftliche und rechtliche Umfeld des zu prüfenden Unternehmens im Rahmen der Abschlußprüfung (IDW PS 230)*<sup>14</sup>).
- (47) Sofern der Abschlußprüfer nicht selbst über die erforderlichen Kenntnisse zur Durchführung einer IT-Systemprüfung verfügt, ist es im Rahmen der Prüfungsdurchführung erforderlich, Arbeitsergebnisse oder Untersuchungen von IT-Sachverständigen in die eigenverantwortliche Bildung des Prüfungsurteils einzubeziehen. Deren Arbeit kann unbeschadet der Eigenverantwortlichkeit des Abschlußprüfers als Prüfungsnachweis für die Abschlußprüfung verwertet werden.
- (48) Im Rahmen der Planung von IT-Systemprüfungen (vgl. *IDW Prüfungsstandard: Grundsätze der Planung von Abschlußprüfungen (IDW PS 240)*<sup>15</sup>) hat der Abschlußprüfer die Auswirkungen des Einsatzes von IT im Unternehmen auf seinen Prüfungsansatz hinreichend zu berücksichtigen. Dazu hat der Abschlußprüfer sich ausreichende Kenntnisse über das eingesetzte IT-System zu verschaffen. Diese Kenntnisse umfassen u.a. den Umgang der Unternehmensleitung mit den IT-Risiken und die Organisation der IT-gestützten Geschäftsprozesse. Die Prüfungsplanung umfaßt die Entwicklung einer Prüfungsstrategie und darauf aufbauend ein Prüfungsprogramm, welches die im einzelnen durchzuführenden Prüfungshandlungen enthält. Im Rahmen der Entwicklung der Prüfungsstrategie ist die Beurteilung der inhärenten IT-Risiken auf Unternehmensebene vorzunehmen. Bei der Entwicklung des Prüfungsprogramms sind die prüffeldspezifischen inhärenten IT-Risiken zu beurteilen.

### **3.2. Erhebung von Informationen**

- (49) Die Erhebung der rechnungslegungsrelevanten IT-Systemelemente kann anhand von Organigrammen, Prozeßbeschreibungen und -richtlinien sowie Aufstellungen über Hard- und Software erfolgen.
- (50) Die Aufnahme der folgenden Bereiche umfaßt auch jeweils die Aufnahme des zugeordneten IT-Überwachungssystems:

#### **IT-Umfeld**

---

<sup>13</sup> WPg 1995, S. 824 ff.

<sup>14</sup> WPg 2000, S. 842 ff.

<sup>15</sup> WPg 2000, S. 846 ff.

- Grundeinstellung zum Einsatz von IT-Systemen, beispielsweise dokumentiert im IT-Sicherheitskonzept (Unternehmensleitlinien, IT-Sicherheitshandbücher u.a.)
- verbindlich niedergelegte IT-Strategie, abgeleitet aus der Unternehmensstrategie
- High Level Controls (vgl. *IDW PS 260*, Tz. 6)

### **IT-Organisation**

- Organigramme und Ablaufpläne
- Verantwortlichkeiten und Kompetenzen
- Regelungen und Verfahren zur Steuerung des IT-Betriebs
- Maßnahmen und Regelungen für die Entwicklung, Einführung und Änderung von IT-Anwendungen

### **IT-Infrastruktur**

- Hardware (Großrechner, Client-Server-Systeme, PC und PC-Netzwerke)
- Betriebssysteme (z.B. MVS, UNIX-Derivate, Netzwerkbetriebssysteme, PC-Systeme) sowie Middleware (z.B. Archivierungs- oder Bibliothekssysteme)
- Netzwerke (Local Area Network (LAN), Wide Area Network (WAN), Internet/Intranet/Extranet)
- IT-Betrieb (Organisation, Systemverwaltung, Produktionsabwicklung, Ressourcen-, Change- und Problemmanagement)
- Sicherheitskonzept (Zugriffskontrollsysteme, Firewalls, Datensicherung)

### **IT-Anwendungen**

- Bezeichnung der Software, Kurzbeschreibung des Aufgabengebietes und zugrunde liegende Hardwareplattform
- Klassifizierung der Software nach Dialog- und/oder Batchanwendung
- Software-Typ (Individual-Software, Standard-Software, modifizierte Standard-Software, Hersteller und eingesetzte Version)
- Angaben zu den verwendeten Programmiersprachen und zur Datenhaltung (Datenbank- bzw. Dateiorganisation)

### **IT-Geschäftsprozesse**

- rechnungslegungsrelevante Unternehmensabläufe anhand der funktions- oder prozeßorientierten Beschreibung der Ablauforganisation
- dazu eingesetzte IT-Infrastruktur und IT-Anwendungen sowie relevante Schnittstellen
- Datenfluß (Datenherkunft, Verarbeitung, Datenübergabe)

- Verbindung zur Buchführung (vgl. *IDW ERS FAIT 1*, Tz. 15).

### **3.3. Prüfung des IT-Umfelds und der IT-Organisation**

- (51) Die Aufbauprüfung des IT-Umfelds und der IT-Organisation erfolgt auf Basis des vorgelegten Sicherheitskonzeptes, der IT-Strategie, der Regelungen zur Aufbau- und Ablauforganisation (Organisationsplan, Richtlinien und Arbeitsanweisungen) sowie auf der Grundlage von Prozeß- und Funktionsbeschreibungen. Anhand der vorgelegten Unterlagen hat der Abschlußprüfer die Angemessenheit der Richtlinien und Verfahren im Hinblick auf Vollständigkeit, Aktualität und hinreichende Beachtung von Organisationsprinzipien (z.B. Funktionstrennung und Vertretungsregelungen) zu beurteilen.
- (52) Die Prüfung der Wirksamkeit der Maßnahmen im Bereich von IT-Umfeld und IT-Organisation wird der Abschlußprüfer anhand von Stichproben im Unternehmen durchführen.

Mögliche Prüfungshandlungen sind

- die Beobachtung von Abläufen und Vergleich mit Organisationsrichtlinien und Prozeßbeschreibungen,
- der Abgleich von im Sicherheitskonzept festgelegten Richtlinien zum Zugriffsschutz (z.B. Passwortlänge) mit den entsprechenden Parametern von Zugriffsschutzverfahren oder
- die Verifizierung der Maßnahmen zur Funktionstrennung durch Kompetenzregelungen und Bearbeitungsvermerke.

### **3.4. Prüfung der IT-Infrastruktur**

- (53) Die Prüfung der IT-Infrastruktur richtet sich auf
- die physischen Sicherungsmaßnahmen,
  - logische Zugriffskontrollen,
  - Datensicherungs- und Auslagerungsverfahren,
  - Maßnahmen für den geordneten Regelbetrieb,
  - Verfahren für den Notbetrieb sowie
  - Maßnahmen zur Sicherung der Betriebsbereitschaft.

#### **3.4.1. Physische Sicherungsmaßnahmen**

- (54) Physische Sicherungsmaßnahmen zum Schutz der Hardware sowie der Programme, Daten und Informationen umfassen u.a. bauliche Maßnahmen, Zugangskontrollen, Feuerschutzmaßnahmen und Maßnahmen zur Sicherung der Stromversorgung. Sie dienen der Datensicherheit und dem Datenschutz und sollen die Integrität sowie die Verfügbarkeit der IT gewährleisten (vgl. *IDW ERS FAIT 1*, Tz. 23).

- (55) Die Aufbauprüfung der physischen Sicherungsmaßnahmen richtet sich auf die Beurteilung der Angemessenheit der festgelegten Sicherheitsmaßnahmen im Hinblick auf die eingesetzte Technik und den gewünschten Schutzzweck.
- (56) Zur Prüfung der Wirksamkeit der Maßnahmen im Rahmen der Funktionsprüfung muß sich der Abschlußprüfer bspw. durch eine Begehung des Rechenzentrums bzw. des Rechnerraums von der Existenz der technischen Sicherungsmaßnahmen (Zutrittskontrollsysteme, Feuerlöschsysteme, Brandabschnitte) überzeugen. Zusätzlich sollte sich der Abschlußprüfer durch Stichproben (z.B. Abgleich der im Zugangskontrollsystem eingerichteten persönlichen Zugangsberechtigten mit den Zugangsberechtigten laut Organisationsanweisung oder durch Einsicht in Wartungsprotokolle für Klima- und Brandmeldeanlagen) von der Funktionsfähigkeit der Sicherungsmaßnahmen überzeugen.

### **3.4.2. Logische Zugriffskontrollen**

- (57) Logische Zugriffskontrollen sind wesentliche Elemente der Datensicherheit und des Datenschutzes und Voraussetzung zur Gewährleistung der Vertraulichkeit. Die Sicherheitsanforderungen Autorisierung und Authentizität bedingen zwingend logische Zugriffskontrollen (vgl. *IDW ERS FAIT 1*, Tz. 23). Die Prüfungshandlungen im Rahmen der Aufbauprüfung logischer Zugriffskontrollen richten sich auf die Implementierung eines organisatorischen Verfahrens zur Beantragung, Genehmigung und Einrichtung von Benutzerberechtigungen in IT-Systemen. Dies betrifft sowohl die Berechtigungen auf Betriebssystemebene (Anmeldung gegenüber Rechnern in einem Netzwerk) als auch die Rechte zur Ausführung von Transaktionen in einer IT-Anwendung. Zugriffskontrollen sind als angemessen zu beurteilen, wenn sie geeignet sind sicherzustellen, daß die Berechtigungsverwaltung und die eingerichteten Systemrechte den Festlegungen im Sicherheitskonzept entsprechen und damit unberechtigte Zugriffe auf Daten und Informationen sowie Programmabläufe zur Veränderung von Daten ausgeschlossen sind. Zudem müssen Zugriffskontrollen so ausgestaltet sein, daß sie die Identität des Benutzers eindeutig feststellen und nicht autorisierte Zugriffsversuche abgewiesen werden.
- (58) Die Prüfung der Wirksamkeit der logischen Zugriffskontrollen erstreckt sich zum einen auf die Übereinstimmung von definierten Verfahren mit den tatsächlichen Abläufen der Benutzeradministration und -pflege. Zum anderen sind Benutzerberechtigungen in Stichproben daraufhin zu prüfen, ob die eingerichteten Berechtigungen den beantragten Rechten und dem tatsächlichen Aufgabengebiet des Mitarbeiters entsprechen.

### **3.4.3. Datensicherungs- und Auslagerungsverfahren**

- (59) Datensicherungs- und Auslagerungsverfahren sind Voraussetzungen für die Funktionsfähigkeit der Datenverarbeitung und zudem Voraussetzung zur Si-

cherung der Vollständigkeit und Verfügbarkeit der Daten und Programme. Sie sind erforderlich, um den Anforderungen nach Lesbarmachung der Daten – auch i.S.e. ordnungsmäßigen Buchführung – gerecht zu werden.

- (60) Die Aufbauprüfung der Datensicherungs- und Auslagerungsverfahren erstreckt sich u.a. auf die Angemessenheit des Datensicherungsverfahrens (Mehr-Generationen-Prinzip mit Tages-, Wochen-, Monats- und evtl. Jahressicherungen), die verwendeten Sicherungsmedien (z.B. Bänder, CD-WORM, Platten) sowie die Auslagerungsorte und -intervalle. Die Prüfung der Funktionsfähigkeit der Datensicherung richtet sich auf die Einsichtnahme in Logaufzeichnungen der zur Datensicherung verwendeten Programme, den stichprobenhaften Abgleich von Medienverzeichnissen mit den im Archiv gelagerten Sicherungsmedien oder die Begehung des zur Auslagerung verwendeten Archivs mit Inaugenscheinnahme der Zugangskontroll- und Brandschutzeinrichtungen.
- (61) Sofern das Unternehmen Sicherungsmedien auch zur Erfüllung gesetzlicher Aufbewahrungsfristen erstellt, sind die Maßnahmen zur Gewährleistung der jederzeitigen Lesbarkeit der Daten über die gesamte Aufbewahrungsfrist zu prüfen. Hierzu zählen das Übertragen von Sicherungsmedien bei Medienwechsel und der Test der Lauffähigkeit von Anwendungen und Daten in einer anderen als der ursprünglichen Systemumgebung. Der Abschlußprüfer muß beurteilen, ob das Unternehmen, z.B. durch Tests der Datenrücksicherung, die Wiederherstellbarkeit von Programmen und Daten aus den Sicherungsmedien sichergestellt hat.

#### **3.4.4. Maßnahmen für den Regel- und Notbetrieb**

- (62) Die Maßnahmen für den geordneten Regelbetrieb von IT-Anwendungen sind abhängig von der Art und Komplexität der eingesetzten Hardware und der Netzkomponenten. Beispielsweise sind in einem Rechenzentrum zur Sicherung der Integrität und Verfügbarkeit des IT-Systems (vgl. *IDW ERS FAIT 1*, Tz. 23) sowohl detaillierte organisatorische Anweisungen zur Abwicklung der Datenverarbeitung (RZ-Handbuch, Operatoranweisungen) als auch technische Systeme zur Steuerung des Rechnerbetriebs (Jobsteuerungssysteme, Überwachungssysteme, Verfahren zur Gewährleistung eines operatorlosen RZ-Betriebs) erforderlich. Bei IT-Systemen, die aus kleinen PC-Netzwerken oder nur einem Server bestehen, kann der Regelungsbedarf entsprechend weniger umfassend sein. Damit können separate technische Verfahren zur Rechnersteuerung oft nicht erforderlich sein.
- (63) Die Maßnahmen für den geordneten Regelbetrieb sind angemessen, wenn die Abläufe hinreichend geregelt und dokumentiert sind und die Abwicklung der IT-Anwendungen nachvollziehbar ist (z.B. durch Jobprotokolle) und damit geeignet sind, die Verfügbarkeit des IT-Systems sicherzustellen.
- (64) Die Funktionsfähigkeit und kontinuierliche Anwendung der Maßnahmen für den geordneten Regelbetrieb kann durch Prüfung der sachgerechten Umsetzung der Organisationsanweisungen und Einsichtnahme in die Aufzeich-

nungen der technischen Systeme zur Steuerung des Rechnerbetriebs beurteilt werden:

- Abgleich der Anweisungen zur Jobdokumentation mit den tatsächlichen Jobs
  - Prüfung der im RZ-Handbuch aufgeführten Protokolle, Jobs und Nachweise auf deren Existenz und angemessene Aufbewahrung
  - Durchsicht von Job- und Operatorprotokollen auf wiederkehrende Fehler.
- (65) Die Maßnahmen für den Notbetrieb ergänzen die Maßnahmen für den Regelbetrieb um organisatorische Regelungen und technische Verfahren zur Wiederherstellung der IT nach teilweisem oder vollständigem Ausfall der IT-Infrastruktur. Die Prüfungshandlungen zur Aufbauprüfung entsprechen denen des Regelbetriebs.

### 3.4.5. Sicherung der Betriebsbereitschaft

- (66) Maßnahmen zur Sicherheit der Betriebsbereitschaft umfassen den Einsatz einzelner Systemkomponenten und sogenannte Katastrophenfall-Szenarien. Die Maßnahmen sind Voraussetzung für die Sicherung der Verfügbarkeit der IT (vgl. *IDW ERS FAIT 1*, Tz. 23) sowie der Vollständigkeit und Nachvollziehbarkeit i.S.v. Prüfbarkeit über die Aufbewahrungsfrist der Daten (vgl. *IDW ERS FAIT 1*, Tz. 30).
- (67) Durch die Aufbauprüfung sind die Vorkehrungen gegen den Ausfall von IT dahingehend zu beurteilen, ob die unternehmensspezifischen Risiken und die Abhängigkeit des Unternehmens von der Funktionsfähigkeit der IT angemessen berücksichtigt worden sind. Die Gestaltung der organisatorischen Regelungen (Katastrophenfall-Handbuch) und der technischen Sicherungsmaßnahmen (z.B. redundante Auslegung der Hardware, vertragliche Backup-Vereinbarungen, Ausweich-Rechenzentrum) müssen mit hinreichender Sicherheit gewährleisten, daß der Zeitraum innerhalb dessen beim Eintritt eines Schadensfalls die Wiederherstellung der Programmfunktionen und Programmabläufe sichergestellt werden soll, nicht überschritten wird. Dabei ist insbesondere die Plausibilität der von der Unternehmensleitung festgelegten Schadensszenarien sowie ihre Auswirkungen auf den Fortbestand des Unternehmens anhand der Dokumentation der getroffenen Vorkehrungen kritisch zu würdigen.
- (68) Bei Unternehmen mit hoher Abhängigkeit von IT-Systemen (z.B. Finanzdienstleistungs- oder Telekommunikationsunternehmen) sind besondere Anforderungen an die Qualität der Risikovorsorge und den Detaillierungsgrad einer Notfallplanung zu stellen. Es ist zu untersuchen, ob und inwieweit die vom Unternehmen vorgesehenen Maßnahmen (Eventualplanungen) geeignet sind, einen Wiederanlauf der Funktionalität bei Ausfall einzelner Hardwarekomponenten oder die Wiederherstellung der Funktionalität nach Eintritt eines Katastrophenfalls innerhalb des von den gesetzlichen Vertretern vorgegebenen Zeithorizonts zu ermöglichen. Weiterhin ist zu prüfen, ob ge-

eignete Eskalationsverfahren organisiert und die Wirksamkeit der Wiederanlauf- und Notfallszenarien in regelmäßigen Tests verifiziert werden.

- (69) Bei der Prüfung der Funktionsfähigkeit und Wirksamkeit der Maßnahmen kann der Abschlußprüfer auf eigene Tests verzichten, soweit die erfolgreiche Durchführung von Tests anhand der Testdokumentation mit hinreichender Sicherheit beurteilt werden kann.

### **3.5. Prüfung der IT-Anwendungen**

- (70) Die Prüfung von IT-Anwendungen umfaßt die Erfüllung der verfahrensbezogenen Anforderungen der Grundsätze ordnungsmäßiger Buchführung, die Erfüllung der Anforderungen an die Softwaresicherheit sowie die Anforderungen an rechnungslegungsrelevante Verarbeitungsregeln (vgl. *IDW ERS FAIT 1*, Tz. 92 f.) Dazu sind neben anwendungsbezogenen IT-Kontrollen (Eingabe-, Verarbeitungs- und Ausgabekontrollen) generelle Kontrollen einzurichten, die sich auf den Auswahl- und Entwicklungsprozeß sowie die Implementierung von Software richten. Anwendungsbezogene Zugriffskontrollen müssen im Zusammenhang mit den übrigen logischen Zugriffskontrollen beurteilt werden.
- (71) Soweit die Unternehmensleitung Anforderungen an die Ausgestaltung einer IT-Anwendung aufstellt, sind diese nur Gegenstand der Abschlußprüfung, soweit sie zur Einhaltung der rechnungslegungsrelevanten Programmfunktionen und Programmabläufe von Bedeutung sind. Eine darüber hinausgehende Beurteilung kann nur Gegenstand einer gesonderten Beauftragung durch das Unternehmen sein.

#### **3.5.1. Programmfunktionen**

- (72) Ziel der Prüfung der Programmfunktionen ist die Beurteilung der Einhaltung der Grundsätze ordnungsmäßiger Buchführung im Rahmen der durch die Software vorgegebenen Verfahren (vgl. *IDW ERS FAIT 1*). Gegenstand, Art und Umfang der erforderlichen Prüfungshandlungen sowie der Berücksichtigung vorliegender Softwarebescheinigungen bei der Abschlußprüfung sind in *IDW PS 880 dargestellt*.
- (73) Die Beurteilung der richtigen Umsetzung und Wirksamkeit von Ordnungsmäßigkeits- und Sicherheitskriterien in IT-Anwendungen und der Angemessenheit der IT-Kontrollen ist Gegenstand von Programm- bzw. Softwareprüfungen. Eine Softwareprüfung i.S.d. *IDW PS 880* besteht aus der Beurteilung der Programmfunktionen, der Softwaresicherheit und der Dokumentation.
- (74) Die Prüfung der angemessenen und richtigen Umsetzung der von den gesetzlichen Vertretern an die IT-Anwendung gestellten Anforderungen an Funktionalität, Ordnungsmäßigkeit und Sicherheit im Rahmen der Aufbauprüfung setzt das Vorliegen einer vollständigen und aktuellen Verfahrensdokumentation voraus. Dazu müssen eine Anwenderdokumentation und eine

technische Systemdokumentation vorliegen, die sämtliche Bestandteile enthalten, die für die Nachvollziehbarkeit der IT-Anwendung erforderlich sind. Soweit technische Systemdokumentationen fehlen (i.d.R. bei Anwendungen von Standardsoftware) sind die Funktionstests des Abschlußprüfers so auszuweiten, daß mit hinreichender Sicherheit festgestellt werden kann, ob die Programmfunktionalitäten die Einhaltung der Grundsätze ordnungsmäßiger Buchführung gewährleisten.

- (75) Nachdem im Rahmen der Aufbauprüfung die Programmfunktionen als angemessen beurteilt werden, hängen die notwendigen Prüfungshandlungen zur Prüfung der Funktionsfähigkeit und Wirksamkeit der Programmfunktionen davon ab, ob dem Abschlußprüfer für Programmprüfungen ein Testsystem zur Verfügung gestellt wird.

In einem Testsystem können die Richtigkeit der Programmabläufe, die sachlogische Richtigkeit der programmierten Verarbeitungsregeln und die Wirksamkeit der im Programm enthaltenen IT-Kontrollen durch eigene Testfälle verifiziert werden.

Sofern kein Testsystem zur Verfügung steht, muß der Abschlußprüfer die Einhaltung der Aussagen zur Dokumentation auf andere Weise überprüfen, etwa durch Beobachtung von Eingaben und Nachvollziehen der erzielten Ergebnisse oder Parallelverarbeitung der Eingabedaten mit einem vom Abschlußprüfer erstellten Verarbeitungsalgorithmus.

- (76) Weitere Informationen, die bei Programmprüfungen berücksichtigt werden können, sind u.a. Fachkonzepte, Berichtsprotokolle, Revisionsberichte, Dokumentation der Anwender- und Integrationstests sowie Abnahmeprotokolle.

### **3.5.2. Auswahl-, Entwicklungs- und Änderungsprozeß**

- (77) Voraussetzung für die Ordnungsmäßigkeit und Sicherheit von IT-Anwendungen ist eine angemessene Organisation der Systementwicklung bzw. der Vorgehensweise bei der Auswahl von Standardsoftware. Ebenso sind Regelungen zur Änderung bzw. Erweiterung von IT-Anwendungen erforderlich.

- (78) Hierzu muß der Abschlußprüfer die Regelungen und Verfahren auf Angemessenheit beurteilen, die das Unternehmen

- zur Entwicklung von Individualsoftware,
- zur Auswahl, Beschaffung und Einführung von Standardsoftware,
- für Test- und Freigabeverfahren und
- zur Änderung von IT-Anwendungen (Change-Management) definiert hat (vgl. *IDW ERS FAIT 1*, Tz. 95).

- (79) Gegenstand der Aufbauprüfung der Anwendungsentwicklung und -pflege sind neben den Grob- und Feinkonzepten, in denen die Umsetzung der Anforderungen an Verarbeitungsfunktionen und Verarbeitungsregeln beschrieben sind,

- das Projektmanagement- und die Qualitätssicherung,

- die Richtlinien für Programmierung, Dokumentation, Test und Freigabe,
  - die adäquate Verwendung der Entwicklungstools und das Change- bzw. Versions-Management (vgl. *IDW ERS FAIT 1*, Tz. 97).
- (80) Organisatorische Regelungen müssen zur Auswahl, Entwicklung, Änderung, zum Test und zur Dokumentation von IT-Anwendungen bestehen. Aus ihrer Prüfung kann der Abschlußprüfer Rückschlüsse auf die Eignung der Software ziehen. Bei der Einführung einer Standardsoftware kann der Abschlußprüfer sich anhand der Durchsicht des Pflichtenheftes davon überzeugen, ob die hierfür geltenden rechtlichen und fachlichen Anforderungen berücksichtigt und die Sicherheit durch die IT-Anwendung gewährleistet ist.
- (81) Zur Prüfung der Wirksamkeit der Regelungen und Verfahren wird der Abschlußprüfer die im Rahmen von Auswahl-, Entwicklungs- und Änderungsprojekten erstellten Dokumentationsunterlagen sichten und die Einhaltung der Regelungen und Verfahren in Stichproben prüfen.

### **3.5.3. Implementierung**

- (82) Die Prüfung der Ordnungsmäßigkeit der Implementierung richtet sich auf die Regelungen und Maßnahmen für die Implementierung von rechnungslegungsrelevanter Software, einschließlich der zur Berücksichtigung unternehmensindividueller Besonderheiten vom Anwender vorgenommenen Anpassungen gegenüber einem vom Softwarehersteller definierten Standard. Gegenstand der Prüfung sind damit die zumeist in Tabellen hinterlegten Parameter, mit denen der Anwender bestimmte Verarbeitungsabläufe und -funktionen innerhalb der IT-Anwendung steuern kann. Beispiele sind unternehmensindividuelle Regeln für automatische Kontenfindungen und Buchungen, die Gestaltung von Bewertungsverfahren in der Materialwirtschaft, die Ausgestaltung des Zugriffsschutzsystems oder die Erstellung unternehmensindividueller Auswertungen. Der Abschlußprüfer muß im Rahmen einer Aufbauprüfung beurteilen, ob die spezifischen Anpassungen der IT-Anwendung ausreichend dokumentiert sind und die Einhaltung der Ordnungsmäßigkeits- und Sicherheitskriterien gewährleisten.
- (83) Zur Funktionsprüfung der Implementierung prüft der Abschlußprüfer durch Einzelfallprüfung, ob die in der Dokumentation beschriebenen Parametrisierungen (z.B. automatische Kontenfindung) auch tatsächlich bei der Abwicklung eines Geschäftsvorfalles wirksam werden. Diese Untersuchungen können auf Testfällen des Unternehmens, eigenen Testfällen oder auf der Grundlage konkreter Verarbeitungsergebnisse beruhen.
- (84) Die Übernahme sogenannter Altdaten (Stamm- oder Bewegungsdaten) aus den abgelösten Systemen ist auf Vollständigkeit und Richtigkeit zu prüfen. Insbesondere bei unterjährigen Systemwechseln sind geeignete Abstimm- und Kontrollauswertungen durch das Unternehmen zu erstellen und vom Abschlußprüfer zu untersuchen.

### 3.6. Prüfung IT-gestützter Geschäftsprozesse

- (85) Die Aufbauprüfung der zu untersuchenden Geschäftsprozesse umfaßt Prozeßaufnahmen, die dokumentieren
- in welchen Prozeßschritten IT-Anwendungen integriert sind und/oder manuelle Tätigkeiten ausgeführt werden,
  - wie rechnungslegungsrelevante Informationen aus dem Geschäftsprozeß in die Rechnungslegung übergeleitet werden (Daten-, Belegfluß, Schnittstellen) und
  - welche Anwendungs- und Prozeßkontrollen bei der Erfassung und Verarbeitung von Geschäftsvorfällen bestehen.
- (86) Anwendungsbezogene Kontrollen betreffen sowohl manuelle, in der Verantwortung der Fachbereiche liegende Kontrollen als auch maschinelle Kontrollen in IT-Anwendungen wie
- zutreffende Einstellung der Steuerungsparameter,
  - richtige Belegaufbereitung (z.B. sachliche und rechnerische Prüfung, Vorkontierung),
  - verlässliche Plausibilitätskontrollen bei der Belegerfassung,
  - wirksame Kontroll- und Abstimmverfahren zwischen Teilprozessen,
  - zeitnahe Bearbeitung von Fehlermeldungen und -protokollen.
- (87) Im Rahmen der Aufbauprüfung hat der Abschlußprüfer neben den anwendungsbezogenen Kontrollen insbesondere auch die Angemessenheit der im Geschäftsprozeß integrierten Kontrollen zu beurteilen, die die vollständige und richtige Verarbeitung über mehrere Prozeßschritte gewährleisten.
- (88) Durch Funktionsprüfungen muß die Wirksamkeit der IT-Kontrollen in IT-gestützten Geschäftsprozessen verifiziert werden. So ist zu prüfen, ob die Beurteilung der Angemessenheit und Wirksamkeit der Zugriffskontrollen auch auf der Geschäftsprozeßebene bestätigt werden kann.

### 3.7. Prüfung des IT-Überwachungssystems

- (89) Der Abschlußprüfer hat auch die wesentlichen auf die Überwachung des internen Kontrollsystems bezogenen Maßnahmen zu beurteilen und die Auswirkungen dieser Überwachungsmaßnahmen im Rahmen der Beurteilung der Kontrollrisiken zu berücksichtigen (vgl. *IDW ERS FAIT 1*, Tz. 108 ff.).
- (90) Hierzu zählen bspw.:
- die Prüfung des internen Kontrollsystems durch die Interne Revision (vgl. *IDW EPS 321*)
  - die Prüfung des internen Kontrollsystems durch einen anderen externen Prüfer i.S.v. *IDW EPS 320*
  - spontane Prüfungen einzelner Regelungen des internen Kontrollsystems durch andere Mitarbeiter des Unternehmens oder die Unternehmensleitung (High-level-Controls).

### 3rd8th Prüfung des IT-Outsourcing

- (91) Wenn ein Unternehmen IT-Systeme oder IT-gestützte betriebliche Funktionen ausgelagert, muß der Abschlußprüfer beurteilen, wie sich dies auf das Interne Kontrollsystem des Unternehmens auswirkt. Hierfür können u.a. die Art der erbrachten Dienstleistung, das Ausmaß des Zusammenspiels zwischen den internen Kontrollen des zu prüfenden Unternehmens und des Dienstleistungsunternehmens, die Art der Kontrollen, die das zu prüfende Unternehmen zur Überwachung der ausgelagerten Funktionen eingerichtet hat, die wirtschaftliche Lage des Dienstleistungsunternehmens und dessen Internes Kontrollsystem von Bedeutung sein. In diesen Fällen sind auch die im Dienstleistungsunternehmen eingerichteten organisatorischen Regelungen und die dort vorgehaltenen Aufzeichnungen für die Abschlußprüfung zu beurteilen.
- (92) Kommt der Abschlußprüfer zu dem Schluß, daß die Aktivitäten eines Dienstleistungsunternehmens eine wesentliche Auswirkung auf die Abschlußprüfung haben, hat er ausreichende Informationen einzuholen, um sich mit dem Internen Kontrollsystem dieses Unternehmens vertraut zu machen und um die Kontrollrisiken beurteilen zu können. Gegebenenfalls sollte der Abschlußprüfer versuchen, Informationen vom Abschlußprüfer des Dienstleistungsunternehmens zu erhalten und abwägen, ob Prüfungshandlungen vor Ort im Dienstleistungsunternehmen durchzuführen sind.
- (93) Sofern ein Unternehmen das Rechnungswesen ganz oder teilweise ausgelagert hat (Buchführung außer Haus, Shared Services) muß der Abschlußprüfer sich von der Erfüllung der Anforderungen an die Ordnungsmäßigkeit durch das Serviceunternehmen, welches das Rechnungswesen für das zu prüfende Unternehmen führt, überzeugen. Für den Abschlußprüfer ist dabei die Art und Ausgestaltung der Auslagerung rechnungslegungsrelevanter Teile des IT-Systems von Bedeutung.
- (94) Für diese Beurteilung kann der Abschlußprüfer auch Prüfungsergebnisse des Abschlußprüfers des Dienstleistungsunternehmens oder Sachverständiger heranziehen, die sich auf die Qualität des internen Kontrollsystems des Dienstleistungsunternehmens beziehen. Beabsichtigt der Abschlußprüfer die Verwertung von Prüfungsergebnissen eines anderen externen Prüfers oder Sachverständigen, sind *IDW EPS 320* oder *IDW EPS 322* anzuwenden.

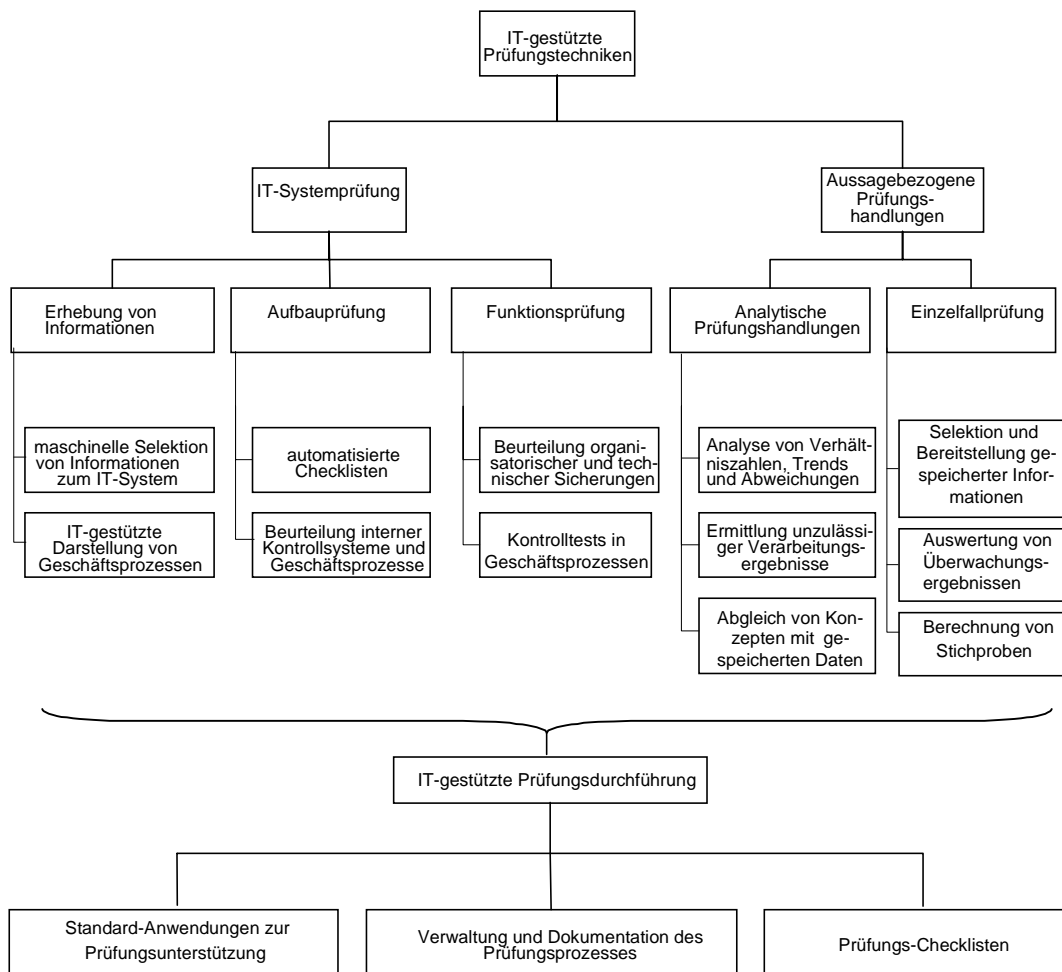
### 4. IT-gestützte Prüfungstechniken

- (95) Die Verwendung IT-gestützter Prüfungstechniken (Computer-Assisted Audit Techniques, CAAT) kann die Wirksamkeit und Wirtschaftlichkeit der Prüfung wesentlich erhöhen. Der Einsatz von CAAT für Aufbau- und Funktionsprüfungen ist insbesondere in den Fällen empfehlenswert, in denen nur Belege in elektronischer Form übermittelt, generiert und gespeichert werden oder eine sehr große Zahl von Geschäftsvorfällen vorliegt.

- (96) Die Entscheidung über Art und Umfang IT-gestützter Prüfungshandlungen ist im Rahmen der risikoorientierten Prüfungsplanung unter Berücksichtigung der Ausgestaltung des IT-Systems und der zugrundeliegenden unternehmensspezifischen Gegebenheiten festzulegen. Dabei sind die folgenden Faktoren zu berücksichtigen:
- fehlende konventionelle Prüfungsmöglichkeit durch fehlende Ausgabemöglichkeiten im gewünschten Datenformat
  - Verfügbarkeit IT-gestützter Prüfungstechniken (Software), der erforderlichen IT-Infrastruktur und der zu prüfenden produktiven Daten sowie von Testdaten im erforderlichen Format
  - Kenntnisstand und Erfahrung des Prüfers
  - Vorhandensein prüfungsrelevanter Informationen in maschinell lesbarem Format
  - zeitliche Verfügbarkeit der zu prüfenden Systeme und Daten
  - Möglichkeit der Verwendung des IT-Systems des Mandanten für Prüfungszwecke.

#### **4.1. Einsatzbereiche**

- (97) IT-gestützte Prüfungstechniken können zur Unterstützung des gesamten Prüfungsprozesses eingesetzt werden.



#### 4.1.1. Einsatz im Rahmen der IT-Systemprüfung

- (98) Zur IT-gestützten Erhebung von Informationen über das IT-System kann der Abschlußprüfer auf Inventarisierungs- und Überwachungsprogramme des Unternehmens zurückgreifen, die neben Informationen über die Hardwarekomponenten auch Auskunft über installierte IT-Programme geben. Sofern Geschäftsprozesse durch den Abschlußprüfer dokumentiert werden, stehen hierfür Programme zur Visualisierung von Geschäftsprozessen und Kontrollschritten (nach DIN- und ISO-Normen) zur Verfügung.
- (99) Bei der Aufbauprüfung werden z.B. automatisierte Checklisten zur Prüfungsdurchführung oder durch Expertensysteme unterstützte Anwendungen zur Dokumentation und Beurteilung interner Kontrollsysteme und Geschäftsprozesse genutzt.

Funktionsprüfungen werden durch Programme zur Beurteilung der Wirksamkeit technischer und organisatorischer Sicherungsmaßnahmen etwa bei der Prüfung der Konfiguration von Betriebssystemen oder zur Beurteilung von Zugriffsrechten auf Programmbibliotheken unterstützt. Zu den Werkzeugen

zur Prüfung der Wirksamkeit von in Geschäftsprozessen eingebauten Kontrollen zählen u.a. die programmgesteuerte Generierung von Testfällen zur Prüfung der Eingabe-, Verarbeitungs- und Ausgabekontrollen.

#### 4.1.2. Aussagebezogene Prüfungshandlungen

(100) Analytische Prüfungshandlungen können mittels IT-gestützter Prüfungstechniken z.B. in den folgenden Bereichen unterstützt werden:

- bei der risikoorientierten sachlichen Prüfungsplanung, beispielsweise durch Ermittlung kennzahlengestützter Bonitätsindices bei der Auswahl von Prüfungsschwerpunkten und der Beurteilung von inhärenten Risiken
- bei der Ermittlung und Analyse von Verhältniszahlen und Trends, durch die die Beziehungen von maschinell verfügbaren prüfungsrelevanten Daten eines Unternehmens zu anderen Daten aufgezeigt werden (vgl. *IDW Prüfungsstandard: Prüfungsnachweise im Rahmen der Abschlußprüfung (IDW PS 300)*<sup>16</sup>, Tz. 22)
- bei der Ermittlung und Analyse auffälliger Abweichungen durch Vergleich gespeicherter Sollwerte mit der korrespondierenden Entwicklung von Ist-daten
- Selektion und Auswertung von Schwankungen oder Zusammenhängen, die in Widerspruch zu anderen einschlägigen Informationen stehen oder von erwarteten Beträgen abweichen (vgl. *IDW Prüfungsstandard: Analytische Prüfungshandlungen (IDW PS 312)*<sup>17</sup>, Tz. 5 ff.)

(101) Einzelfallprüfungen werden insbesondere in den folgenden Fällen durch IT-gestützte Prüfungstechniken unterstützt (vgl. *IDW PS 300*, Tz. 26):

- Selektion und Bereitstellung maschinell hinterlegter Informationen als Basis für die strukturierte Einsichtnahme in Unterlagen des Unternehmens
- Auswertung gespeicherter Protokollierungs- oder Überwachungsergebnisse
- maschinelle Berechnung von Stichprobenumfängen oder Ermittlung der bei der Durchführung unmittelbarer Soll-Ist-Vergleiche einzelner Geschäftsvorfälle und Bestände heranzuziehenden Sollergebnisse.

#### 4.2. IT-gestützte Prüfungsdurchführung

(102) IT-Unterstützung kann auch im Rahmen der Prüfungsdurchführung sinnvoll sein, um wiederkehrende Arbeiten im Rahmen der Abschlußprüfung zu automatisieren. Dies ist u.a. der Fall:

- bei der zeitlichen Prüfungsplanung, z.B. mit Hilfe von Projektplanungs-Anwendungen

---

<sup>16</sup> WPg 2001, S. ■

<sup>17</sup> WPg 2001, S. ■

- beim Einsatz von Standard-Anwendungen zur Prüfungsunterstützung, z.B. mit Hilfe von Tabellenkalkulationsprogrammen
- bei der Dokumentation von Strukturen und Abläufen, z.B. mittels Flow Charting-Software oder Präsentationsprogrammen
- bei der prüfungsbegleitenden Verwaltung und Dokumentation des Prüfungsprozesses, z.B. integrierte Checklisten-, Referenzierungs- und Arbeitspapierverwaltungswerkzeuge.

#### **4.3. Verwendung des IT-Systems des Unternehmens für Prüfungszwecke**

- (103) Neben dem Einsatz eigener Programme auf der Hardware des Abschlußprüfers kann auch die Verwendung des IT-Systems des Mandanten für *Prüfungszwecke* geboten sein.
- (104) Der Abschlußprüfer kann auf der Hardware des Unternehmens installierte Programme mitnutzen. Im wesentlichen sind die folgenden Einsatzmöglichkeiten für Prüfungszwecke denkbar:
- Nutzung allgemeiner Dienstprogramme (Utilities) sowie spezifischer Datensелеktions- und -aufbereitungsprogramme
  - Erstellung und Ausführung spezieller Auswertungen
  - Verwendung von in IT-Anwendungen eingebetteten Prüfungswerkzeugen und Prüfungsschnittstellen (z.B. sog. Embedded Audit-Routines)
  - Nutzung eingebetteter Funktionen zur kontinuierlichen Verarbeitung von Testfällen (Integrated Test Facility).
- (105) Ferner kann der Abschlußprüfer eigene Programme auf das IT-System des Unternehmens laden und dort einsetzen. Hierbei ist sicherzustellen, daß die notwendigen Einsatzvoraussetzungen gegeben sind und gewährleistet ist, daß Veränderungen an den für Prüfungszwecke eingesetzten Programmen durch das Unternehmen ausgeschlossen sind. Daher hat der Abschlußprüfer durch geeignete Maßnahmen insbesondere sicherzustellen, daß
- die technischen Voraussetzungen für den Einsatz der Prüfprogramme gegeben sind und diese vor der Installation überprüft werden,
  - die Bereiche des IT-Kontrollsystems, die die Integrität der eingesetzten Prüfprogramme gewährleisten, angemessen und wirksam sind,
  - die eingesetzten Prüfprogramme hinsichtlich ihrer Sicherheit und Ordnungsmäßigkeit der Verarbeitungsergebnisse getestet werden,
  - die Prüfprogramme richtig und vollständig auf dem IT-System des Unternehmens installiert wurden,
  - nach erfolgreicher Installation durch Testläufe die Richtigkeit und Vollständigkeit der Installation sowie die korrekte Funktionsweise des Programms überprüft werden, bevor auf Unternehmensdaten zugegriffen wird,
  - der Zugriff auf Unternehmensdaten ordnungsgemäß erfolgt,

- die Sicherheit der Unternehmensdaten durch den Einsatz IT-gestützter Prüfungstechniken nicht beeinträchtigt sowie
  - bei der Installation der Prüfprogramme durch Mitarbeiter der Fachabteilung des Unternehmens die Testergebnisse nicht beeinflusst werden.
- (106) Soweit Testdatensätze zur Prüfung der Verarbeitungsergebnisse von IT-Anwendungen eingesetzt werden, ist weiterhin sicherzustellen, daß
- die Übertragung von Testdatensätzen in das IT-System des Mandanten überwacht wird, insbesondere wenn die Testdatensätze zur Prüfung mehrerer IT-Geschäftsprozesse eingesetzt werden,
  - Testläufe durchgeführt werden, bevor die Testdaten in produktiv eingesetzte IT-Anwendungen eingesetzt werden,
  - die getesteten Versionen der IT-Anwendungen auch während des gesamten Prüfungszeitraums eingesetzt bzw. andere Versionen im entsprechenden Zeitraum durch ggf. angepaßte Testdatensätze geprüft wurden.

#### **4.4. Besonderheiten bei Einsatz IT-gestützter Prüfungstechniken**

- (107) Besonderheiten bei der Planung und Durchführung des Einsatzes IT-gestützter Prüfungstechniken ergeben sich in den folgenden Bereichen:
- Festlegung der Ziele sowie von Art und Umfang IT-gestützter Prüfungshandlungen im Rahmen einer Prüfungsstrategie
  - Darstellung des Inhalts und der Zugriffsmöglichkeit auf die zu prüfenden Daten
  - Identifikation der zu prüfenden Dateien und/oder Datenbanktabellen
  - Auswahl der Prüfungsroutinen und der zu prüfenden Geschäftsvorfälle bzw. Datensätze
  - Festlegung der Ausgabeformate
  - Gewährleistung der zur Prüfung erforderlichen IT-Infrastruktur.
- (108) Die Prüfungsdurchführung und die Ableitung der Prüfungsergebnisse ist zu überwachen. Hierzu gehört insbesondere:
- Mitwirkung bei Entwicklung und Test der zur Prüfung eingesetzten Programme
  - Verifizierung ausgewählter Bereiche des entwickelten Programmcodes (z.B. Ausschlußbedingungen bei der Datenselektion)
  - Überwachung der Verfügbarkeit der benötigten Daten
  - gesonderte Überwachung des systemtechnischen Umfelds zur Sicherstellung der zur Prüfung erforderlichen Systemumgebung sowie zur Verhinderung einer Veränderung der Systemumgebung durch Dritte (z.B. durch Kontrolle des Versionsstandes von Dateien)
  - Test der entwickelten Prüfungsanwendung mit kleinen Testdatenvolumina vor dem Einsatz mit umfassenden Datenbeständen.

## 5. Dokumentation und Berichterstattung

- (109) Der Abschlußprüfer hat die gewonnenen Kenntnisse über das IT-System sowie die dazu vorgenommenen Prüfungshandlungen aus Aufbau- und Funktionsprüfungen angemessen in den Arbeitspapieren und im Prüfungsbericht zu dokumentieren (vgl. *IDW Prüfungsstandard: Arbeitspapiere des Abschlußprüfers (IDW PS 460)*<sup>18</sup>).
- (110) Art und Umfang der Dokumentation sind abhängig von der Ausgestaltung des IT-Systems. Je komplexer das IT-System ausgestaltet ist und je umfassender die Prüfungshandlungen des Abschlußprüfers sind, desto detaillierter hat der Abschlußprüfer den Aufbau des IT-Systems und die Prüfungshandlungen zu dokumentieren.
- (111) Führen die festgestellten Schwächen des IT-Systems zu wesentlichen Mängeln in der Rechnungslegung, ist der Bestätigungsvermerk einzuschränken oder ggf. zu versagen (vgl. *IDW PS 400*, Tz. 50 ff. und Tz. 65 ff.).
- (112) Im Prüfungsbericht ist zur Ordnungsmäßigkeit der Buchführung Stellung zu nehmen (vgl. *IDW PS 450*, Tz. 60 ff.).
- (113) Bei der Darstellung im Prüfungsbericht von festgestellten Mängeln in den nicht auf die Rechnungslegung bezogenen Bereichen des IT-Systems empfiehlt sich der ausdrückliche Hinweis, daß der Abschlußprüfer Systemschwächen zwar als Ergebnis seiner Prüfungshandlungen entdeckt hat, die Prüfung aber nicht darauf ausgerichtet ist, die Wirksamkeit des IT-Systems für Geschäftsführungszwecke zu beurteilen (vgl. *IDW PS 450*, Tz. 63).
- (114) Stellt der Abschlußprüfer im Rahmen seiner Prüfungshandlungen wesentliche Schwächen des IT-Systems fest, ist die Unternehmensleitung rechtzeitig und in geeigneter Form auf diese aufmerksam zu machen (vgl. *IDW PS 450*, Tz. 41 ff.).
- (115) Über anlässlich der IT-Systemprüfung festgestellte Optimierungspotentiale des geprüften IT-Systems empfiehlt es sich, den Auftraggeber und/oder die gesetzlichen Vertreter – unbeschadet der Darstellung im Prüfungsbericht – zeitnah und in geeigneter Form (z.B. Management Letter) zu informieren.

Die Prüfungsfeststellungen der durchgeführten IT-Systemprüfungen finden Eingang in die Prüfungsaussagen des Abschlußprüfers über die Rechnungslegung des Unternehmens.

## 6. Übereinstimmung mit ISA

- (116) Der vorliegende *IDW EPS 330* geht über den bestehenden ISA 401 hinaus. Der überarbeitete Entwurf eines International Auditing Standard (ISA) 401 „Auditing in a Computer Information Systems Environment“ ist zur Zeit noch in der Diskussion.

---

<sup>18</sup> WPg 2000, S. 916 ff.