					Index/Ablage:
	Zielgruppe:		Hz. 1: Müller	Hz. 2:	Seite:
Mandant: **Halkit GmbH**		Prüffeld: **[Beispielhaftes Arbeitspapier]**		Anwendung: Stand: 28.03.2024 Version: Datum der Bearbeitung:	

Modellhafte Darstellung der Verständnisgewinnung über die IT-Anwendungen [Wichtiger Bestandteil von Schritt 2][1]
Beispiel für generelle IT-Kontrollen (ITGC) als Reaktion auf Risiken aus dem IT-Einsatz (RAIT)

Hinweis: Vom Prüfer individuell zu beschreiben, hier beispielhafte Formulierungen / Dokumentationen

	Risiken aus dem IT-Einsatz	Generelle IT-Kontrollen	in Ordnung		nicht in Ordnung		Verweis auf andere AP
			zutreffend	n.a.	fehlend	unzutreffend	
IT-Prozess: Zugangsverwaltung	Nutzer haben **Zugriffsberechtigungen**, die **über die zur Erfüllung ihrer zugewiesenen Aufgaben notwendigen hinausgehen** (Funktionstrennung mglw. Unsachgemäß)	• ***Management genehmigt*** *Art und Umfang der Zugriffsberechtigungen und geänderte Nutzerzugriffe; incl. Standardanwenderprofile/-rollen* • ***Zugriff für ausgeschiedene*** *oder versetzte Nutzer wird* ***zeitgerecht gelöscht*** *oder geändert* • ***Nutzerzugriff*** *wird regelmäßig* ***überprüft*** • *Funktionstrennung wird überwacht und entgegenstehender Zugang wird entfernt oder entgegenwirkenden (automatisierter) Kontrollen zugeordnet (dokumentiert und geprüft)* • *Zugriffe auf der* ***Berechtigungsebene*** *(z.B. Konfigurations-, Daten- und Sicherheitsadministratoren)* ***sind autorisiert*** *und entsprechend* ***eingeschränkt***	☑				AP 6.5
	Unmittelbarer Datenzugriff: Unangemessene Änderungen werden direkt an Finanzdaten auf andere Weise als Anwendungstransaktionen vorgenommen	***Zugriff auf Anwendungsdaten-Dateien*** *oder Datenbankobjekte/-tabellen/-daten ist auf* ***befugtes Personal beschränkt*** *und dieser Zugriff ist vom Management* ***genehmigt****.*	☑				AP 6.6
	Systemeinstellungen: Systeme sind nicht angemessen konfiguriert und aktualisiert, um den Systemzugriff auf ordnungsgemäß befugte und geeignete Nutzer zu beschränken	• *Zugriff ist über* ***individuelle Nutzerkennung*** *und Kennwörter oder* ***anderer Methoden*** *authentifiziert als ein Mechanismus zur Bestätigung,* ***dass Nutzer befugt*** *sind.* • *Kennwortparameter entsprechen den Unternehmens- und Branchenstandards (z.B. Mindestlänge und -komplexität des Kennworts; Zeitablauf; Kontosperrung)* • *Die wichtigsten* ***Merkmale der Sicherheitskonfiguration*** *sind ordnungsgemäß implementiert*	☑				AP 6.7
Change-Management	**Anwendungsänderungen**: Unangemessene Änderungen werden an Anwendungssystemen oder -programmen vorgenommen, die relevante automatisierte Kontrollen beinhalten	• ***Änderungen an Anwendungen*** *werden ordnungsgemäß getestet und genehmigt, bevor sie ins Produktivsystem übertragen werden* • ***Zugang****, um Änderungen in der Produktionsumgebung der Anwendung zu implementieren, ist* ***entsprechend beschränkt*** *und von der Entwicklungsumgebung getrennt*	☑				AP 7.1
	Änderungen an Datenbanken: Unangemessene Änderungen an Datenbankstruktur und an Beziehungen zwischen den Daten werden vorgenommen	***Änderungen an Datenbanken*** *werden* ***ordnungsgemäß*** *geprüft und genehmigt, bevor sie in die Produktionsumgebung übertragen werden*	☑				AP 7.2
	Änderungen an Systemsoftware: Unangemessene Änderungen an z.B. Betriebssystem, Netzwerk, Change-Management-Software, Software für Zugriffskontrolle	***Systemsoftwareänderungen*** *werden ordnungsgemäß geprüft und genehmigt, bevor sie für die Produktion übertragen werden*	☑				AP 7.3
	Datenkonvertierung: Aus Altsystemen oder früheren Versionen konvertierte Daten führen zu Datenfehlern, wenn bei der Konvertierung unvollständige, redundante, veraltete oder fehlerhafte Daten übertragen werden	*Management* ***genehmigt das Ergebnis der Konvertierung von Daten*** *(z.B. Abgleichs- und Abstimmungsaktivitäten) aus dem alten Anwendungssystem oder der alten Datenstruktur* ***und überwacht Einhaltung*** *von* ***eingerichteten Konvertierungsregelungen und -maßnahmen***	☑				AP 7.4
		Zusammenfassende Prüfungsfeststellung:	☑				

Prüfungsfeststellung:

Den zuvor identifizierten **Risiken aus dem Einsatz der IT**, die für die Rechnungslegungsdaten relevant sind, wird mit den generellen IT-Kontrollen insbesondere im Bereich der **Zugangsverwaltung und Change-Management**, ausreichend und angemessen begegnet. Sie stellen sicher, dass die installierten Prozesse gewährleisten, dass nur gewollte Berechtigungen für den Zugang zu den rechnungslegungsrelevanten IT-Systemen vergeben und keine unautorisierten Veränderungen an den IT-Systemen vorgenommen werden.
Damit kann der Prüfer im weiteren Prüfungsverlauf in **Stichproben den Prozess prüfen**. Er kann bspw. Einen **Walk-Through** durch den Prozess der Anwendungsänderungen durchführen.

Als Ergebnis der Aufbauprüfung (Angemessenheit und Vorhandensein von IT-bezogenem IKS) kann der Prüfer **vorläufig** die **Wirksamkeit des IT-Systems inkl. des Umfangs der IT-bezogenen Risiken beurteilen.** Die **Funktionsprüfung** im Anschluss dient dann der Beurteilung, **ob die ITGC** den Risiken aus dem Einsatz der IT begegnen und sich der Abschlussprüfer auf die **Datenintegrität verlassen** und sich **auf die automatisierten Kontrollen und Reports verlassen** kann.

[1] Auszug aus ISA [DE] 315 (Revised 2019) Anlage 6.