IT-Prüfung im Rahmen der Jahresabschlussprüfung

Die Liste enthält jeweils eine Grundfrage zur jeweiligen Anforderung sowie Beispiele für mögliche Nachweise. Welche davon für die Abbildung Ihres IT-Systems am besten geeignet, oder ob andere Nachweise zutreffender sind, hängt letztlich von den Gegebenheiten in Ihrem Unternehmen ab.

A – Allgemeine IT-Risiken	
Anforderung	**Dokumentation/Beispiel(e)**
1. Überblick über das IT-System	Liste der eingesetzten Software (i.W. mit Bezug zum ERP-System, Archivsystem), aktuelle Netzwerkübersicht
2. IT-Richtlinien	Sicherheitsrichtlinien, IT-Strategie, Arbeits- und Dienstanweisungen mit IT-Bezug
3. Schulungen	Nachweise über Datenschutz- und IT-Sicherheitsschulungen

B – Risiken des Datenverlustes (RIT01)	
Anforderung	**Dokumentation/Beispiel(e)**
1. Datensicherung und Datenwiederherstellung (KIT01)	*Wie ist die Datensicherung konzipiert und wie wird sie umgesetzt?* Backupkonzept, Protokolle, Screenshots oder E-Mails, die erfolgreiche Datensicherungen belegen; Nachweise über die Auslagerung von Backups, z. B. Verträge mit Cloud-Anbietern oder Dokumentation über physische Sicherungsmedien
2. Sicherheitsmaßnahmen IT-Infrastruktur (KIT06)	*Wie werden die Server vor Schäden und unbefugtem Zugriff geschützt?* Fotos von Serverräumen (Zutrittsschutz Serverräume und -schränke, Klimaanlagen, Rauchmelder)

C – Risiken der Datenmanipulation (RIT02)	
Anforderung	**Dokumentation/Beispiel(e)**
1. Zugriffsschutz (KIT02)	*Besteht eine dokumentierte Passwortrichtlinie und wie ist diese in Windows/im ERP-System umgesetzt?* Passwortrichtlinien (dokumentierte Vorgaben und systemseitige Einstellungen – Screenshot Passwortrestriktionen Windows Domäne und ERP-System)
2. Berechtigungskonzept (KIT03)	*Welche Berechtigungen sind eingerichtet und wie sind die Verantwortlichkeiten zur Anlage/Änderung/Löschung verteilt?* Übersicht der Benutzerrollen und zugehörigen Berechtigungen (z. B. Screenshots aus dem ERP-System), Berechtigungen für elektronische Prozesse im Bereich Auftragsvergabe und Rechnungsprüfungs- und -freigabeverfahren (Zuordnung Mitarbeiter zu Prozessschritten) sowie Zahlungsverkehr; Dokumentation zur Vergabe, Änderung und Entzug von Zugriffsrechten (z. B. bei Mitarbeiterwechsel), Nachweis einer durchgeführten Berechtigungsinventur
3. Einschaltung der systemseitigen Stammdatenänderungs-protokollierung (KIT04)	*Welche Protokollierungen werden mit dem ERP-System durchgeführt?* Systemseitige Protokollierung von Veränderungen bspw. bei Geschäftspartnern wie Kreditoren, Mietern, oder Anlage von FIBU-Konten. Screenshots eines Stammdatenänderungsprotokolls (Änderungshistorie eines Stammdatensatzes wie z.B. Mietvertrag im ERP-System).

D – Risiken falscher Datenverarbeitung (RIT03)	
Anforderung	**Dokumentation/Beispiel(e)**
1. Update-Prozess (KIT05)	*Welche wesentlichen Updates/Änderungen der eingesetzten Software wurden vorgenommen?* Änderungsprotokolle oder Dokumentation wesentlicher Updates im Berichtsjahr, z.B. Screenshots der eingesetzten Versionsstände des ERP-Systems (vor allem bei In-house-Software), elektr. Archiv, Windows
2. Sicherheitsmaßnahme Netzwerk (KIT07)	*Welche Maßnahmen zur Netzwerksicherheit sind konzipiert und angewendet?* Screenshots der aktuellen Version von Firewall und Virenschutz, Art der Verschlüsselung der VPN-Verbindung bei externem Zugriff durch Dienstleister, Art der Verschlüsselung von mobilen Endgeräten, Verwendung eines Mobile Device Managements (MDM), Screenshots vom Monitoring der IT-Systeme
3. Überprüfung Datenverarbeitung und Datenübernahme (KIT08)	*Welche Schnittstellen bestehen zum ERP-System und wie wird die korrekte Übernahme der Daten kontrolliert? Welche automatisierten Prüfungen des ERP-Systems bestehen und werden verwendet?* Nachweis über integrierte Kontrollsysteme wie Plausibilitätsprüfungen oder Fehlerprotokolle (bspw. Sollstellung, Lastschriftlauf, Erstellung Beko-Abrechnung, Mussfeld-Vorgaben im Anlagevermögen) und Dokumentation dieser. Vier-Augen-Prüfung bei Stammdatenänderungen (bspw. Kreditoren), Screenshots einer Freigabemaske Verarbeitungsprotokolle und Schnittstellenprotokolle, vor allem bei Einsatz von weiteren Drittsystemen in Verbindung mit ERP-System (bspw. Handwerkerkopplung)
4. Notfallplan (KIT09)	*Welches Vorgehen ist bei IT-Notfällen dokumentiert?* Dokumentation der durchzuführenden Maßnahmen und Ansprechpartner im Falle eines IT-Notfalls, Protokolle über Tests des Notfallplans, z.B. Datenwiederherstellungen

E – Mit (IT-) Prozessen verbundene Risiken	
Anforderung	**Dokumentation/Beispiel(e)**
Dokumentation/Beschreibung von elektronischen Workflows	*Welche elektronischen Workflows sind eingerichtet und dokumentiert?* - Elektronische Archivierung - Elektronische Auftragsvergabe - Elektronisches Rechnungsprüfungs- und Freigabeverfahren inkl. Zahlungsfreigabe, Beispieldokumentation in Form von Screenshots