Ermittlung von Risiken aus dem Einsatz der IT

Stufe 6

09/2024

Analyse der IT-Infrastruktur notwendig (Beispielsweise)	
1. IT-Infrastruktur	
• Physische Sicherungsmaßnahmen • Logische Zugriffskontrollen • Datensicherungs- und auslagerungsverfahren • Maßnahmen für Regelbetrieb und Notbetrieb • Maßnahmen zur Sicherung der Betriebsbereitschaft	
2. Berechtigungskonzept	
Berechtigungen in den Anwendungen = **automatisierte Kontrollen** **Ziel**: **Sicherstellung** durch Verfahren und Regelungen, dass **nur gewollte Berechtigungen** vergeben werden und im Unternehmen vorhanden sind. **Aufnahme der organisatorischen Verfahren** zur • Beantragung • Genehmigung • Einrichtung • von Berechtigungen zum Zugang von IT-Systemen	Prozess zur Berechtigungsvergabe prüfen (Antrag, Vergabe von Zugriffsrechten) **Beachte**: **Nicht** die Berechtigung **in den** Geschäftsprozessen!
	Prozess der Rollendefinition mit Freigabe durch die Fachabteilungen (in komplexeren EDV-Systemen werden für einzelne Anwendergruppen „Rollen" mit den speziellen Zugriffsrechten definiert, die für das rollenspezifische Aufgabenfeld benötigt werden)
	Prozess **des Entzugs von Berechtigungen** beim Wechsel von Mitarbeitern in andere Abteilungen oder beim Ausscheiden aus dem Unternehmen **Risiko**: Trainee-Berechtigungen sind oft sehr umfassend, da viele unterschiedliche Abteilungen mit immer neuen Systemrechten durchlaufen werden
	Soll-Konzept für die Berechtigungen für die Prozesse
Festgestellte **Mängel** z.B. keine Funktionstrennung	**RAIT** liegt vor (fehlerhafte, unautorisierte Zugriffe auf Daten/Datenbank kann Integrität der Daten gefährden)
Folgen für Abschlussprüfung	**Alternative Prüfungshandlungen (Datenanalysen)** mit dem Ziel, festzustellen, ob die Mängel im IKS sich **ausgewirkt** hat (ggf. **kein Verlass auf IT-Anwendungskontrollen** und damit Ausweitung der aussagebezogenen Prüfungshandlungen)

Stand: 15.09.2024

3. Change-Management	
Veränderungen an den IT-Anwendungssystemen erfolgen in immer **kürzeren Intervallen** **Ziel**: **Sicherstellung**, dass Regelungen zur Änderung bzw. Erweiterung von vorhandenen IT-Anwendungen und deren Dokumentation existieren. Nur dadurch kann der Abschlussprüfer davon ausgehen, dass die Geschäftsprozesse entsprechend den **definierten und bekannten Abläufen** durch die EDV abgebildet werden.	Prozess für **Antragstellung und Genehmigung** von Veränderungen an Software und EDV-Systemen
	Vorgaben für die **Durchführung von Tests** in eigenen Testumgebungen, bevor Änderungen im Produktivsystem aktiviert werden und müssen diese **dokumentiert** werden **Problem**: nur **unzureichend dokumentierte Prozesse** bei den Systemanpassungen – Änderungen nur bedingt nachvollziehbar
	Vorgaben für die **Entwicklung neuer Software** (insbesondere Genehmigungsverfahren und Funktionstrennung) Vorgaben für **Updates und Notfallmaßnahmen**
	Nicht: **Migration**, Einführung **neuer** Rechnungslegungssysteme
4. Datensicherungs- und Auslagerungsverfahren	
Ziel: **Sicherstellung** der **fortlaufenden Betriebsbereitschaft** für den Fall eines versehentlich oder vorsätzlich herbeigeführten **Datenverlustes**	Verfahren, die ein Lesbarmachen von Daten wieder ermöglich
	Angemessenes **Datensicherungsverfahren** (z.B. Mehr-Generationen-Prinzip mit Tages-, Wochen-, Monatssicherungen) mit Sicherungsmedien, Auslagerungsorten und -Intervallen
Festgestellte **Mängel** **Folgen** für Abschlussprüfung	**RAIT** liegt vor (wenn Schwachstellen im Notbetrieb von IT-Anwendungen auftreten. Risiko, dass Integrität der Daten mangels Wiederherstellungsmöglichkeit nicht mehr gegeben ist) **Alternative Prüfungshandlungen (Datenanalysen)** mit dem Ziel, festzustellen, ob die Mängel im IKS sich **ausgewirkt** hat (falls es im abgelaufenen Geschäftsjahr nicht zu einem Datenverlust gekommen ist, liegt dennoch ggf. eine **Schwäche im IKS** vor mit der Pflicht, ggf. darüber zu berichten)
5. IT-Betrieb: Netzwerksicherheit	
Ziel: **Sicherstellung** der Datenintegrität und Schutz vor Angriffen aus dem Internet (v.a. Bedeutung durch zunehmendes Home-Office der Mitarbeiter)	Einbringung von VPN-Verbindungen
	Maßnahmen für stärkerer Sicherheitsbewusstsein der Mitarbeiter (z.B. Schulungen)
Festgestellte **Mängel**	**RAIT** liegt vor (wenn Cyberangriff von außen erfolgreich war, besteht ein Risiko für die Datenintegrität)
Folgen für Abschlussprüfung	**Alternative Prüfungshandlungen (Datenanalysen)** mit dem Ziel, festzustellen, ob die Mängel im IKS sich **ausgewirkt** hat (falls es im abgelaufenen Geschäftsjahr nicht zu einem Angriff von außen und zur Verschlüsselung von Daten gekommen ist, kann dennoch eine berichtspflichtige **Schwäche im IKS** vorliegen)

Stand: 15.09.2024