/ MAURISEC.DE

FIELD NOTES / CHECKLIST 03

Privilegierte Zugriffe: PIM mit belastbaren Grenzen

PRUEFEN. BELEGEN. NACHHALTEN.

Für Entra-Rollen und, ausdrücklich getrennt, Azure-Ressourcenrollen. PIM-Verfügbarkeit, Lizenzbedarf und administrative Befugnisse vorab prüfen. Aktive Notfallberechtigungen vor jeder Umstellung sichern. Quellenstand: 09.11.2026.

Pruefbereich / Team:

Datum:

- [ ] **01 / Aktive und aktivierbare Rollenzuweisungen einschließlich Geltungsbereich und verantwortlicher Person erfassen.**

  Nachweis: Datierter Rollenexport; Entra- und Azure-Rollen getrennt gekennzeichnet.

- [ ] **02 / Für reguläre Administration die kleinste geeignete Rolle statt pauschaler Global-Administrator-Rechte wählen.**

  Nachweis: Aufgaben-Rollen-Zuordnung mit nachvollziehbarer Begründung.

- [ ] **03 / Dauerhaft aktive menschliche Berechtigungen soweit möglich durch zeitlich begrenzte Aktivierung ersetzen.**

  Nachweis: Zuweisungsart und Befristung; begründete Ausnahmen separat dokumentiert.

- [ ] **04 / Aktivierungsdauer, Begründung, Benachrichtigung und bei Bedarf Genehmigung pro Rolle konfigurieren.**

  Nachweis: Rollenrichtlinie und funktionierender Aktivierungstest.

- [ ] **05 / Genehmigende Personen und ihre Vertretung testen; zirkuläre Abhängigkeiten beim Notfallzugriff vermeiden.**

  Nachweis: Genehmigungsprotokoll und getesteter Ausfall- beziehungsweise Vertretungsfall.

/ MAURISEC.DE

FIELD NOTES / CHECKLIST 03

- [ ] **06 / MFA beziehungsweise einen passenden Authentifizierungskontext für die Aktivierung festlegen und prüfen.**

  Nachweis: Aktivierungsereignis und tatsächlich erfüllte Authentifizierungsbedingungen.

- [ ] **07 / Anforderungen an die spätere Nutzung privilegierter Rechte zusätzlich zur Aktivierung absichern.**

  Nachweis: Test mit zulässigem und unzulässigem Gerät oder Anmeldekontext nach Aktivierung.

- [ ] **08 / Rollenzuweisungen regelmäßig überprüfen und Entscheidungen einschließlich Entzug nachverfolgen.**

  Nachweis: Abgeschlossene Access Reviews, Genehmigungen und tatsächlich entfernte Zuweisungen.

- [ ] **09 / Aktivierung, Rollenänderung und Notfallnutzung überwachen und auf einen Reaktionsweg führen.**

  Nachweis: Audit-Auszug, Testalarm und benannte Bereitschaft beziehungsweise Zuständigkeit.

GEGENPROBE / AUTORISIERTE TESTUMGEBUNG

Mit einem Testkonto die Aktivierung und die spätere Rollenaktion getrennt prüfen; erwartete Grenzen und verbleibende Sitzungen protokollieren.

GRENZEN UND VORAUSSETZUNGEN

Notfallkonten benötigen nach Microsoft-Vorgabe dauerhaft aktive Global-Administrator-Zuweisungen statt ausschließlich genehmigungspflichtiger Aktivierbarkeit. MFA bei Aktivierung verlangt nicht zwangsläufig einen neuen Prompt. Ein Aktivierungskontext allein beschränkt nicht jede anschließende Rollennutzung. Dienstprinzipale lassen sich nicht wie Benutzer als eligible zuweisen. Entra- und Azure-Rollenrichtlinien sind getrennt zu prüfen.

PRIMAERQUELLEN / STAND 09.11.2026

Microsoft Learn: Plan PIM deployment
learn.microsoft.com

Microsoft Learn: Configure Entra role settings in PIM
learn.microsoft.com

Microsoft Learn: Configure Azure resource role settings
learn.microsoft.com

Microsoft Learn: Create privileged access reviews
learn.microsoft.com

Microsoft Learn: Security operations for privileged accounts
learn.microsoft.com