

Kontrollrisiko (IKS auf GesamtU-Ebene): Kontrollen im IT-Bereich

AP A-06-04

Grundsatz:

Geregelt

national:

- IDW PS 261 „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“ und
- IDW PH 9.100.1 „Besonderheiten der Abschlussprüfung kleiner und mittelgroßer Unternehmen“

international:

- ISA 315 „Identifizierung und Beurteilung der Risiken wesentlicher falscher Darstellungen aus dem Verstehen der Einheit und ihres Umfelds“.

Der Abschlussprüfer hat sich einen Überblick über die Kontrollaktivitäten der Unternehmensleitung im IT-Bereich zu verschaffen, um festzustellen, ob sie geeignet sind, wesentliche rechnungslegungsrelevante Fehler zu verhindern bzw. aufzudecken und zu korrigieren.

Die für die Aufbauprüfung erforderlichen Informationen zu den Kontrollaktivitäten wird der Prüfer im Wesentlichen durch Gespräche mit der Unternehmensleitung oder den von dieser benannten zuständigen Personen erhalten (Aufbauprüfung).

Ergebnis aus der Checkliste „KMU-Kriterien / Komplexitätsprüfung IT“:

Es liegt ein KMU mit einem wenig komplexen IT-System vor.

Folge:

Der IDW PS 330 i.V.m. IDW PH 9.330.1 ist nicht vollumfänglich abzuarbeiten. Es ist somit ausreichend, wenn die nachfolgenden Fragen beantwortet (Aufbauprüfung) und durch Funktionstests im „Ist“ verifiziert werden.

Beurteilungsgegenstand	Risikobeurteilung	Aufbauprüfung und AP-Verweis	Funktionstests und AP-Verweis
Allgemeines			
<p>Ergeben sich Risiken aus dem Erfordernis eines angemessenen Problembewusstseins bei der Unternehmensleitung und den Mitarbeitern hinsichtlich des IT-Einsatzes?</p> <p>z.B.</p> <ul style="list-style-type: none"> ■ <i>nennenswerte Ausfälle des IT-Systems in der Vergangenheit,</i> ■ <i>unberechtigte Zugriffe auf das IT-System,</i> ■ <i>aufgetretene Schäden aufgrund unzureichender Sicherheitsmaßnahmen.</i> 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>lt. Auskunft Herr Lindenmayer (IT-Leiter), Herr Martin Frey und Herr Mayerhofer gab es in der Vergangenheit keine gravierenden Störfälle</p>	
<p>Ergeben sich Risiken aus der möglichen Abhängigkeit wichtiger Unternehmensaktivitäten von wesentlichen IT-Komponenten?</p>	<p>unbedeutend <input type="checkbox"/></p> <p>gering <input checked="" type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>keine hohe Abhängigkeit, der Betrieb könnte bei einem Totalausfall der EDV noch 1 Woche weiter arbeiten</p>	
<p>Ergeben sich Risiken aus u.U. fehlendem Fachwissen der IT-Anwender und einer evtl. nicht vorhandenen, unterstützenden Dokumentation? Können die IT-Anwender ihre Aufgaben erfüllen und die Programme richtig bedienen?</p> <p><i>Vgl. die entsprechende Frage bei Vorliegen eines KMU und wenig komplexem IT-System gem. IDW PH 9.100.1 (dort Tz. 48).</i></p>	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Herr Lindenmayer ist kompetent</p>	

Beurteilungsgegenstand	Risikobeurteilung	Aufbauprüfung und AP-Verweis	Funktionstests und AP-Verweis
IT-Infrastruktur			
<p>Ergeben sich Risiken aus der Notwendigkeit eines physischen Schutzes sensibler IT-Einrichtungen?</p> <p><i>Vgl. die entsprechende Frage bei Vorliegen eines KMU und wenig komplexem IT-System gem. IDW PH 9.100.1 (dort Tz. 48).</i></p> <p><i>z.B.</i></p> <ul style="list-style-type: none"> ■ bauliche Maßnahmen (Absicherung von Fenster und Türen), ■ Zugangskontrollen (Schlüssel, Codekarten), ■ Feuer- und Wasserschutzmaßnahmen, ■ Maßnahmen zur Sicherung der Stromversorgung, ■ Maßnahmen zur Sicherung vor Einbruch, ■ Maßnahmen zur Sicherung vor Temperaturschwankungen (Klimaanlage). 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Separater Server-Raum mit eigener Kühlung und USV</p>	<p>Der Raum wurde besichtigt, die Schutzvorkehrungen sind ausreichend</p>
<p>Ergeben sich Risiken aus der Notwendigkeit, Verfahren einzuführen, um versuchte oder erfolgte ungenehmigte Zugriffe auf Daten, Programme, Netzwerke und Anwendungen zu überwachen?</p> <p><i>Vgl. die entsprechende Frage bei Vorliegen eines KMU und wenig komplexem IT-System gem. IDW PH 9.100.1 (dort Tz. 48).</i></p> <p><i>z.B.</i></p> <ul style="list-style-type: none"> ■ systembezogene Zugriffskontrollen, ■ anwendungsbezogene Zugriffskontrollen 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Firewall, Zugriffskontrollen sind installiert</p>	<p>Passwortschutz wurde getestet, ok</p>
<p>Ergeben sich Risiken aus der Notwendigkeit regelmäßige Passwortänderungen durchzuführen?</p>	<p>unbedeutend <input type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input checked="" type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Die Passwörter werden nicht regelmäßig geändert</p>	
<p>Ergeben sich Risiken aus dem Erfordernis der regelmäßigen, sachgerechten und nachweislichen Wartung der IT-Komponenten?</p> <p><i>z.B.</i></p> <p><i>für welche IT-Komponenten ist eine Wartung erforderlich?</i></p>	<p>unbedeutend <input type="checkbox"/></p> <p>gering <input checked="" type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Herr Lindenmayer überprüft täglich, ob das System korrekt arbeitet (Versionswechsel auf ifax 9.1 wurde auf Eis gelegt).</p> <p>In 2017/18 wurde auf ein neues Lohnprogramm - CSS eGecko umgestellt</p> <p>Die FiBu soll nun auch auf CSS eGecko umgestellt werden - wird voraussichtlich zum Ende des Geschäftsjahres 2018/19 erfolgen</p>	
<p>Ergeben sich Risiken aus dem i.d.R. notwendigen Erfordernis des Abschlusses von Versicherungen, die die relevanten Risiken im IT-Bereich abdecken?</p> <p><i>z.B.</i></p> <ul style="list-style-type: none"> ■ Betriebsunterbrechung, ■ Sachschäden, ■ Ertragsausfälle. 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Die erforderlichen Versicherungen sind abgeschlossen, BU</p> <p>Haftpflcht Elektro</p> <p>Außerdem existiert eine Versicherung gegen Cyberkriminalität und Datenklau</p>	

Beurteilungsgegenstand	Risikobeurteilung	Aufbauprüfung und AP-Verweis	Funktionstests und AP-Verweis
<p>Ergeben sich Risiken aus der Notwendigkeit Verfahren zu implementieren, die Computerviren vermeiden oder erkennen?</p> <p>z.B.</p> <ul style="list-style-type: none"> werden Virens Scanner eingesetzt? Ist sichergestellt, dass der jeweils aktuellste Stand der Virens Scan-Software auf allen Rechnern implementiert ist? 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	Virenschutz - Virens Scanner, vorhanden	
<p>Ergeben sich Risiken aus dem Erfordernis, Datensicherungsverfahren einzuführen?</p> <p>z.B.</p> <ul style="list-style-type: none"> Mehr-Generationen-Prinzip mit Tages-, Wochen-, Monats- und evtl. Jahressicherungen, Sicherungsmedien (z.B. Bänder, CD-WORM, Platten), angemessene Auslagerungsorte und -intervalle (sind diese feuer- und einbruchssicher?), wer hat Zugang zu den gesicherten Datenbeständen? 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	Datensicherungsverfahren RAID System + tägliche Datensicherung + tägliche Images	
<p>Ergeben sich Risiken aus im Berichtszeitraum stattgefundenen bedeutenden Betriebsausfällen für die Systemsicherheit?</p>	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	Herr Lindenmayer- keine Ausfälle	
<p>Ergeben sich Risiken aus einem möglichen Ausfall des IT-Systems auf die IT-Geschäftsprozesse (Risikoanalyse)?</p> <p>z.B.</p> <ul style="list-style-type: none"> welche wichtigen Unternehmensaktivitäten sind von einem Ausfall betroffen? Welche Vorkehrungen wurden getroffen? Gibt es ein Notfallkonzept: z.B. Ausweichszenarien für die Abwicklung der Kernprozesse u.U auch ohne EDV; Erreichbarkeit von unbedingt erforderlichen Mitarbeitern; Erreichbarkeit von IT-Dienstleistern und Lieferanten; Daten-sicherungs- und Wiederanlaufverfahren? Wurde sichergestellt, dass Eventualpläne vorhanden, aktuell sowie angemessen dokumentiert sind? Wurde sichergestellt, dass diese Pläne regelmäßig getestet werden? Wurden Maßnahmen zur Sicherung der Betriebsbereitschaft getroffen (z.B. Backup Systeme)? 	<p>unbedeutend <input type="checkbox"/></p> <p>gering <input checked="" type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	Bei einem Totalausfall könnte der Betrieb ca. 1 Woche ohne IT weiterarbeiten	
<p>Ergeben sich Risiken aus der Notwendigkeit der jederzeitigen Verfügbarkeit der Daten über die gesamte Aufbewahrungsfrist?</p>	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	keine Risiken ersichtlich	
IT-Anwendungen			
<p>Ergeben sich Risiken aus Notwendigkeit von Kontrollen, die gewährleisten, dass eine vollständige und richtige Erfassung von Geschäftsvorfällen erfolgt?</p>	<p>unbedeutend <input type="checkbox"/></p> <p>gering <input checked="" type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	Systemseitig über fortlaufende Fakturanummern und Belegnummern sichergestellt	

Beurteilungsgegenstand	Risikobeurteilung	Aufbauprüfung und AP-Verweis	Funktionstests und AP-Verweis
<p>Ergeben sich Risiken aus dem Erfordernis programmierter, rechnungslegungsbezogener Verarbeitungsregeln, die die Richtigkeit der Programmabläufe sowie deren sachlogische Richtigkeit gewährleisten?</p> <p>z.B.</p> <ul style="list-style-type: none"> ■ Plausibilitätskontrollen, ■ Summierungen, ■ Saldierungen 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Steuerung der programmierten Verarbeitungsregeln in der FiBu über Belegarten, hierdurch sind die Buchungsmöglichkeiten auf solche beschränkt, die sachgerecht sind.</p>	
<p>Ergeben sich Risiken aus dem Erfordernis, dass die Software-Steuerungsparameter zutreffend eingestellt werden müssen?</p> <p>Vgl. die entsprechende Frage bei Vorliegen eines KMU und wenig komplexem IT-System gem. IDW PH 9.100.1 (dort Tz. 48).</p> <p>z.B.</p> <ul style="list-style-type: none"> ■ Steuerung der Kontenzuordnung, ■ Steuerung der Umsatzkonten / Einrichtung von Automatikkonten 	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Das Programm ist seit vielen Jahren im Einsatz ohne dass die Steuerungsparameter verändert worden sind</p>	<p>Kontrolle erfolgt über die parallele Auswertung der Bilanz und GuV bei der Abschlussprüfung über DATEV</p>
<p>Ergeben sich Risiken aus Änderungen der IT-Anwendungen?</p> <p>z.B.</p> <p>wird gewährleistet, dass nur genehmigte und kontrollierte Änderungen der IT-Anwendungen vorgenommen werden?</p>	<p>unbedeutend <input checked="" type="checkbox"/></p> <p>gering <input type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Herr Lindenmayer: Einführung des neuen Lohnprogramm CSS eGecko, keine Risiken ersichtlich (Standardsoftware und eine kompetente Firma)</p>	
<p>Ergeben sich Risiken aus der Notwendigkeit, die Implementierung von rechnungslegungsrelevanter Software, einschließlich der zur Berücksichtigung unternehmensindividueller Besonderheiten vorgenommenen Anpassungen (Customizing) zu überwachen?</p>	<p>unbedeutend <input type="checkbox"/></p> <p>gering <input checked="" type="checkbox"/></p> <p>hoch <input type="checkbox"/></p> <p>sehr hoch <input type="checkbox"/></p>	<p>Herr Lindenmayer- nur eingeschränkte Möglichkeiten zum Customizing, z.B. Anlage neuer Konten</p> <p>generell ist Customizing nur mit Admin-Rechten möglich</p>	

Ergebnis:

Die Beurteilung des IKS – grundlegende Kontrollen im IT-Bereich führt insgesamt zu dem folgenden - mathematisch ermittelten - inhärenten Risiko und daraus resultierend zu der folgenden Einschätzung:

Risikoprozentsatz: 5,39 %

Das Risiko ist mittel

Ergebnis Prüfer:

Das mathematisch ermittelte Ergebnis stimmt mit der Gesamtbeurteilung des Prüfers überein

☒ Ja
☐ Nein

Folge:

Die Auswirkungen dieses Ergebnisses zeigen sich

- in der Höhe des Fehlerrisikos auf der Gesamtunternehmensebene und - daraus resultierend -
- in der Höhe des festzulegenden Prüfungsrisikos auf der Prüffeldebene.

Ordnerablage: AP A-06-04

bearbeitet von:

Florian Hermann

26.09.2018 fertig bearbeitet ☒

genehmigt von:

Jochen Christoffel

26.09.2018 genehmigt ☐