Access review

Review business need, privilege combinations and evidence of removal together.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

Human accounts, local application roles, cloud groups and external users. Use the non-human identity pack for service identities. Examples are fictional; do not upload real identities or passwords.

Process and expected evidence

1. Validate the population

Source system, snapshot date, record count and coverage gaps.

2. Assign business ownership

Role description and named decision owner.

3. Review combined privileges

Separation-of-duties analysis and rationale.

4. Record the decision

Decision, rationale, approver and exception expiry.

5. Apply the change

Implementation ticket and post-change output.

6. Verify closure

Retest result and outstanding actions.

Work record

Scope / date:
Business / technical owner:
Decision and rationale:
Evidence reference / retest:

Example and closure

Fictional example; not evidence of actual work.

Record ID: ACC-001

Account / role: Example ERP / payment approval

Business rationale: No longer needed after role change

Business owner: Finance process owner

Decision: Remove

Exception expiry: No exception

Evidence / ticket: Fictional CHG-017 and role output

Closure test: Group and direct role removed; retested

Closure checklist

[ ] Population sources and snapshot date verified.

[ ] Owner and separation of duties checked.

[ ] Removal or exception decision is justified.

[ ] Implementation and retest records exist.

Official sources

CISA / NSA — Identity and Access Management

https://www.cisa.gov/sites/default/files/2023-12/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.pdf

NIST Cybersecurity Framework 2.0

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final