Fachgutachten

des **Fachsenats für Datenverarbeitung** der **Kammer der Wirtschaftstreuhänder** über die

Prüfung der Informationstechnik im Rahmen der Abschlussprüfung

(Auf Prüfungen von Abschlüssen für Geschäftsjahre, die am oder nach dem 30. Juni 2017 enden, anzuwenden. Eine frühere Anwendung ist zulässig.)

(beschlossen in der Sitzung des Fachsenats für Datenverarbeitung am 23. Februar 2017 als Fachgutachten KFS/DV 2; von der Abschlussprüferaufsichtsbehörde (APAB) genehmigt)

Inhaltsverzeichnis Seite

1. Einleitung

1.1. Anwendungsbereich des Fachgutachtens

(1) Dieses Fachgutachten ersetzt das Fachgutachten KFS/DV 2 in der Fassung vom 22. Juni 2004. Der Fachsenat legt darin die Berufsauffassung dar, wie Abschlussprüfer – unbeschadet ihrer Eigenverantwortung – bei der Prüfung der Informationstechnik (IT) im Rahmen von Abschlussprüfungen vorzugehen haben. Aufgrund der großen Bedeutung der IT in zahlreichen, insbesondere in rechnungslegungsrelevanten Unternehmensbereichen, ist deren Prüfung ein wichtiger Bestandteil der Abschlussprüfungen.

(2) Dieses Fachgutachten konkretisiert das Fachgutachten zur Durchführung von Abschlussprüfungen KFS/PG 1 und die International Standards on Auditing / ISA 315 und 330 sowie die daraus resultierenden Anforderungen an die Abschlussprüfung bei Einsatz von IT durch das zu prüfende Unternehmen. Bezüglich der Anforderungen an die IT-gestützte Führung von Büchern wird auf § 190 UGB und das Fachgutachten zur Ordnungsmäßigkeit von IT-Buchführungen KFS/DV 1 verwiesen.

(3) Auf Besonderheiten und zusätzliche Anforderungen aufgrund von sondergesetzlichen Vorschriften (z.B. aufsichtsrechtliche Vorschriften des Bankwesengesetzes) wird in diesem Fachgutachten nicht eingegangen.

1.2. Ziel der Prüfung der IT und Einbindung in die Abschlussprüfung

(4) Setzt ein Unternehmen IT ein, bestehen die Ziele des Abschlussprüfers darin,

a) ein Verständnis darüber zu erlangen, inwiefern mittels dieser IT rechnungslegungsbezogene Informationen verarbeitet und/oder rechnungslegungsrelevante Prozesse unterstützt werden und diese Teil des für den Abschlussprüfer relevanten internen Kontrollsystems sind (ISA 315, Rz 21; A103-A105) und dann
b) gegebenenfalls festzustellen, welche Risiken wesentlicher falscher Angaben in der Rechnungslegung daraus resultieren, um durch deren Beurteilung eine Grundlage für die Planung und Umsetzung von Reaktionen auf diese Risiken zu schaffen (ISA 315, Rz 3).

(5) Daneben ist es für den Abschlussprüfer von Relevanz

a) festzustellen, ob rechnungslegungsrelevante Systeme den gesetzlichen Anforderungen entsprechen, um die nach § 269 Abs. 1 und 3 UGB i.V.m. den in § 273 UGB geforderten Aussagen über die Gesetzmäßigkeit der Buchführung treffen zu können, sowie
b) festzustellen, ob die Darstellung der aus dem Einsatz der IT resultierenden Risiken im Lagebericht bzw. Konzernlagebericht, insbesondere hinsichtlich der Gefährdung des Fortbestands, zutreffend ist, um die geforderten Aussagen gemäß § 273 (Abs. 1 und 2) UGB treffen zu können.

2. Tätigkeiten des Abschlussprüfers bei der Prüfung der IT

2.1. Berücksichtigung der Prüfung der IT bei der Prüfungsplanung

(6) Die Planung hat zeitlich, sachlich und personell zu erfolgen und ist im Zuge der Prüfung bei Bedarf zu aktualisieren. Bei der personellen Planung ist – in Abhängigkeit

von Art und Umfang der weiteren IT-bezogenen Prüfungshandlungen – auf die Einbindung von entsprechend qualifizierten Mitarbeitern (IT-Prüfern) oder geeigneten externen Experten (ISA 620, Rz 7) zu achten. Bei der zeitlichen Planung ist darauf zu achten, dass die IT-Prüfer frühzeitig in die Prüfung eingebunden werden und ausreichend Zeit für die Durchführung der Prüfungshandlungen zur Verfügung steht.

2.2. Gewinnung eines Überblicks über die IT des geprüften Unternehmens

(7) Im Hinblick auf die unter Abschnitt 1.2. angeführten Ziele hat sich der Abschlussprüfer einen Überblick über die IT und auf diese sich auswirkenden Elemente des internen Kontrollsystems zu verschaffen (ISA 315, Rz 18; A89-A93).

(8) Die Elemente des internen Kontrollsystems umfassen in diesem Zusammenhang:

a) das IT-Kontrollumfeld, die IT-Organisation inklusive gegebenenfalls vorhandener, prüfungsrelevanter Auslagerungen („Outsourcing“)
b) den Risikobeurteilungsprozess hinsichtlich eingesetzter IT (ISA 315, Rz 15-16; A87)
c) die im Unternehmen eingesetzten, prüfungsrelevanten IT-Systeme und Anwendungen sowie die in diesen Anwendungen abgebildeten Informationsflüsse
d) diesbezügliche generelle IT-Kontrollen und Anwendungskontrollen
e) IT-bezogene Überwachungsmaßnahmen, wie z.B. jene der internen Revision

2.3. Identifikation der wesentlichen aus dem Einsatz und der Anwendung der IT resultierenden Risiken

(9) Der Abschlussprüfer hat auf Basis des gewonnen Überblicks die für die Prüfung relevanten Risiken festzustellen (ISA 315, Rz 5; A1-A5). Diese umfassen beispielsweise bezüglich:

a) wesentlicher falscher Angaben in der Rechnungslegung oder mangelnder Ordnungsmäßigkeit der Buchführung:
   – fehlerhafte oder unvollständige Datenverarbeitung (z.B. in Form von falschen Berechnungen oder erwarteter jedoch nicht vorhandener Funktionalität)
   – Dateninkonsistenz
   – unautorisierte Änderungen von Daten und Programmen
   – fehlende Nachvollziehbarkeit der Geschäftsfälle
b) der Gefährdung des Fortbestands des Unternehmens:
   – weitreichender Datenverlust
   – Nichtverfügbarkeit von geschäftskritischen IT-Systemen

(10) Im Hinblick auf die weiteren Prüfungshandlungen kann eine Zuordnung der Risiken zu den eingesetzten IT-Systemen und Anwendungen sinnvoll sein.

2.4. Identifikation der Maßnahmen des geprüften Unternehmens zur Adressierung der Risiken

(11) Die Unternehmen haben durch geeignete Kontrollen dafür zu sorgen, dass oben angeführte Risiken verhindert oder angemessen vermindert werden (ISA 315, Rz 12; A49-A72).

(12) Es wird dabei zwischen Anwendungskontrollen und generellen IT-Kontrollen unterschieden.

(13) Anwendungskontrollen sind jene, durch welche die Richtigkeit der Verarbeitungsergebnisse unmittelbar sichergestellt werden sollen. Dazu gehören jedenfalls Kontrollen, die im Source Code der Anwendungen enthalten sind, sowie durch Parameter gesteuerte Kontrollen. Anwendungskontrollen können wiederum in Eingabe-, Verarbeitungs- und Ausgabekontrollen untergliedert werden. Beispiele dazu sind in KFS/DV 1, Rz 68 angeführt (siehe auch ISA 315, A105).

(14) Generelle (manuell oder automatisiert ausgestaltete) IT-Kontrollen können den einzelnen IT-Prozessen zugeordnet werden (siehe KFS/DV 1, Rz 61 ff.), wie insbesondere:

a) der Beschaffung, Entwicklung und Pflege von Systemen;
b) dem Zugriffsschutz;
c) dem Betrieb.
(ISA 315, A104)

2.5. Vorgehensweise zur Festlegung und Prüfung der einzubeziehenden IT-Kontrollen

(15) Der Abschlussprüfer hat jene Anwendungskontrollen und generellen IT-Kontrollen zu identifizieren, die in Abhängigkeit der gewählten Prüfungsstrategie geeignet scheinen, ausreichende Prüfungssicherheit hinsichtlich der in Abschnitt 1.2. angeführten Prüfziele zu ermöglichen (ISA 315, Rz 14; A76-A86).

(16) Bei Vorhandensein hoch automatisierter rechnungslegungsrelevanter Prozesse, im Rahmen derer, mit geringer oder ohne manueller Interaktion, eine große Anzahl an Transaktionen verarbeitet werden (z.B. automatisch verbuchte Transaktionen der Warenwirtschaft, des Zahlungsverkehrs, des Online-Handels), ist regelmäßig zu erwarten, dass Anwendungskontrollen in die Prüfung einzubeziehen sind.

(17) Verwendet der Abschlussprüfer Auswertungen oder andere Informationen, die durch das geprüfte Unternehmen erzeugt werden (Information Produced by the Entity, „IPE"), als Prüfungsnachweise, dann hat er deren Verlässlichkeit (das heißt Vollständigkeit und Richtigkeit) zu beurteilen. Dies gilt gleichermaßen für jene IPE, die das Unternehmen selbst bei der Durchführung von Kontrollen verwendet, wenn sich der Abschlussprüfer auf eine solche Kontrolle verlassen will. Eine solche Beurteilung der Verlässlichkeit wird oft für die Erzeugung der Information relevante Anwendungskontrollen und für diese wesentliche generelle IT-Kontrollen umfassen (ISA 315, A70; ISA 500, Rz 9, 49-51).

(18) Die dauerhafte Wirksamkeit der Anwendungskontrollen hängt auch von der Wirksamkeit der generellen IT-Kontrollen ab, da diese sicherstellen, dass Anwendungskontrollen nicht umgangen, außer Kraft gesetzt oder unbeabsichtigt verändert werden. Daher sind solche generellen IT-Kontrollen zusätzlich in die Prüfung einzuplanen.

(19) Durch die Konsistenz der Verarbeitung, die IT-Systemen inhärent ist, ist ein zeitpunktbezogener Funktionstest („Test of Design and Implementation") – bei Vorhandensein wirksamer genereller IT-Kontrollen – regelmäßig ausreichend, um die Wirksamkeit von Anwendungskontrollen festzustellen (ISA 330, A31; ISA 315, A75).

(20) Bei Identifikation von unwirksamen allgemeinen IT-Kontrollen hat der Abschlussprüfer die Auswirkungen auf die dauerhafte Wirksamkeit sämtlicher betroffener, prüfungsrelevanter Anwendungskontrollen sowie auf die Verlässlichkeit von durch das Unternehmen erstellten, prüfungsrelevanten Informationen zu beurteilen.

(21) Bei unwirksamen allgemeinen IT-Kontrollen oder unwirksamen Anwendungskontrollen kann der Abschlussprüfer häufig Prüfsicherheit durch das Testen kompensierender Kontrollen, andernfalls durch zusätzliche Prüfungshandlungen erlangen.

2.6. Outsourcing

(22) Die Beurteilung der Prüfungsrelevanz von und das Vorgehen des Abschlussprüfers bei prüfungsrelevanten Auslagerungen ist in ISA 402 beschrieben.