

Aspekte der IT

Die fünf Komponenten des IKS

IT-PRÜFUNG NACH ISA [DE] 315 (REVISED 2019) - INTEGRATION IN DEN ALLGEMEINEN PRÜFUNGSPROZESS -

Ereignisse, Informationen, Geschäftsvorfälle

- Wie gelangen Informationen über Geschäftsvorfälle und sonstige Ereignisse in das Informationssystem des Unternehmens **hinein**
- Wie werden sie **verarbeitet** (IT-Prozesse / Speicherung)
- Wie werden sie zugänglich gemacht/vermittelt (**Ausfluss**) [Kommunikation/Berichterstattung]?

IT-Anwendungen: Unterstützung bei Erfassung, Verarbeitung, Speicherung, Kommunikation der Daten

Für den betrieblichen Bereich | Für Informationen, die relevant für die Aufstellung des Abschlusses in Übereinstimmung mit den Rechnungslegungsgrundsätzen sind | Für Compliance-Bedürfnisse

IT-Anwendungen:

- Vordefinierte Regeln für Verarbeitung großer Volumen von Geschäftsvorfällen / komplexe Berechnungen für Daten
- Verbesserung von
 - Zeitgerechtigkeit, Verfügbarkeit, Genauigkeit von Informationen und Überwachungsmöglichkeiten
- Erleichtern zusätzliche Analyse von Informationen
- Automatisierte Kontrollen (verlässlicher als manuelle Kontrollen)

Identifikation von relevanten IT-Kontrollen

IT-Kontrolle 1 | IT-Kontrolle 2 | IT-Kontrolle 3

Andere Aspekte der IT-Umgebung

IT-Infrastruktur:

- Datenbank**
Speichern der von IT-Anwendungen genutzten Daten
- Betriebssystem**
Steuerung der Kommunikation zwischen Hardware, IT-Anwendungen und anderer im Netzwerk eingesetzter Software
- Netzwerk**
Für Übertragung/Nutzung von Daten über gemeinsame Kommunikationsverbindung

General controls (Sicherheit)

General controls (Berechtigungen)

Ermittlung Risiken aus dem IT-Einsatz

1 Kontrollumfeld

Übergeordnete Grundlage für Funktion anderer Komponenten; ethische und verhaltensbezogene Standards/Verhaltenskodizes und deren Kommunikation

Verstehen der Kontrollen, Prozesse und Strukturen, wie die Aufsichtsverantwortlichkeiten des Managements vollzogen wurden

Zuordnung von Befugnissen und Verantwortlichkeiten etc.

UND **Beurteilung**, ob das Management eine Kultur von Ehrlichkeit und ethischem Verhalten geschaffen hat und aufrechterhält

das **Kontrollumfeld** eine angemessene Grundlage für die anderen Komponenten des IKS bildet und identifizierte Kontrollmängel die andere Komponenten des IKS der Einheit untergraben

2 Risikobeurteilungsprozess der Einheit

Prozess, wie die Einheit die für Abschluss relevanten Geschäftsrisiken identifiziert, ihre Bedeutsamkeit und Eintrittswahrscheinlichkeit beurteilt und Reaktionen darauf steuert

Verstehen der Prozesse zur Identifizierung von für die RL relevanten Geschäftsrisiken

- Beurteilung der Bedeutsamkeit dieser Risiken (inkl. Eintrittswahrscheinlichkeit)
- Behandlung dieser Risiken

UND **Beurteilung**, ob der **Risikobeurteilungsprozess** der Einheit **angemessen** ist (unter Würdigung der Art und Komplexität der Einheit)

3 Prozess der Einheit zur Überwachung des IKS

Kontinuierlicher Prozess, um Wirksamkeit des IKS zu beurteilen und notwendige Abhilfemaßnahmen zeitgerecht zu ergreifen

Verstehen der Aspekte des Prozesses zur Beurteilung / zur Überwachung der **Wirksamkeit von Kontrollen** und Behebung von identifizierten Kontrollmängeln; interne Revision

Verstehen der **Quellen** der zur Überwachung genutzten Informationen und Grundlagen, warum diese als verlässlich erachtet werden

Beurteilung, ob der Prozess zur Überwachung des IKS angemessen ist (unter Würdigung der Art und Komplexität der Einheit)

4 Informationssystem und Kommunikation

Tätigkeiten und Regelungen und Unterlagen, die implementiert wurden, um Geschäftsvorfälle auszulösen, aufzuzeichnen und zu verarbeiten; deren fehlerhafte Bearbeitung zu entdecken und zu beheben; Kommunikation von einzelnen IKS-Aufgaben und Verantwortlichkeiten

Informationsverarbeitungsprozess:

- Handbücher** zu Unternehmensregeln zum Rechnungswesen und zur Rechnungslegung
- Elektronische oder mündliche Kommunikation**
- Verständnis, über **wechselseitigen Zusammenhang** der Tätigkeit im **Informationssystem**
- Vorgaben zur **Berichterstattung** von Abweichungen an **höheren Hierarchieebenen**
- Informationsqualität beeinflusst Qualität von **Führungsentscheidungen** und verlässliche **Finanzberichterstattung**

Verstehen der **Informationsverarbeitungstätigkeiten** der Einheit, inkl. Ihrer Daten und Informationen, Ressourcen und **Regelungen**, die für bedeutsame Arten von Geschäftsvorfällen, Kontensalden, Abschlussangaben Folgendes definieren:

- Wie** die **Informationen** durch das Informationssystem der Einheit **fließen** (Auslösung von Geschäftsvorfällen, deren Verarbeitung und Aufzeichnung; Informationen über Ereignisse und Umstände, die keine Geschäftsvorfälle sind)
- Die **Unterlagen** des Rechnungswesens, **spezifische Konten** im Abschluss und weitere unterstützende Unterlagen in Bezug auf die Informationsflüsse
- Den angewandten **Rechnungslegungsprozess** zur Aufstellung des Abschlusses
- Die für die oben relevanten Ressourcen, inkl. IT-Umgebung

Beurteilung, ob Informationssystem und die Kommunikation die Aufstellung des Abschlusses in Übereinstimmung mit Rechnungslegungsgrundsätzen angemessen unterstützen.

Kommunikation:

- Auslösen**, Aufzeichnen, Verarbeitung von Geschäftsvorfällen
- Behoben** von **fehlerhafter Verarbeitung** von Daten
- Verarbeitung/Registrierung der **bewussten Außerkräftsetzung** von Systemen/ Umgebung von Kontrollen
- Erfassung und Verarbeitung von Informationen aus Geschäftsvorfällen und **sonstigen Ereignissen**
- Sicherstellung der vollständigen Informationserfassung, -aufzeichnung, -verarbeitung nach maßgebenden Rechnungslegungsgrundsätzen

Verstehen der **Art der Kommunikation** über bedeutsame Sachverhalte, die die Aufstellung des Abschlusses und damit zusammenhängende Berichtspflichten im IT-System unterstützen

5 Kontrollaktivitäten

Manuelle und automatisierte Kontrollen der Informationsverarbeitung; generelle IT-Kontrollen (ob automatisierte Aspekte der Kontrollen funktionieren) z.B. Autorisierung, Genehmigung, Abstimmungen, Verifizierungen, Funktionstrennung, phys. Kontrollen

Identifizieren von folgenden Kontrollen, die die Risiken wesentlicher falscher Aussagen behandeln:

- Kontrollen bezogen auf **bedeutsame Risiken**
- Kontrollen über **Journalbuchungen**
- Kontrollen, für die der Prüfer **plant, die Wirksamkeit** deren Funktion zu **prüfen**, inkl. Kontrollen bezogen auf Risiken, für die aussagebezogene Prüfungshandlungen alleine nicht ausreichend sind
- Andere Kontrollen, die der Prüfer im Rahmen seines **Ermessens** als angemessen erachtet, für ihn hinreichende Prüfungssicherheit zu erlangen

Auf Grund obiger Erkenntnisse: **Identifizierung** von IT-Anwendungen und anderen Aspekten, aus dem IT-Einsatz und Identifizierung für diese:

- Damit verbundene, sich aus dem IT-Einsatz ergebende Risiken und
- die generellen IT-Kontrollen der Einheit, die solche Risiken behandeln

Beurteilung, für jede oben identifizierte Kontrolle:

- Ob die Kontrolle **wirksam ausgestaltet** ist, um Risiken wesentlicher falscher Darstellungen auf Aussageebene zu behandeln oder Funktion anderer Kontrollen zu unterstützen
- Feststellung, ob die Kontrolle **implementiert** wurde, (zusätzlich zur Befragung weitere Prüfungshandlungen)

Implementierung genereller IT-Kontrollen, die abstellen auf das kontinuierliche Funktionieren der automatisierten Aspekte der Kontrollen der IT-Verarbeitung

Autorisierung und Genehmigungen | Abstimmungen | Kontrollen in Komponente Kontrollaktivität | Verifizierungen | Funktionstrennung | Physische oder logische Kontrollen/Sicherungen

Bei Beurteilung jeder der Komponenten liegt evtl. ein KONTROLLMANGEL vor!

Feststellung, dass bestimmte Regelungen der Einheit in einer Komponente **nicht** der Art und den Umständen der Einheit **angemessen** sind

Indikator für Identifizierung eines Kontrollmangels

Nicht bedeutsamer Kontrollmangel

Bedeutsamer Kontrollmangel

Beispiele (A183)

- Dolose Handlungen, in die das obere Management involviert ist
- Identifizierung interner Prozesse, die bzgl. der Berichterstattung und Kommunikation bereits von der internen Revision bemängelt wurden
- Zuvor mitgeteilte Mängel, die vom Management nicht zeitgerecht korrigiert wurden
- Versäumnis des Managements, auf bedeutsame Risiken zu reagieren
- Anpassung eines zuvor herausgegebenen Abschlusses

Würdigung bei Planung weiterer Prüfungshandlungen (ISA [DE] 330)

Stand: 04.10.2023

3/2 Zusammenwirken von IKS-Prüfung und IT-Prüfung [zu Schritt 1 von 10]