**Fachgutachten**

des **Fachsenats für IT** der **Kammer der Steuerberater und Wirtschaftsprüfer** über die

# Prüfung der Informationstechnik im Rahmen der Abschlussprüfung

*(beschlossen in der Sitzung des Fachsenats für IT am 05. September 2022 als Neufassung des Fachgutachtens 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 23. Februar 2017. Der Fachsenat legt darin die Berufsauffassung dar, wie Abschlussprüfer auf Basis ISA 315[1] – unbeschadet ihrer Eigenverantwortung – bei der Prüfung der Informationstechnik (IT[2]) im Rahmen von Abschlussprüfungen vorzugehen haben. Aufgrund der großen Bedeutung der IT in zahlreichen, insbesondere in rechnungslegungsrelevanten Unternehmensbereichen, ist deren Prüfung ein wichtiger und in der Regel integrierter Bestandteil von Abschlussprüfungen.

(2) Dieses Fachgutachten konkretisiert das Fachgutachten zur Durchführung von Abschlussprüfungen KFS/PG 1 und die International Standards on Auditing / ISA 315 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 daher Teil des für den Abschlussprüfer relevanten internen Kontrollsystems ist (ISA 315, Tz25; A140-A143; Tz 26; A166-A174 und Appendix 5), um dann
b) festzustellen, inwiefern gegebenenfalls IT bezogene Risiken (ISA 315, Tz 12 (i)) die Integrität der Informationsverarbeitung beeinträchtigen und zu wesentlichen falschen Darstellungen in der Rechnungslegung führen können, und um anschließend
c) durch deren Beurteilung eine Grundlage für die Planung und Durchführung von Prüfungshandlungen als Reaktion auf diese Risiken zu schaffen (ISA 315, Tz 8).

(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 Abs. 1 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.

---

1 Bezugnahmen auf ISA 315 in diesem Fachgutachten betreffen ISA 315 (Revised 2019).
2 Informationstechnik wird im allgemeinen Sprachgebrauch häufig „Informationstechnologie“ genannt.

# 2. Tätigkeiten des Abschlussprüfers bei der Prüfung der IT

## 2.1. Berücksichtigung der Prüfung der IT bei der Prüfungsplanung

(6) Die Planung hat in zeitlicher, sachlicher und personeller Hinsicht 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; ISA 315, Tz A171) oder geeigneten externen Experten (ISA 620, Tz 7) zu achten. Bei der zeitlichen Planung ist zu berücksichtigen, dass die IT-Prüfer bzw die externen Experten bereits frühzeitig in der Prüfungsplanung 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

a) über die Rolle der IT im Geschäftsmodell des Unternehmens (ISA 315, Tz 19 (a) (i)) und
b) über die IT bezogenen Elemente des internen Kontrollsystems (ISA 315, Tz 25, Appendix 5), insbesondere
   - die rechnungslegungsrelevanten Datenflüsse in der IT und diesbezüglichen (automatischen) Kontrollen der Informationsverarbeitung (ISA 315, Tz 12 (e) sowie
   - die IT-Umgebung: Anwendungen, Infrastruktur und Prozesse und diesbezüglichen generellen IT-Kontrollen (ISA 315, Tz 12 (g)),

zu verschaffen.

(8) Dabei ist das Vorhandensein prüfungsrelevanter Auslagerungen inklusive der Nutzung von Cloud-Diensten zu berücksichtigen. Die Beurteilung der Prüfungsrelevanz von und das Vorgehen des Abschlussprüfers bei prüfungsrelevanten Auslagerungen ist in ISA 402 beschrieben.

(9) Aufgrund des erlangten Verständnisses kann die Komplexität des Einsatzes von IT eingeschätzt werden. (ISA 315, Appendix 5, Tz 4-7)

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

(10) Der Abschlussprüfer hat auf Basis des gewonnenen Überblicks ein Verständnis der für die Prüfung relevanten Risiken hinsichtlich wesentlicher falscher Angaben in der Rechnungslegung oder mangelnder Ordnungsmäßigkeit der Buchführung bzw. der Gefährdung des Fortbestands des Unternehmens zu erlangen.

(11) Aus dem Einsatz und der Anwendung der IT sind folgende Risiken beispielhaft:

a) betreffend die Informationsverarbeitung:
   - fehlerhafte oder unvollständige Datenverarbeitung (z.B. in Form von falschen Berechnungen oder erwarteter, jedoch nicht vorhandener Funktionalität)
   - Dateninkonsistenz
   - fehlende Nachvollziehbarkeit der Geschäftsfälle
b) betreffend das IT-Umfeld (ISA 315, Appendix 5, Tz 18):

- zu weitreichende Zugriffsrechte
- unautorisierte Änderung von Programmen
- Datenverlust
- Nichtverfügbarkeit von geschäftskritischen IT-Systemen

(12) Oben angeführte Risiken können auch aufgrund von Cyber-Sicherheitsvorfällen schlagend werden; bei Kenntnis solcher sind allfällige Auswirkungen auf die Abschlussprüfung zu beurteilen (ISA 315, Appendix 5 Tz 19).

(13) Im Hinblick auf die weiteren Prüfungshandlungen hat eine Zuordnung der prüfungsrelevanten Risiken zu den eingesetzten IT-Systemen und Anwendungen zu erfolgen; darüber hinaus hilft die Berücksichtigung der eingeschätzten, jeweiligen Komplexität bei Festlegung von Art, zeitlicher Einteilung und Umfang der weiteren Prüfungshandlungen.

(14) Falls der Abschlussprüfer feststellt, dass das Management des geprüften Unternehmens Risiken einer wesentlichen falschen Darstellung in der Rechnungslegung nicht identifiziert, hat er die Ursache dafür zu ermitteln und die Auswirkungen auf die Angemessenheit des Risikobeurteilungsprozesses des Unternehmens zu berücksichtigen (ISA 315, Tz 23).

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

(15) Es liegt in der Verantwortung der geprüften Unternehmen, durch geeignete Kontrollen (ISA 315, Tz 26 (b), Tz 26 (c); A166-A174) dafür zu sorgen, dass die unter 2.3. angeführte Risiken angemessen adressiert werden.

(16) Es wird bei diesen Kontrollen zwischen manuellen bzw automatischen Kontrollen der Informationsverarbeitung („Information Processing Controls“) einerseits und generellen IT-Kontrollen („General Information Technology Controls“) andererseits unterschieden (ISA 315, Tz 12 (d), Tz 12 (e); A6). In der Folge wird auf manuelle Kontrollen der Informationsverarbeitung nicht weiter eingegangen.

(17) Automatische Kontrollen der Informationsverarbeitung sind jene, durch welche die Integrität, das sind insbesondere die Vollständigkeit, Richtigkeit und Gültigkeit von Transaktionen und Verarbeitungsergebnissen, unmittelbar in den IT-Anwendungen sichergestellt werden soll (ISA 315, Tz 12 (e)). Dazu gehören insbesondere Kontrollen, die im Quellcode („Source Code“) der Anwendungen enthalten sind, sowie durch Parameter gesteuerte Kontrollen. Automatische Kontrollen der Informationsverarbeitung können in Eingabe-, Verarbeitungs- bzw automatische Berechnungs- und Ausgabekontrollen untergliedert werden. Beispiele dazu sind in KFS/DV 1, Rz 68, angeführt (siehe auch ISA 315, Appendix 5, Tz 8).

(18) Generelle IT-Kontrollen unterstützen die dauerhafte Wirksamkeit von Kontrollen der Informationsverarbeitung sowie das angemessene Funktionieren der IT-Umgebung (ISA 315, Tz 12 (d), siehe auch KFS/DV 1, Rz 61 ff.); diese können automatisch oder manuell ausgestaltet sein.

(19) Generelle IT-Kontrollen können auf verschiedenen Bestandteilen der IT-Umgebung, wie zB Anwendungen oder Infrastruktur (Datenbank, Betriebssystem und Netzwerk) eingerichtet und je nach Komplexität des Einsatzes von IT unterschiedlich ausgestaltet sein (ISA 315, Tz 12 (g); Appendix 5, Tz 16-17; Appendix 6, Tz 1). Im Rahmen der

Abschlussprüfung sind typischerweise generelle IT-Kontrollen folgender IT-Prozesse relevant:

a) Verwaltung des Zugriffsschutzes;
b) Beschaffung, Entwicklung und Pflege von Systemen;
c) Betrieb.

(ISA 315, Appendix 6, Tz 2)

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

(20) Bei hoher Komplexität der IT-Umgebung, wie zB Vorhandensein hochgradig automatisierter rechnungslegungsrelevanter Prozesse, im Rahmen derer mit geringer oder ohne manuelle Interaktion eine sehr große Anzahl an Transaktionen verarbeitet werden, ist zu erwarten, dass automatische Kontrollen der Informationsverarbeitung in die Prüfung einzubeziehen sind (ISA 315, Appendix 5, Tz 2, Tz 13).

(21) Der Abschlussprüfer wird jene automatischen Kontrollen der Informationsverarbeitung identifizieren, die in Abhängigkeit der gewählten Prüfungsstrategie geeignet scheinen, ausreichende Prüfungssicherheit hinsichtlich der in Abschnitt 1.2., Rz (4), angeführten Prüfziele zu ermöglichen (ISA 315, Tz 26 (b), Tz 26 (c); A166-A174). Ein Vorteil automatischer Kontrollen ist, dass diese in der Regel verlässlicher als manuelle Kontrollen sind, da sie schwieriger umgangen, ignoriert oder überschrieben werden können und weniger fehleranfällig sind (ISA 315, Appendix 5, Tz 2).

(22) In einem nächsten Schritt werden jene IT-Anwendungen identifiziert, in denen diese automatischen Kontrollen der Informationsverarbeitung umgesetzt sind. Für diese IT-Anwendungen werden die relevanten generellen IT-Kontrollen identifiziert.

(23) Falls der Abschlussprüfer plant, Auswertungen, systemgenerierte Berichte ("System-generated Reports") oder andere Informationen, die durch das geprüfte Unternehmen erzeugt werden, als Prüfungsnachweise zu verwenden (ISA 315, A166), hat er deren Relevanz (Inhalt und Detaillierungsgrad) sowie Verlässlichkeit (Vollständigkeit und Richtigkeit) für den Prüfzweck zu beurteilen und – analog zur Vorgehensweise in Rz 21 und Rz 22 – die für die Erzeugung dieser „System-generated Reports“ relevanten IT-Anwendungen und die dazugehörigen generellen IT-Kontrollen zu identifizieren, sofern Vollständigkeit und Richtigkeit der „System-generated Reports“ nicht durch andere aussagebezogene Prüfungshandlungen adressiert werden. Dieses Vorgehen gilt gleichermaßen für jene Informationen, die das Unternehmen selbst bei der Durchführung von prüfungsrelevanten Kontrollen verwendet (ISA 315, A169; ISA 500, Tz 9, A50-A52).

(24) Die dauerhafte Wirksamkeit der automatischen Kontrollen der Informationsverarbeitung hängt auch von der Wirksamkeit der diesbezüglichen generellen IT-Kontrollen ab, da diese sicherstellen, dass automatische Kontrollen der Informationsverarbeitung nicht umgangen, außer Kraft gesetzt oder unbeabsichtigt verändert werden.

(25) Durch die inhärente Konsistenz der Verarbeitung bei Verwendung von IT-Systemen
a) ist ein einzelner, zeitpunktbezogener Test – bei Vorhandensein wirksamer genereller IT-Kontrollen – regelmäßig ausreichend, um die Wirksamkeit einer automatischen Kontrolle der Informationsverarbeitung festzustellen, und
b) kann in Folgeperioden – falls es nachweislich keine Änderung an der automatischen Kontrolle der Informationsverarbeitung (insbesondere hierfür relevanten Programmobjekten oder Parametern) gegeben hat – das Testen der Wirksamkeit

von generellen IT-Kontrollen allein ausreichend sein, um die Wirksamkeit der automatischen Kontrolle der Informationsverarbeitung ohne neulichen Test derselben festzustellen. (ISA 330, A29).

### 2.6. Weitere Vorgehensweise bei unwirksamen automatischen Kontrollen oder unwirksamen generellen IT-Kontrollen

(26) Bei Identifikation von unwirksamen generellen IT-Kontrollen hat der Abschlussprüfer die Auswirkungen auf die dauerhafte Wirksamkeit sämtlicher betroffener, prüfungsrelevanter automatischer Kontrollen der Informationsverarbeitung sowie auf die Verlässlichkeit von durch das Unternehmen erstellten, prüfungsrelevanten Informationen zu beurteilen (ISA 330, Tz A29b).

(27) Bei unwirksamen generellen IT-Kontrollen oder unwirksamen automatischen Kontrollen der Informationsverarbeitung kann der Abschlussprüfer häufig Prüfsicherheit durch das Testen kompensierender Kontrollen sowie durch zusätzliche Prüfungshandlungen erlangen (ISA 330, Tz A29b).

(28) Falls der Abschlussprüfer sich nicht auf generelle IT-Kontrollen verlassen möchte oder erwartet, dass diese nicht wirksam sind, kann die dauerhafte Wirksamkeit automatischer Kontrollen der Informationsverarbeitung auch durch direktes Testen derselben festgestellt werden. (vgl ISA 315, Tz A180).

## 3. Anwendungszeitpunkt

(29) Dieses Fachgutachten ist auf Prüfungen von Abschlüssen für Geschäftsjahre, die am oder nach dem 15. Dezember 2022 enden, anzuwenden.