Access Management & User Lifecycle – Executive Summary (One Page)

Date: 2026-01-19 | System: Shahin AI GRC | Scope: User creation, role assignment, and access reviews

Purpose

Provide leadership/auditors a concise view of how the platform enforces controlled user onboarding, role assignment, and periodic access review, and where audit evidence is produced.

In-Scope User Creation Paths

- **Self-Registration** (POST /api/auth/register): creates user; access after verification/password set.
- **Trial Signup** (POST /api/trial/signup): creates trial record (no user).
- **Trial Provision** (POST /api/trial/provision): creates tenant + tenant admin user; immediate access.
- **Admin Invite** (POST /api/tenants/{tenantId}/users/invite): creates invitation; user activates via accept.
- **Invitation Accept** (POST /api/invitation/accept): creates user + assigns role; activates access.

Audit Evidence Model

For each access-management action, emit immutable audit events capturing actor, tenant, target user, role changes, timestamps, and request correlation identifiers. These events support AM control testing and can be reconciled to application logs and database records.

Process	Primary Evidence (Audit Events)
User registered	AM01_USER_CREATED, AM01_USER_REGISTERED
Trial signup initiated	AM01_TRIAL_SIGNUP_INITIATED
Tenant & admin provisioned	AM01_TENANT_CREATED, AM01_USER_CREATED, AM03_ROLE_ASSIGNED
User invited	AM01_USER_INVITED
Invitation accepted	AM01_USER_CREATED, AM03_ROLE_ASSIGNED
Access review (planned)	AM04_ACCESS_REVIEW_CREATED, AM04_ACCESS_REVIEW_COMPLETED, AM0

Access Reviews (Next Practical Build Item)

Implement Access Review tables (EF migration), optional API endpoints, and a scheduled background job to detect overdue reviews and send reminders. This closes the gap between role assignment events (AM03) and periodic certification (AM04).

Key Risks / Assumptions

- Audit event taxonomy must be finalized and enforced consistently across services/controllers.
- Background processing should use Hangfire (current approach) if ABP background workers remain disabled.
- Evidence retention and tamper-resistance controls must be defined (log retention, DB backups, access controls).