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

09/2024

Risiken aus dem IT-Einsatz		Generelle IT-Kontrollen	IT-Anwendungen			in Ordnung		nicht in Ordnung		Verweis auf andere AP
			Nicht komplexe Standard-Software	Mittelgroße und mäßig komplexe Software	Große oder komplexe IT-Anwendungen	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*	Ja	Ja	Ja					
		• ***Zugriff für ausgeschiedene*** *oder versetzte Nutzer wird* ***zeitgerecht gelöscht*** *oder geändert*	Ja	Ja	Ja					
		• ***Nutzerzugriff*** *wird regelmäßig* ***überprüft***	Ja	Ja	Ja					
		• *Funktionstrennung wird überwacht und entgegenstehender Zugang wird entfernt oder entgegenwirkenden (automatisierter) Kontrollen zugeordnet (dokumentiert und geprüft)*	N.a.	Ja	Ja					
		• *Zugriffe auf der* ***Berechtigungsebene*** *(z.B. Konfigurations-, Daten- und Sicherheitsadministratoren)* ***sind autorisiert*** *und entsprechend* ***eingeschränkt***	Ja (IT-Anwendungsebene)	Ja (IT-Anwendung u. best. Ebenen IT-Umgebung)	Ja (sämtliche Ebenen der IT-Umgebung)					
	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****.*	N.a.	Ja (für bestimmte Anw.)	Ja					
	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.*	Ja	Ja (für best. Anw)	Ja					
		• ***Kennwortparameter*** *entsprechen den* ***Unternehmens- und Branchenstandards*** *(z.B. Mindestlänge und -komplexität des Kennworts; Ablauf des Kennworts; Kontosperrung)*	Ja – nur Kennwort-authentifizierung	Ja – Mischung aus Kennwrot und Multi-Faktor-Authentifizierung	Ja					
		• *Die wichtigsten* ***Merkmale der Sicherheitskonfiguration*** *sind ordnungsgemäß implementiert*	n.a.	Ja (für best. Anwe.)	Ja					
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*	n.a.	Ja – für Nicht-Standard-Software	Ja					
		• ***Zugang****, um Änderungen in der Produktionsumgebung der Anwendung zu implementieren, ist* ***entsprechend beschränkt*** *und* ***von der Entwicklungsumgebung getrennt***	n.a.	Ja, für Nicht-Standard-Software	Ja					
	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*	n.a.	Ja, für Nicht-Standard-Software	Ja					
	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*	n.a.	Ja	Ja					

	Risiken aus dem IT-Einsatz	Generelle IT-Kontrollen	IT-Anwendungen: Nicht komplexe Standard-Software	IT-Anwendungen: Mittelgroße und mäßig komplexe Software	IT-Anwendungen: Große oder komplexe IT-Anwendungen	in Ordnung: zutreffend	in Ordnung: n.a.	nicht in Ordnung: fehlend	nicht in Ordnung: unzutreffend	Verweis auf andere AP
	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***	n.a.	Ja	Ja					
IT-Betrieb	**Netzwerk:** Das Netzwerk verhindert nicht ausreichend, dass **unberechtigte** Nutzer unangemessen **Zugriff auf Informationssysteme** erhalten	*Zugriff ist **über individuelle Nutzerkennung und Kennwörter** oder **andere Methoden** authentifiziert als ein Mechanismus **zur Bestätigung, dass Nutzer befugt** sind, Zugriff auf das System zu erlangen. **Kennwortparameter** entsprechen den Unternehmens- oder Berufsstandregelungen und -standards (z.B. Mindestlänge und -komplexität des Kennworts, Ablauf des Kennworts, Kontosperrung)*	n.a.	Ja	Ja					
		*Das Netzwerk ist **so gestaltet**, dass **webbasierte Anwendungen getrennt** sind vom **internen** Netzwerk, wo Anwendungen zugegriffen wird**, die für interne Kontrollen über die Finanzberichterstattung relevant** sind.*	n.a.	Ja (mit Ermessen)	Ja (mit Ermessen)					
		*In regelmäßigen Abständen führt das Netzwerk-Managementteam **Schwachstellenscans der Netzwerkumgebung** durch und untersucht ebenfalls **potenzielle Schwachstellen**.*	n.a.	Ja (mit Ermessen)	Ja (mit Ermessen)					
		Kontrollen** werden implementiert, um den **Virtual Private Network (VPN)-Zugang** auf **autorisierte und geeignete Nutzer zu beschränken.	n.a.	Ja (mit Ermessen)	Ja (mit Ermessen)					
	Daten-Back-up und -wiederherstellung: Finanzdaten können **bei einem Datenverlust nicht zeitgerecht wiederhergestellt** oder **abgerufen** werden.	***Finanzdaten** werden **regelmäßig** nach einem **festgelegten Zeitplan** und in einer festgelegten **Häufigkeit** gesichert.*	n.a. (manuelle Backups)	Ja	Ja					
	Job-Steuerung: Produktionssysteme, -programme oder -jobs führen zu einer **ungenauen, unvollständigen oder unautorisierten Verarbeitung** von Daten	*Nur autorisierte Nutzer haben Zugriff, um Batch-Jobs (einschließlich Schnittstellen-Jobs) in der Job-Steuerungssoftware zu aktualisieren*	n.a.	Ja (für best. Anwendungen)	Ja					
		***Kritische Systeme**, Programme oder Jobs werden **überwacht** und Verarbeitungsfehler werden **korrigiert**, um eine erfolgreiche Fertigstellung sicherzustellen*	n.a.	Ja (für best. Anwendungen)	Ja					
	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.