Kurzprotokoll zum Ablauf der Prüfung von IT-bezogenen Aspekten im Rahmen der Verständnisgewinnung über die Einheit und das interne Kontrollsystem

09/2024

	IT-Aspekt im Bereich	Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
1	**IT-Aspekte im Bereich „Verständnisgewinnung der Einheit und ihrem Umfeld“**		
1.1	**Erlangung Verständnis vom IT-Einsatz im Geschäftsmodell**	Information darüber, wie im Geschäftsmodell der **IT-Einsatz** in die **Interaktionen** mit Kunden, Lieferanten, Banken etc. durch • IT-Schnittstellen und • andere Technologien **integriert** ist (vgl. Anlage 1 zu ISA [DE] 315 (Revised 2019).	**Fragebogen** an Mandanten versenden • Befragungen • Beobachtung • Inaugenscheinnahme • Einsichtnahme in Unterlagen
		Verständnisgewinnung insbesondere von • **IT-Umgebung** (gesamter Rahmen der IT, die zur Unterstützung des Geschäftsbetriebs eingesetzt wird) • **IT-Infrastruktur** (Netzwerk, Betriebssystemen, Datenbanken, Hard- und Software) • **IT-Anwendungen** (Programme für die Initiierung, Verarbeitung, Aufzeichnung und Berichterstattung von Geschäftsvorfällen und Informationen) • **IT-Prozesse** (Prozesse zur Verwaltung des Zugriffs auf die IT-Umgebung der Programmänderungen oder Änderungen der IT-Umgebung und des IT-Betriebs)	
		Beachte: Konzentration auf die IT-Anwendungen und andere Aspekte, über die bedeutsame Arten von Geschäftsvorfällen, Kontensalden und Abschlussangaben abgewickelt werden.	

Stand: 15.09.2024

	IT-Aspekt im Bereich	Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
2	**IT-Aspekte im Bereich „Verständnisgewinnung von Informationssystem“**		

2.1	**Erlangung eines Verständnisses vom Informationssystem der Einheit, das für Aufstellung Abschluss und Lagebericht relevant ist**	Das rechnungslegungsrelevante Informationssystem **besteht** aus den – zumeist IT-gestützten –
		• **Tätigkeiten und Regelungen** sowie
		• **Unterlagen** des Rechnungswesens und
		• unterstützenden **Aufzeichnungen**,
		die **ausgestaltet und eingerichtet** wurden, um
		• **Geschäftsvorfälle** der Einheit
		  o auszulösen
		  o aufzuzeichnen
		  o zu verarbeiten
		• **fehlerhafte Verarbeitung** von Geschäftsvorfällen zu **beheben**
		• **bewusste Außerkraftsetzung** von Systemen oder Umgehung von Kontrollen zu verarbeiten/ **protokollieren**
		• Informationen **aus der Verarbeitung von Geschäftsvorfällen** aus den Nebenbüchern in das **Hauptbuch** aufzunehmen
		• für die Aufstellung des Abschlusses **relevante Informationen** zu Ereignissen und Umständen zu erfassen und zu verarbeiten, die **keine Geschäftsvorfälle** sind (z. B. planmäßige Abschreibung)
		• sicherstellen, dass die nach den maßgegebenen Rechnungslegungsgrundsätzen anzugebenden **Informationen gesammelt, aufgezeichnet, verarbeitet, zusammengefasst** werden und darüber im **Abschluss** angemessen berichtet wird.
			Anlage 3 Nr. 15 zu ISA [DE] 315 (Revised 2019)
			
			Befragungen
			Einrichtungen
			Beobachtungen
			Nachverfolgung von Geschäfts-vorfällen
			z.B. Walk-Through.

Stand: 15.09.2024

IT-Aspekt im Bereich		Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
IT-Aspekte im Bereich „Verständnisgewinnung von Informationssystem"; Forts.			
2.2	**Vorläufige Beurteilung der Komplexität der eingesetzten IT-Anwendungen**	Umfang der Prüfungshandlungen mit Bezug zur IT hängt von der Komplexität der eingesetzten IT ab, die wiederum abhängig ist von der abgebildeten wirtschaftlichen Tätigkeit des Unternehmens. Einteilung von „nicht-komplex" bis hin zu „komplex".	**Anlage 5** des ISA [DE] 315 (Revised 2019)
		Beispiel: • Mehrere IT-Altysteme in diversen Geschäftszweigen, die nicht gut integriert sind (komplexe IT-Umgebung) • Nutzung externer Dienstleister für Aspekte der IT-Umgebung (z. B. Auslagerung Hosting der IT-Umgebung oder Nutzung von Shared Service Centers für zentrale Verwaltung von IT-Prozessen im Konzern)	
2.3	**Vorgehen bei „nicht-komplexen Systemen"**	Nur **grundlegende Aspekte** zu den **allgemeinen IT-Kontrollen (ITGC)** notwendig, wie zum Beispiel: • **Datensicherung** (wie z. B.: redundante Aufbewahrung, Angemessenheit der Frequenz – täglich, wöchentlich, monatlich); Vorhandensein Dokumentation) • **Berechtigungen** (z. B. Prozess der Vergabe von Berechtigungen, administrative Berechtigungen) • **Zugriff auf den Quellcode** (z. B. Passwortvergabe) • **Change-Management** (z. B. Test von Updates) **Physische Sicherungsmaßnahmen im Serverraum** (z. B. Zugangs- und Brandschutz)	

IT-Aspekt im Bereich		Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
2. IT-Aspekte im Bereich „Verständnisgewinnung von Informationssystem"; Forts.			
2.4	**Vorgehen bei komplexen IT-Systemen**	Zur • Identifizierung von IT-Anwendungen und anderer Aspekte der IT-Umgebung • Feststellung der aus dem IT-Einsatz resultierenden Risiken und • Identifizierung der generellen IT-Kontrollen: Einbindung von Mitgliedern des Prüfungsteams mit **besonderen Kenntnissen der IT notwendig**	
3.	**Verständnisgewinnung über Kontrollaktivitäten**		
3.1	**Identifikation von IT-gestützten/automatisierten Kontrollaktivitäten und zugrundeliegende Prozesse bezüglich:**	• Bedeutsamer Risiken • Journalbuchungen	Prüfung von IT-gestützten Kontrollen in wesentlichen risikobehafteten Geschäftsprozessen (Verkaufs-, Einkaufsprozess, Materialwirtschaft etc.)
3.2	**Ermittlung Datenfluss innerhalb der relevanten IT-Anwendungen** **Prüfung der Angemessenheit der IT-gestützten prüfungsrelevanten Kontrollen**	**Beispiel: Workflow** für Ausgangsrechnungen ermöglicht Versand von Rechnungen abhängig vom Rechnungsbetrag durch verschiedene Hierarchiestufen. Der **Workflow im IT-System verhindert** aufgrund des Datenabgleichs mit dem hinterlegten Berechtigungssystem das **Umgehen der vorgegebenen Regelungen**. Es liegt eine **IT-gestützte Kontrolle** vor.	

Stand: 15.09.2024

IT-Aspekt im Bereich		Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
3. Verständnisgewinnung über Kontrollaktivitäten; Forts.			
3.3	**Prüfung der Implementierung der IT-gestützten Kontrollen**	Prüfung der durchgängigen Verwaltung des Berechtigungskonzepts während des zu prüfenden Zeitraums Bei IT-gestützten Kontrollen, die personell zugewiesene Berechtigungen abprüfen, könnte **folgendes geprüft** werden: • Regelungen im Berechtigungskonzept sind angemessen? • Wurden die vorgesehenen Regelungen tatsächlich im Berechtigungskonzept in der IT umgesetzt und implementiert? • Können diese Regelungen umgangen werden? Zum Beispiel durch mächtige, bereichsübergreifende Nutzerrechte) (Generelle IT-Kontrollen) • Datenanalysen (wer hat tatsächlich die mittels geprüfter IT-Kontrolle gesicherten Daten geändert)	
4.	**Identifikation von relevanten IT-Anwendungen und anderen Aspekten der IT-Umgebung, aus deren Einsatz sich Risiken ergeben können sowie die Risiken aus dem IT-Einsatz selbst**		
4.1	**Identifizierung von IT-Anwendungen, die Risiken aus dem IT-Einsatz unterliegen**	Auf welche IT-Anwendungen **verlässt sich die Einheit**, um die Finanzinformationen **zu verarbeiten** und deren **Integrität** aufrechtzuerhalten? **Annahme**: **Automatisierte Kontrollen** in diesen IT-Anwendungen können identifizierte **Risiken wesentlicher falscher Darstellungen behandeln**. Wenn - **Automatisierte Kontrollen** identifiziert werden, und - Abschlussprüfer stellt aufgrund Verständnisgewinnung fest, dass sich die **Einheit auf die IT-Anwendung verlässt,** - Die diese automatisierte Kontrolle **beinhaltet**, dann ist es **wahrscheinlich**, dass - diese IT-Anwendung - als eine identifiziert wird, die **den aus dem IT-Einsatz resultierenden Risiken unterliegt.**	Vgl. Anlage 5 ISA 315 Tz. 8

Stand: 15.09.2024

IT-Aspekt im Bereich		Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
4.2	**Würdigung, ob die IT-Einwendung tatsächlich Risiken aus dem IT-Einsatz unterliegt**	Dafür hat der Abschlussprüfer zu würdigen - ob und in welchem Ausmaß die Einheit **Zugriff auf den Quellcode** haben kann, - der das Management **in die Lage** versetzt, - **Programmänderungen an solchen Kontrollen oder der IT-Anwendung** vorzunehmen. Zu würdigende Aspekte dabei sind: - **Ausmaß**, in dem **Programm- oder Konfigurationsänderungen vorgenommen** werden - Ausmaß der **Formalisierung** der IT-Prozesse - **Risiko unangemessener Zugriffs auf oder unangemessener Änderung an Daten**	
4.3	**(im Vergleich zu 1 detaillierter) Identifizierung von Anwendungen und anderen Aspekten der IT-Umgebung, die Risiken unterliegen (inkl. ITGC)** **Identifizierung von Risiken, die sich aus dem IT-Einsatz ergeben können**	Inhärente IT-Risiken liegen dann vor, wenn durch den Einsatz von IT-Systemen Fehler auftreten können, die Auswirkungen auf die Ordnungsmäßigkeit der Rechnungslegung haben. Sie können sich beziehen auf • korrekte Ausgestaltung des Buchführungsverfahrens • Richtigkeit der rechnungslegungsrelevanten Programmabläufe und Verarbeitungsregeln • Sicherheit der rechnungsrelevanten Daten	

Stand: 15.09.2024

IT-Aspekt im Bereich		Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
4.4	**Vier IT-bezogene Risikoindikatoren**		

		Risikoindikator **„Abhängigkeit“**
		
		Zunehmende Automatisierung und Komplexität der IT-Systeme, die ganze Prozessketten unterstützen führen zu einer hohen Abhängigkeit des Unternehmens von der Funktionsfähigkeit und dauernden Betriebsbereitschaft der Systeme
		
		Risikoindikator **„Änderungen“**
		• **Aus größeren Änderungsprojekten im IT-Bereich** (z. B. Einführung neuer Systeme) resultieren oft wesentliche **Risiken** wie z. B.
		  ○ wesentliche Kosten- und/oder
		  ○ Terminüberschreitungen sowie
		  ○ Mängel im Verfahrensablauf
		bei fehlgelaufenen Projekten
		• Einführung neuer Technologien (Produktionsverfahren; elektronisches Einkaufswesen) stellen **hohe Anforderungen an Mitarbeiter**
		
		Risikoindikator **„Know-how und Ressourcen“**
		• **Aktuelles und spezifisches Fachwissen** bei IT-Abteilungen und Anwendern **notwendig**
		• **Überlastungen im IT- und Anwenderbereich** führen zu höherem Risiko, z.B. unzureichende Pflege und Fehlbedienungen führen zu Unzuverlässigkeit IT-System
		Risikoindikator **„Geschäftliche Ausrichtung“**
		IT-Strategie muss adäquat auf Geschäftsstrategie und Prozessanforderungen ausgerichtet sein
			Vgl. Tz. 18 des IDW Ps 330

Stand: 15.09.2024

IT-Aspekt im Bereich		Beschreibung der zu prüfenden Aspekte	Prüferische Maßnahmen
4.5	**Entscheidung des Abschlussprüfers, welche IT-gestützten Kontrollen in den IT-Anwendungen geprüft werden sollen**	Indizien: • Eigene Erkenntnisse aus der Prüfung • Prüfungsschwerpunkte • Mandant verlässt sich/verlässt sich nicht auf IT-Anwendung	
5.	**Identifizierung relevanter genereller IT-Kontrollen**		
5.1	**Beispiele für allgemeine IT-Kontrollen**	Zum Beispiel: • Einbindung relevanter IT-Anwendungen in Datensicherung • Berechtigungskonzept • Sicherungsmaßnahmen für Cyberattacken	Vgl. Anlage 6 ISA [DE] (Revised 2019)
6.	**Prüfung der IT-Kontrollen**		
6.1	**Aufbau- und Funktionsprüfung**	• Ausgestaltung und Festlegung der Implementierung von automatisierten und generellen IT-Kontrollen • Beurteilung der Wirksamkeit der Kontrollen	
6.2	**Dokumentation im Bereich der IKS-Prüfung**		
7.	**Umgang mit Feststellungen in der IT-Prüfung**		
7.1	**Alternative Prüfungshandlungen mit IT-Bezug**	Datenanalysen	
7.2	**Bei bedeutsamen Kontrollmängeln**	Kommunikation an die für die Überwachung Verantwortlichen (IDW PS 470 n.F.) bzw. Redepflicht im Prüfungsbericht (IDW PS 450 n.F.)	

Stand: 15.09.2024