SAP R/3® im Kontext der Ordnungsmäßigkeitsanforderungen

oder

woraus resultieren Ordnungsmäßigkeitsanforderungen im SAP R/3®-Umfeld für die Prüfung?

Bei SAP R/3® handelt es sich um eine Software, die auch gerne als ERP System bezeichnet wird.
ERP steht dabei für Enterprise Resource Planning, was soviel bedeutet dass unter anderem die unternehmenseigenen Produktionsfaktoren wie beispielsweise Mensch und Betriebsmittel in eine planvoll organisierte Wirtschaftseinheit effizient integriert werden.
Dies soll unter zu Hilfenahme einer Software geschehen, die die beteiligten Geschäftsprozesse integrativ abbildet und somit sämtliche Ressourcen unternehmensweit verwaltet.
Unternehmensbereiche, die durch eine ERP Software abgebildet werden können, sind unter anderem

- Finanz- und Rechnungswesen,
- Materialwirtschaft,
- Controlling,
- Personalwirtschaft,
- Fertigung,
- Forschung und Entwicklung,
- Verkauf und Vertrieb.

Wenn ein Unternehmen nunmehr SAP R/3® einsetzt, dann auch regelhaft um die finanzbuchhalterischen Aspekte abzubilden.

Als normensetzende Instanz für die Buchführung wirkt meist die nationale Gesetzgebung. Im Zeitalter der Globalisierung und Wirken der internationalen Märkte haben sich internationale Rechnungslegungsvorschriften etabliert, die häufig als Additiv zur nationalen Gesetzgebung wirken oder sie ggfs. langfristig auch ersetzen werden.

SAP® wird als Software weltweit in über 120 Ländern bei 24.000 Kunden mit mehr als 84.000 Installationen eingesetzt.
Demzufolge gilt es die jeweiligen Landesvorschriften zu berücksichtigen als auch internationale Vorgaben zu erfüllen.

In diesem weit verzweigten Kontext müssen Prüfer ihre jeweiligen Ordnungsmäßigkeitsvorgaben rekrutieren und in eine gesamtheitliche Prüfstrategie integrieren.
Die nachfolgenden Ausführungen sollen dabei ein wenig behilflich sein.

I. Rechnungslegung

1. GoB - GoBS

Mit der Einführung des Handelsrechts im Jahre 1886 wurden bereits die ersten GoB definiert. 1985 erst erfolgte anlässlich der EG-Harmonisierung der Rechnungslegungsvorschriften die gesetzliche Verankerung.
Jedes Unternehmen, das seine Buchhaltung EDV-seitig abbildet unterliegt in Deutschland den Anforderungen zu den Grundsätzen ordnungsmäßiger DV-gestützer Buchführungssysteme (GoBS).
Dieses Regelwerk wurde 1995 durch ein Schreiben des Bundesministeriums der Finanzen veröffentlicht und maßgeblich mit der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV) entwickelt.
Ursprünglich war der Geltungsbereich auf die steuerlichen Buchführungsaspekte beschränkt; da jedoch vielfach in Klein- und Mittelständischen Unternehmen (KMU) die Einheitsbilanz Anwendung erfährt, wirkt sich das Grundsatzregelwerk entsprechend ergänzend handelsrechtlich aus.
Im Wesentlichen geht es natürlich darum, die Grundsätze ordnungsmäßiger Buchführung auf eine EDV-seitige Lösung zu transformieren und somit dem Kern der Anforderungen Rechnung zu tragen.

Bei den Grundsätzen ordnungsmäßiger Buchführung (GoB) können ein paar essentielle Regeln vereinfacht zusammengefasst werden:

1. Keine Buchung ohne Beleg, und wiederum kein relevanter Beleg ohne Buchung(en).
2. Jede Buchung muss eindeutig auf einen Beleg verweisen und vice versa.
3. Es dürfen keine nachträglichen Veränderungen einer Buchung vorgenommen werden, sondern nur Umbuchungen oder Stornierungen.
4. Die Buchführung muss zweckmäßig chronologisch geordnet und lückenlos sein.

Faktisch handelt es sich bei den benannten GoB ausschließlich um einen unbestimmten Rechtsbegriff, deren elementare Anforderung aus dem HGB (Handelsgesetzbuch) resultieren.

Es gilt nach:
§ 238 Abs. 1 HGB (für alle Unternehmungen): „Jeder Kaufmann ist verpflichtet Bücher zu führen und in diesen seine Handelsgeschäfte und die Lage seine Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen."

§ 243, I HGB (für alle Unternehmungen): „Der Jahresabschluss ist nach den GoB aufzustellen."

§ 264, II HGB (für Kapitalgesellschaften): „Der Jahresabschluss hat unter Beachtung der GoB ein den tatsächlichen Verhältnissen entsprechendes Bild (...) zu vermitteln."

Die gesetzlichen Rahmenanforderungen an die inhaltliche Ausgestaltung der GoBS lassen sich konkret wie folgt zusammenfassen (§§ 238 Abs.2, 239 Abs.4, 257, 261 HGB und §§ 145, 146 AO):

- Die buchführungspflichtigen Geschäftsfälle müssen richtig, vollständig und zeitgerecht erfasst sein und sich in ihrer Entstehung und Entwicklung verfolgen lassen (Beleg- und Journalfunktion).
- Die Geschäftsfälle sind so zu verarbeiten, dass sie geordnet darstellbar sind und demnach ein Überblick über die Vermögens und Ertragslage gewährleistet ist (Kontenfunktion).
- Die Buchungen müssen einzeln und geordnet nach Konten erfolgen. Die Konten müssen fortgeschrieben werden nach Kontensummen oder Salden, sowie nach Abschlusspositionen. Diese müssen alle jederzeit darstellbar und lesbar gemacht werden können.
- Einem sachverständigen Dritten muss es möglich sein, sich in angemessener Zeit mit dem Buchführungsverfahren vertraut zu machen, damit er sich einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens machen kann.

- Das Verfahren der DV-gestützten Buchführung muss durch eine Verfahrensdokumentation sowohl die aktuellen als auch die historischen Verfahrensinhalte nachweisen, verständlich und nachvollziehbar machen.
- Eine Programmidentität muss dahingehend gewährleistet sein, dass das in der Dokumentation beschriebene Verfahren dem in der Praxis eingesetzten entspricht.

Führung der Handelsbücher
Für die Führung der Handelsbücher nach § 239 HGB (Radierverbot) gilt:

1. Die Eintragungen in Bücher und die sonst erforderlichen Aufzeichnungen müssen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden.
2. Eine Eintragung oder Aufzeichnung darf nicht in einer Weise verändert werden, dass ihr ursprünglicher Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.
3. Die Handelsbücher und die sonst erforderlichen Aufzeichnungen können auch auf Datenträgern geführt werden, soweit diese Form der Buchführung einschließlich des dabei angewandten Verfahrens den Grundsätzen ordnungsmäßiger Buchführung entspricht.

2. IRFS

Die internationale Rechnungslegung nach IAS / IRFS äußert sich hinsichtlich der Anforderungen an eine ordnungsmäßige Buchführung nicht in ähnlich detaillierter Form. Im Rahmenkonzept werden zwar qualitative Anforderungen an den Abschluss (Qualitative characteristics of financial statements) wie Verständlichkeit, Relevanz, Verläßlichkeit und Vergleichbarkeit deklariert, die Ausführungen geben inhaltlich jedoch keine konkreteren Hinweise.
Einzig im Abschnitt der zu Grunde liegenden Anforderungen (Underlying assumptions) kann ein Hinweis zur Zeitnähe der Datenabbildung gewonnen werden, indem eine Zuordnung der Erfassung der Geschäftsfälle zu der Buchungsperiode vorgenommen wird, der sie zuzurechnen sind.

3. Prüfungshandlungen nach GoBS

Aus den Anforderungen der GoBS lassen sich folgende elementare Prüfungshandlungen direkt ableiten.

Nr.	Prüfungshandlung nach GoBS	SAP® Prüffeld
1	Es muss geprüft werden ob Geschäftsvorfälle bei DV-Buchführungen (batch-/ dialogorientierte Verfahren) ordnungsgemäß gebucht sind. Um diese Anforderung zu erfüllen müssen sie nach einem Ordnungsprinzip vollständig, formal richtig, zeitgerecht und verarbeitungsfähig erfasst und gespeichert sein.	Verbuchungsabbrüche Batch-Input Mappen Direct-Input Verfahren Belegnummernpufferung Lücken in Belegnummern
2	Es muss geprüft werden, ob die Forderung nach einem Ordnungsprinzip erfüllt ist. Dazu muss auf die gespeicherten Geschäftsvorfälle und/oder Teile von diesen gezielt zugegriffen werden können.	Beleganzeige Belegübersichten
3	Es muss geprüft werden, ob die Verarbeitungsfähigkeit der Buchungen, angefangen von der maschinellen Erfassung über die weiteren Bearbeitungsstufen, sichergestellt ist. Dazu gehören neben der Speicherung der Daten zum Geschäftsvorfall selbst - auch die Speicherung für die Verarbeitung erforderlichen Tabellendaten und Programme.	Verbuchungsabbrüche Batch-Input Mappen Direct-Input Verfahren Tabellenprotokollierung Programmdokumentation Große Umsatzprobe

Nr.	Prüfungshandlung nach GoBS	SAP® Prüffeld
4	Es muss geprüft werden, ob durch Kontrollen sichergestellt ist, dass alle Geschäftsvorfälle vollständig erfasst wurden und nach erfolgter Buchung nicht unbefugt (d. h. nicht ohne Zugriffsschutzverfahren) und nicht ohne Nachweis des vorausgegangenen Zustandes verändert werden könnten.	Verbuchungsabbrüche Berechtigungskonzept Änderungsbelegprinzip Tabelle TBAER Tabellenprotokollierung
5	Es muss geprüft werden, ob die Forderung nach zeitgerechter Verbuchung eingehalten werden. Dies bezieht sich auf die zeitnahe und periodengerechte (der richtigen Abrechnungsperiode zugeordnete) Erfassung der Geschäftsvorfälle.	Buchungsperiodenpflege Buchungsstoff Vorerfassung Batch-Input-Mappen
6	Es muss geprüft werden, ob der Zusammenhang zwischen dem zugrunde liegenden Geschäftsvorfall und dessen Buchung bzw. dessen DV-Verarbeitung durch eine aussagekräftige Verfahrensdokumentation ergänzt und durch den Nachweis ihrer ordnungsmäßigen Anwendung dargestellt werden kann.	Job-Dokumentationen Freigabeverfahren Korrektur- und Transportwesen Tabellenprotokollierung DBTABLOG
7	Es muss geprüft werden ob die Merkmale (Belegbestandteile, Kontierung) einer erfolgten Buchung verändert werden können. Der Inhalt der ursprünglichen Buchung muss in jedem Fall feststellbar bleiben, z. B. durch Aufzeichnungen über durchgeführte Änderungen (Storno- und Neubuchung). Diese Änderungsnachweise sind Bestandteil der Buchführung und aufzubewahren.	Berechtigungskonzept Aufbewahrungsumsetzung Änderungsbelege Tabelle TBAER

Nr.	Prüfungshandlung nach GoBS	SAP® Prüffeld
8	Es muss geprüft werden, ob die eingerichteten IKS Maßnahmen hinsichtlich der Ordnungsmäßigkeitsanforderungen (Ausgestaltung organisatorischer Kontrollmechanismen, wie z.B. Funktions-trennungen und Abstimmkontrollen) ausreichend sind. Dazu müssen: • manuelle und automatische Kontrollen zur Vollständigkeit und Korrektheit durchgeführt werden, • eindeutige Regelungen für Zuständigkeiten definiert sein, • buchungsrelevante Abläufe definiert und in der Reihenfolge festgelegt sein, • durchgeführte Kontrollen (Abstimmungs-kontrollen / Plausibilitätskontrollen, Freigabeverfahren dokumentiert sein, • die Programmidentitäten nachgewiesen sein.	Berechtigungskonzept Vier-Augen-Prinzipien Funktionstrennungen Dokumentation Protokollierungsverfahren Test- und Freigabeverfahren Korrektur- und Transportwesen Versionshistorie
9	Es muss geprüft werden, ob das IKS mit seinen Maßnahmen ausreichend dokumentiert ist.	Dokumentation
10	Es muss geprüft werden ob ein Datensicherungskonzept vorliegt, das eine Sicherung der Software (Betriebssystem, Anwendungsprogramme), der Tabellen- und Stammdaten, der Bewegungsdaten (z. B. der Daten eines Geschäftsvorfalles) sowie der sonstigen Aufzeichnungen vorsieht. Die Sicherung muss gegen Verlust und unberechtigte Änderungen Schutz bieten.	Dokumentation Berechtigungskonzept Änderungsbelege Tabellenprotokollierung Datensicherung
11	Es ist zu prüfen, ob die gesetzlichen Aufbewahrungsfristen eingehalten werden.	Tabellenprotokollierung DBTABLOG Änderungsbelege Belegsicherung
12	Es ist zu prüfen ob der Schutz der Daten durch wirksame Zugangs- und Zugriffsverfahren realisiert ist.	Berechtigungskonzept Lokaler Zugang

Nr.	Prüfungshandlung nach GoBS	SAP® Prüffeld
13	Es ist zu prüfen, ob der Vergabenachweis für Zugriffsberechtigungen dokumentiert ist.	Berechtigungskonzept Änderungsbelege
14	Es ist zu prüfen, ob die Arbeitsanweisungen für die Anwender dokumentiert sind.	Dokumentation Handbuch / Manual
15	Es ist zu prüfen, ob die Lesbarkeit und Wiederherstellbarkeit von gesicherten Daten gewährleistet ist.	DBTABLOG Änderungshistorien Beleganzeigen
16	Es ist zu prüfen, ob das Datensicherungskonzept dokumentiert ist.	Dokumentation
17	Es ist zu prüfen, ob die jeweilige Verfahrensdokumentationen die folgenden Aspekte beinhaltet: • eine Beschreibung der sachlogischen Lösung, • die Beschreibung der programmtechnischen Lösung, • eine Beschreibung, wie die Programm-Identität gewährt wird, • Beschreibung, wie die Integrität von Daten gewahrt wird • Arbeitsanweisungen für den Anwender.	Job-Dokumentation Unternehmenseigene ABAP/4 Programme und Tabellen Dokumentation Manual
18	Es ist zu prüfen, ob die gesetzliche Aufbewahrungsfrist von 10 Jahren für die Bestandteile der Verfahrensdokumentation eingehalten wird.	Job-Dokumentation Unternehmenseigene ABAP/4 Programme und Tabellen Dokumentation Tabellenprotokollierung
19	Es ist zu prüfen, ob das Datenwiedergabeverfahren in einer Arbeitsanweisung abgebildet wurde.	Dokumentation

II. Sarbanes Oxley Act 2002

Der Sarbanes-Oxley Act ist als politische Reaktion auf verschiedene Unternehmenszusammenbrüche und Finanzskandale (Enron, Worldcom) in den vereinigten Staaten zu verstehen. Durch ihn soll dem entstandenen Vertrauensverlust in die Wirtschaft und den Aktienmarkt entgegengewirkt werden. Er wurde im Juli 2002 mit nur drei Gegenstimmen verabschiedet.
Der Sarbanes Oxley Act hat Gesetzeswirkung.
Er gilt für inländische und ausländische Unternehmen, die an US-Börsen oder der NASDAQ gelistet sind.
Inhaltlich untergliedert sich der Act in verschiedene Abschnitte (Sections). Der wesentliche Anspruch an die Prüfer resultiert aus der Section 404 *Management assessment of internal controls*, die besagt, dass das Management ein adäquates internes Kontrollsystem einzurichten hat. Dieses ist kontinuierlich zu pflegen, zu adaptieren und zu überwachen. Jährlich ist der SEC (US Securities and Exchange Commission) ein Bericht über die Wirksamkeit des IKS vorzulegen. Zusätzlich muss der Abschlussprüfer die Richtigkeit des Berichts testieren.
Erstmalig sollen für die Einhaltung die Vorstandsvorsitzenden und Finanzvorstände persönlich haftbar gemacht werden.

Nr.	Prüfungshandlung nach Sarbanes Oxley	SAP® Prüffeld
1	Es ist zu prüfen, ob eine Aufnahme aller IST-Geschäftsprozesse, insbesondere der (Kontroll-) Prozesse, die in unmittelbarem Zusammenhang mit der Rechnungslegung stehen, erfolgt ist.	Arbeitsplatzanalyse Funktionstrennung Vier-Augen-Prinzip Berechtigungskonzept
2	Es ist eine Schwachstellenanalyse der IST-Prozesse, inklusive aktuell vorhandener Unterstützungen durch IT-Lösungen durchzuführen.	SAP® Komplettaudit inkl. Systemsicherheit, Berechtigungskonzept
3	Es ist zu prüfen, ob die Auswahl eines anerkannten Regelwerks zur Unterstützung und Ausprägung eines Internen Kontrollsystems (IKS), wie z.B. Integrated Framework for Internal Control vom COSO (Committee on Sponsoring Organisations of the Treadway Commission) oder IT Control Objectives for Sarbanes Oxley vom IT Governance Institute erfolgt ist.	Dokumentation
4	Es ist zu prüfen, ob die IST-Prozesse mit dem IKS korrespondieren.	Berechtigungskonzept
5	Es ist zu prüfen, ob bestehende Defizite der Eliminierung zugeführt werden.	Berechtigungskonzept Dokumentation
6	Es ist zu prüfen, ob ein SOLL-Prozess-Design in Anlehnung an die IKS-Richtlinien eingerichtet ist.	Berechtigungskonzept Prozessanalysen
7	Es ist zu prüfen, ob eine Dokumentation der SOLL-Prozesse vorliegt.	Dokumentation
8	Es ist zu prüfen, ob ein Design und eine Dokumentation zu Review-Prozessen vorliegen.	Dokumentation

Die weiterführenden Prüfungshandlungen, die sich hieraus für ein SAP® System ableiten lassen korrespondieren im Wesentlichen mit den Tätigkeiten aus den GoBS.

III. Stellungnahmen
FAIT 1 / FAIT 2 und ERS FAIT3

Der Fachausschuss für Informationstechnologie hat mit FAIT1 eine Stellungnahme zu den Grundsätzen ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie abgegeben und löst damit FAMA 1/1987 ab.
FAIT 2 beschäftigt sich ausführlich mit den Grundsätzen ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce.
Der Entwurf zu FAIT 3 widmet sich den Grundsätzen ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren.

Um grundsätzlichen Sicherheitsanforderungen gerecht zu werden, sind die gängigen Voraussetzungen für eine ordnungsmäßige Rechnungslegung in FAIT 1 einführend benannt. Dazu zählen Datensicherheit und Datenschutz, Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit.

Nr.	Sicherheitsprüfung nach FAIT 1	SAP® Prüffeld
1	Es muss geprüft werden, ob gängige Sicherheitsanforderungen zu Datenschutz und Datensicherheit umgesetzt sind.	Benutzer- und Berechtigungskonzept Passwortsicherheit
2	Es muss geprüft werden, ob die Löschvorschriften für personenbezogene Daten gem. Bundesdatenschutzgesetz eingehalten werden.	HR
3	Es muss geprüft werden, ob Schutzmaßnahmen vor unautorisierten Änderungen eingerichtet sind.	Benutzer- und Berechtigungskonzept Änderungsbelege Protokollierung
4	Es muss geprüft werden, ob ausreichende Maßnahmen im Rahmen von Back-Up Strategien eingerichtet sind.	Datensicherung Back-Up
5	Es muss geprüft werden, ob ausschließlich autorisierte Zugriffe erfolgen.	Benutzer- und Berechtigungskonzept Protokollierung
6	Es muss geprüft werden, ob ausreichende Maßnahmen zur Wahrung von Authentizitätsrichtlinien getroffen sind.	Benutzer- und Berechtigungskonzept
7	Es muss geprüft werden, ob den Verbindlichkeitsaspekten bei geschäftlichen Transaktionen Rechnung getragen wird.	Benutzer- und Berechtigungskonzept Authentifikationsrichtlinien

Für die detailliertere Überprüfung der Ordnungsmäßigkeit der Buchführung ist die Einhaltung der nachfolgend zitierten Grundsätze als Maßgabe eingerichtet:

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

Daraus lassen sich die folgenden Prüfungshandlungen direkt ableiten.

Nr.	**Prüfungshandlung nach FAIT 1**	**SAP® Prüffeld**
1	Es ist zu prüfen, ob sämtliche Geschäftsfälle einzeln abgebildet und vollständig, unter Wahrung der gesetzlichen Aufbewahrungsfristen nach § 257 HGB, vorgehalten werden.	Buchungsstoff - Abstimmanalyse Belegübersicht Verbuchungsabbrüche Batch-Input-Mappen Direct-Input Verfahren Belegnummernpufferung Protokollierung
2	Es ist zu prüfen, ob die Abbildung der Geschäftsfälle inhaltlich konsistent erfolgt.	Buchungsstoffe Beleganzeige
3	Es ist zu prüfen, ob jeder Geschäftsfall der Buchungsperiode zugeordnet ist, in der er aufgetreten ist.	Buchungsstoff Belegauswertungen Buchungsperiodenpflege
4	Es ist zu prüfen, ob sämtliche Maßnahmen zur Sicherung der Unveränderlichkeit für Buchungsbelege getroffen sind. (§ 239 Abs. 3 Satz 2 HGB)	Protokollierung Tabelle TBAER Änderungsbelege Berechtigungskonzept Datensicherungsverfahren Archivierungsrichtlinien
5	Es ist zu prüfen, ob für automatisierte Buchungen die Parametrisierungsinformationen dokumentiert sind und ob Änderungsbelege erzeugt werden.	Batch-Input-Mappen Änderungsbelge Protokollierung Job-Dokumentationen
6	Es ist zu prüfen, ob für programminterne Vorschriften zur Generierung der Buchungen eine Dokumentation vorliegt.	Job-Dokumentation Dokumentation von Eigenentwicklungen

Nr.	Prüfungshandlung nach FAIT 1	SAP® Prüffeld
7	Es ist zu prüfen, ob ein autorisiertes Änderungsverfahren für programminterne Vorschriften eingerichtet ist.	Versionshistorie Dokumentation von Eigenentwicklungen Korrektur- und Transportwesen Test- und Freigabeverfahren Berechtigungskonzept
8	Es ist zu prüfen, ob ein Belegaustausch über externe Schnittstellen erfolgt und durch Autorisierungskonzepte abgesichert wird.	Schnittstellen Batch-Input Mappen Direct-Input Autorisierung Berechtigungskonzept
9	Es ist zu prüfen, ob eine Verfahrensdokumentation vorliegt, die Regeln für die Generierung und Kontrolle der maschinellen Buchungen festlegt.	Verfahrensdokumentation Job-Dokumentation
10	Es ist zu prüfen, ob eingesetzte Programme gegen unautorisierte und undokumentierte Änderungen geschützt sind.	Systemparameter Berechtigungskonzept
11	Es ist zu prüfen, ob für die Journale der Buchungen die gesetzlichen Aufbewahrungs-pflichten eingehalten werden.	Protokollierung Datensicherungsverfahren Datenarchivierungsverfahren Wiederherstellbarkeit
12	Es ist zu prüfen, ob eine ordnungsgemäße Verfahrensdokumentation vorliegt, die die Beschreibung aller zum Verständnis der Rechnungslegung erforderlichen Verfahrensbestandteile beinhaltet.	Dokumentation Dokumentation von Eigenentwicklungen Job-Dokumentation Tabellenprotokollierung
13	Es ist zu prüfen ob für sämtliche anwendungsspezifischen Anpassungen und die eingerichteten internen Kontrollsysteme des Anwenders (z.B. Parametrisierungen, Verwendung der Eingabefelder, Schlüsselsystematiken) eine Dokumentation vorliegt.	Protokollierung Systemparameter Repository Dokumentation von Eigenentwicklungen

Nr.	Prüfungshandlung nach FAIT 1	SAP® Prüffeld
14	Es ist zu prüfen, ob für unternehmensspezifische Einstellungen und Anpassungen, Parametrisierungen und Änderungen in Tabellen und Stammdaten, die für die Verarbeitung aufzeichnungspflichtiger Geschäftsvorfälle erforderlich sind, die Anforderungen an die 10-jährige Aufbewahrungspflicht gewährleistet sind (§ 257 HGB).	Protokollierung Tabellenprotokollierung Änderungsbelege Änderungshistorie Systemparameter Dokumentation von Eigenentwicklungen Job-Dokumentation
15	Es ist zu prüfen, ob gewährleistet ist, das Systemprotokolle 10 Jahre aufbewahrt werden, wenn eine Ordnungsmäßigkeitsbeurteilung nur hier nach getroffen werden kann.	SysLog Security Audit Log Systemparameter
16	Es ist zu prüfen, ob im Rahmen von Outsourcing-Prozessen gesichert ist, dass der Dienstleister buchführungsrelevante Informationen nachvollziehbar dokumentiert und ggfs. aushändigt.	Dokumentation von Eigenentwicklungen Job-Dokumentation Systemparameter Änderungsbelege Änderungshistorien Vertragsprüfung

Weitere, die grundsätzliche IT-Technologie betreffende Prüfaspekte, werden in der nachfolgenden Ausführung zum PS 330 ausführlich behandelt.

Inhaltlich verweist FAIT 2 bezüglich der Ordnungsmäßigkeit der Buchführung auf FAIT 1 und widmet sich neben den speziellen juristischen Aspekten nach BDSG (Bundesdatenschutzgesetz), TDDSG (Teledienstdatenschutzgesetz), TDG (Teledienstgesetz), Signaturgesetz und Fernabsatzgesetz, im Anhang den besonderen Anforderungen an die Ordnungsmäßigkeit bei Einsatz von E-Commerce. Diese besonderen Aspekte sind nachstehend einmal zusammenfassend dargestellt.

Die beschriebenen Handlungen stützen sich primär auf die Schnittstelle zum angeschlossenen E-Commerce System.

Nr.	Prüfungshandlung nach FAIT 2	SAP® Prüffeld
1	Es ist zu prüfen, ob ein Schutz vor Veränderungen bzw. Verlust von Daten auf der Übertragungsstrecke durch Manipulation, nicht autorisierte Änderungen sowie aufgrund des Auftretens von technischen Fehlern implementiert ist.	Schnittstellenkonfiguration Berechtigungskonzept Technisches Rahmenkonzept Verschlüsselungsalgorithmen
2	Es ist zu prüfen, ob ein Schutz vor Integritätsverletzungen durch unautorisierte Zugriffe eingerichtet ist.	Berechtigungskonzept Zugriffskontrollen Zugangskontrollen
3	Es ist zu prüfen, ob die E-Commerce Anwendung durch unautorisierte Zugriffe von außen geschützt ist.	Internet-Security Firewall-Policy Virenschutz Contentschutz Passwortsichehrheit Datenbanksicherheit
4	Es ist zu prüfen, ob die eingesetzten Backup- und Notfall-Lösungen (Business Continuity Planning), System-, Programm- und Datensicherungsverfahren dokumentiert und getestet sind.	Back-Up Stratgegie Notfallplan Systemparametrisierung
5	Es ist zu prüfen, ob Sicherheitsvorkehrungen im Sinne von Intrusion-Detection (Eindringungserkennung) eingeführt sind.	Dokumentation Systemcheck Penetration
6	Es ist zu prüfen, ob verifizierende Authentifikationseinrichtungen zur Anwendung kommen.	Authentifikation Digitale Signatur
7	Es ist zu prüfen, ob verifizierende Authentifikationseinrichtungen zur Anwendung kommen, die den Verbindlichkeitsanforderungen an eine geschäftliche Transaktion genügen.	Zertifizierung Rahmenverträg Digitale Signature Bestätigungsverfahren
8	Es ist zu prüfen, ob sichergestellt ist, dass nur vollständige und sachlich korrekte Daten über das E-Commerce System erfasst werden.	Schnittstellenkonfiguration Verbuchungsprozess Transaktionssicherung
9	Es ist zu prüfen, inwieweit abgesichert ist, dass nur reale Geschäftsfälle buchhalterisch abgebildet werden.	Buchungsstoff Belegübersicht
10	Es ist zu prüfen, ob die Autorisierungsverfahren den Buchungsprozess absichern.	Berechtigungskonzept Protokollierung Änderungsbelege
11	Es ist zu prüfen, ob sichergestellt ist, dass der Zeitpunkt einer Transaktion ordnungsmäßig abgebildet und dokumentiert wird.	Belegübersicht Änderungsbelege

Nr.	Prüfungshandlung nach FAIT 2	SAP® Prüffeld
12	Es ist zu prüfen, inwieweit die Datenübertragung in das Buchführende System abgesichert ist.	Batch-Input Mappen Direct-Input Verbuchungsprozess Belegnummernvergabe Buchungsstoff Elektronische Belege
13	Es ist zu prüfen, inwieweit die Vollständigkeit des übertragenen Buchungsstoffes geprüft und dokumentiert wird.	- Vorsystem – Prozessbegleitpapiere
14	Es ist zu prüfen, ob sämtliche Änderungen an den Prozessabläufen nachvollziehbar dokumentiert und aufbewahrt werden.	Dokumentation

Im ERS FAIT 3 werden nunmehr die Anforderungen an die ordnungsmäßige Buchführung im Hinblick auf die eingesetzten Archivierungsverfahren und die Umsetzung der gesetzlichen Forderungen u.a. an die Nachvollziehbarkeit und Aufbewahrungspflicht präzisiert und adaptiert.
Unter Berücksichtigung der erforderlichen Sicherheitsaspekte wie Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit, werden die gängigen Ordnungsmäßigkeitskriterien Vollständigkeit, Richtigkeit, Zeitgerechtheit, Nachvollziehbarkeit und Unveränderlichkeit auf die Grundsätze der Archivierung projiziert.

IV. Corporate Governance

Der Deutsche Corporate Governance Kodex stellt die wesentlichen gesetzlichen Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften (Unternehmensführung) dar.
Ergänzend beinhaltet er international und national anerkannte Standards hinsichtlich einer „guten und verantwortungsvollen Unternehmensführung".

So wird der Vorstand im Abschnitt (Aufgaben und Zuständigkeiten) 4.1.3 verpflichtet für die „Einhaltung der gesetzlichen Regelungen" zu sorgen; der Abschnitt 4.1.4 verpflichtet ihn für ein „angemessenes Risikomanagement und Risikocontrolling im Unternehmen" zu sorgen.

Laut Abschnitt 5.3 (Bildung von Ausschüssen) soll der Aufsichtsrat nach Abschnitt 5.2.3 einen „Prüfungsausschuss (Audit Committee) einrichten, der sich insbesondere mit Fragen der Rechnungslegung und des Risikomanagements, der erforderlichen Unabhängigkeit des Abschlussprüfers, der Erteilung des Prüfungsauftrags an den Abschlussprüfer, der Bestimmung von Prüfungsschwerpunkten und der Honorarvereinbarung befasst."

Für die Rechnungslegung (Abschnitt 7.1.1) gilt, dass der „Konzernabschluss und die Zwischenberichte unter Beachtung international anerkannter Rechnungslegungsgrundsätze aufgestellt werden sollen. Für gesellschaftsrechtliche Zwecke (Ausschüttungsbemessung, Gläubigerschutz) werden Jahresabschlüsse nach nationalen Vorschriften (HGB) aufgestellt, die auch Grundlage für die Besteuerung sind".

V. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) von 1998

Vorstände und Geschäftsführer haben bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Kaufmanns anzuwenden.
Hierzu sind sie bereits seit Einführung des Aktiengesetzes gesetzlich verpflichtet (§93 Abs.1 AktG). Zu diesen Sorgfaltspflichten gehört neben der Festlegung der Unternehmenspolitik auch die Implementierung der zugehörigen funktionsfähigen Unternehmensüberwachung (§ 91 (2) AktG).
Mit dem bereits im Mai 1998 verabschiedeten Artikel-Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) werden Unternehmen u.a. verpflichtet, ein Überwachungssystem zur Früherkennung existenzgefährdender Entwicklungen einzurichten. Damit wurde die Verpflichtung der Geschäftsführung gesetzlich konstituiert, ein unternehmensweites Risikomanagement zu implementieren.
Mit dem KonTraG wurden die Unternehmen außerdem verpflichtet, im Lagebericht zu den Risiken der künftigen Geschäftsentwicklung Stellung zu beziehen. Diese Anforderung ist ohne ein Risikomanagementsystem nicht erfüllbar.

Versäumnisse bei der Einrichtung eines solchen Risikomanagementsystems können bei prüfungspflichtigen Unternehmen zu einem Versagen des Bestätigungsvermerks führen. Damit wären beispielsweise Gewinnausschüttungen oder Kreditaufnahmen bei Banken unmöglich. Zudem sind die Geschäftsführer/Vorstände im Schadensfalle den Anteilseignern persönlich schadensersatzpflichtig.
Anzuwenden sind die Bestimmungen des KonTraG auf alle Wirtschaftsjahre, die nach dem 31.12.1998 beginnen. Eine Übergangsregelung ist nicht vorgesehen. Dies ist vom Abschlussprüfer im Rahmen seiner Jahresabschlussprüfung zu testieren. Im Prüfungsstandard (PS) 340 des IDW "Die Prüfung des Risikofrüherkennungssystems" heißt es dazu: "Der Abschlussprüfer hat nach § 317 Abs. 4 HGB bei Aktiengesellschaften im Rahmen der Abschlussprüfung zu beurteilen, ob der Vorstand die nach § 91 AktG erforderlichen Maßnahmen in einer geeigneten Form getroffen hat und ob das danach einzurichtende Überwachungssystem seine Aufgaben erfüllen kann."

VI. Prüfungsstandard
PS 330 / ISA 401

Abschlussprüfung bei Einsatz von Informationstechnologie vom 24.09.2002.

Der *IDW Prüfungsstandard* entspricht dem International Standard on Auditing (ISA) 401 „Auditing in a Computer Information Systems Environment“ unter Berücksichtigung neuer Entwicklungen. Der *IDW Prüfungsstandard* beinhaltet zudem ergänzende Anforderungen, die sich aus der deutschen Rechtslage und Berufsübung ergeben.
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
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 (rechnungslegungsrelevant). 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).

Das Ziel der IT-Systemprüfung ist die Beurteilung der IT-Fehlerrisiken.

Dies bedeutet, dass potentielle Fehler hinsichtlich der Rechnungslegungsrelevanz somit prophylaktisch zu prüfen sind.
Es geht dabei grundsätzlich um Risikokategorisierung und Risikominimierung; dabei sind sämtliche Risiken zu prüfen, die zu einer Störung führen könnten.
Beim Einsatz von komplexen Buchführungssystemen bedarf es einer entsprechend komplexen IT-Systemprüfung.

Dazu gehören:
- Aufnahme der eingesetzten IT-Systeme im Unternehmen
- Aufnahme ausgelagerter Bestandteile

Prüfungshandlungen können
- ex-post,
- nach Modifikationen,
- nach Neueinführungen,
- nach Erweiterungen rechnungslegungsrelevanter Bestandteile

erfolgen.

Bezugnehmend auf den IDW Prüfungsstandard 340: „*Die Prüfung des Risikofrüherkennungssystems nach §317 Abs. 4 HGB*“ (unter Berücksichtigung des § 91 Abs. 2 AktG) sind unternehmensspezifische Risikobeurteilungen vorzunehmen.
Das Verfahren und die Ergebnisse dieser Beurteilungen bilden wiederum den Ausgangspunkt für die Risikobeurteilungen im Rahmen der Risikoorientierten Prüfungsplanung des Abschlussprüfers.

Der Abschlussprüfer muss feststellen, ob das Unternehmen ein wirksames Internes Kontrollsystem implementiert hat. Das IKS gilt dann als wirksam, wenn Fehler in der Rechnungslegung vermieden sind. Dabei bezieht sich der Abschlussprüfer auch auf die Bewertungsmaßstäbe der Unternehmensleitung bei der Kategorisierung der Fehlerrisiken.
Die Herleitung dieser Bewertungsmaßstäbe wird ebenfalls überprüft und muss daher nachvollziehbar ausgestaltet sein, genauso wie die Risikoidentifizierung selbst.

Nr:	**Checkliste zur IKS – Überprüfung und Beurteilung**
1	Einsetzung eines Internen Kontrollsystem sofern nicht vorhanden
2	Identifikation sämtlicher Risiken in Zusammenhang mit der Rechnungslegung (zzgl. Dokumentation)
3	Klassifizierung sämtlicher identifizierter Risiken mit nachvollziehbaren Bewertungsmaßstäben (zzgl. Dokumentation)
4	Maßnahmenkatalog zur Risikominimierung (zzgl. Dokumentation)
5	Prüfprozedur des IKS mit zugehöriger Dokumentation in fest definierter Zeitsystematik

Sofern ein Unternehmen IT-Bestandteile outgesourct hat, ist durch den Abschlussprüfer zu beurteilen, inwieweit Auswirkungen für das IKS vorliegen.

Nachfolgend ist ein Handlungsleitfaden zusammengestellt, der die integrativen Prüfaspekte hinsichtlich des Einsatzes von Informationstechnologie abbilden soll. Aus dem Prüfungsstandard sind die wesentlichen Prüfschritte den jeweiligen Bereichen zugeordnet, ergänzend dazu sind die relevanten Informationsbereiche aufgelistet, die es zu eruieren gilt. Abschließend sind exemplarische Prüfansätze beigefügt.

Prüfungsschritte	**Bereich**	**Informationen**
Aufnahme des IT Systems	IT-Umfeld	• Grundeinstellungen zum Einsatz (Unternehmens-leitlinien, Sicher-heitshandbücher) • verbindliche Strategien • High-Level-Controls
	IT-Organisation	• Organigramme + Ablaufpläne • Verantwortlichkeiten + Kompetenzen • Regelung + Verfahren zur Steuerung des IT-Betriebes • Maßnahmen und Regelungen für die Entwicklung, Einführung und Änderungen von IT-Anwendungen
z.B. Prüfung auf: • Beobachtung von Abläufen und Vergleich mit Organisationsrichtlinien und Prozessbeschreibungen. • Abgleich von im Sicherheitskonzept festgelegten Richtlinien zum Zugriffsschutz (z.B. Passwortlänge) mit den entsprechenden Parametern von Zugriffsschutzverfahren • Verifizierung von Maßnahmen zur Funktionstrennung durch Kompetenzregelungen und Arbeitsvermerke		

<table>
<tr><th>Prüfungsschritte</th><th>Bereich</th><th>Informationen</th></tr>
<tr><td></td><td>IT-Infrastruktur</td><td>• Hardware
• Betriebssysteme
• Netzwerke
• IT-Betrieb
• Sicherheitskonzept</td></tr>
<tr><td colspan="3">z.B. Prüfung auf:
• physische Sicherungsmaßnahmen
• Logische Zugriffskontrollen
• Datensicherungs- und Auslagerungsverfahren
• Maßnahmen für geordneten Regelbetrieb
• Verfahren für Notbetrieb
• Maßnahmen zu Sicherung der Betriebsbereitschaft</td></tr>
<tr><td></td><td>IT-Anwendungen</td><td>• Bezeichnungen der Software, Kurzbeschreibung des Aufgabengebietes, inkl. Hardwareplattform
• Klassifizierung der Software nach Dialog- und /oder Batchanwendung
• Software Typ
• Angaben zu verwendeten Programmier-sprachen und Datenhaltung</td></tr>
<tr><td colspan="3">z.B. Prüfung auf:
• Erfüllung verfahrensbezogener Anforderungen der Grundsätze ordnungsmäßiger Buchführung.
• Erfüllung der Anforderungen an Softwaresicherheit.
• Erfüllung der Anforderungen an rechnungslegungsrelevante Verarbeitungsregeln.
• Anwendungsbezogene IT-Kontrollen.
• Kontrollen auf Auswahl- und Entwicklungsprozess sowie Implementierung von Software.</td></tr>
</table>

Prüfungsschritte	Bereich	Informationen
	IT-Geschäftsprozesse	• Rechnungslegungs-relevante Unternehmens-abläufe anhand der funktions- oder prozessorientierten Beschreibung der Ablauforganisation • Dazu eingesetzte IT-Infrastruktur und IT-Anwendungen sowie relevante Schnittstellen • Datenfluss • Verbindung zur Buchführung
z.B. Prüfung auf: 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 • welche Anwendungs- und Prozesskontrollen bei der Verarbeitung von Geschäftsvorfällen bestehen • zutreffende Einstellungen 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		

Prüfungsschritte	**Bereich**	**Informationen**
Aufbauprüfung des IT-Kontrollsystems	Beurteilung der Angemessenheit	
	Vorläufige Beurteilung der Wirksamkeit	
Funktionsprüfung des IT-Kontrollsystems	Prüfung der Wirksamkeit	
	Beurteilung der Wirksamkeit	
z.B. Prüfung auf: • die Prüfung des IKS durch die Interne Revision • die Prüfung des IKS durch einen anderen externen Prüfer • spontane Prüfung einzelner Regelungen des IKS durch andere Unternehmensmitarbeiter oder die Unternehmensleitung (High-Level-Controls)		

VII. Fazit

Zusammenfassend kann man schon konstatieren, dass sich die wesentlichen Prüfaspekte im Kontext der unterschiedlichen Anforderungen durchaus wiederholen, wobei sich selbstverständlich der jeweilige Fokus ein wenig verschiebt.
Daraus kann man die folgende Prüfpyramide ableiten, die letztlich die relevanten Schnittstellen vereint und neben der Integration der Prüffelder, natürlich auch die Integration eines buchführenden IT-Systems repräsentiert.