# Checkliste: Prüfung der Zugriffskontrolle

| Anforderungen | Erfüllt | Nicht erfüllt |
| --- | --- | --- |
| Organisatorische Voraussetzungen (Organigramm, Stellenbeschreibungen, Aufgabenbeschreibungen) vorhanden |[ ] [ ]
| Organigramm, Stellenbeschreibungen, Aufgabenbeschreibungen werden regelmäßig aktualisiert und in Rollendefinitionen umgesetzt |[ ] [ ]
| Rollendefinition entspricht Need-to-know-Prinzip |[ ] [ ]
| Nutzerinnen und Nutzern werden Rollen zugeordnet |[ ] [ ]
| Rollenzuordnung wird regelmäßig überprüft (Wiedervorlage) |[ ] [ ]
| Rollenkonflikte werden bei der Rollenzuordnung beachtet |[ ] [ ]
| Rollenzuordnungen bei Projekten werden zeitlich befristet |[ ] [ ]
| Ausscheidende Mitarbeiter werden von ihren Rollen getrennt |[ ] [ ]
| Rollenprüfung nutzt Module/Tools der IAM-Lösung (Identity and Access Management) |[ ] [ ]
| Warnungen des „Rollenprüfers“ werden überprüft |[ ] [ ]
| „Rollenprüfer“-Software wird durch manuelle Stichproben ergänzt |[ ] [ ]
| Zero-Trust-Konzept wird umgesetzt (Zugriffe werden risikoabhängig erteilt, es gibt kein Anfangsvertrauen – auch nicht für interne Nutzende, Geräte oder Standorte) |[ ] [ ]