DEEP INFOSEC / ENGINEERING ACCOUNT

Identity controls that survive real operational complexity

During a cloud or application transformation, staff identities, service accounts and privileged roles cross multiple directories and environments. An apparently correct access policy can fail when groups, provisioning jobs and application permissions diverge.

We map the identity lifecycle, federation and provisioning paths, and the application’s actual authorization logic. Our engineers test joiner/mover/leaver flows, role exclusions, emergency access and audit trails, then implement corrections alongside the owning teams.

Start with the real identity lifecycle

A regulated application estate may contain a central identity provider, local directories, cloud accounts and applications with independent role models. New joiners, staff movements and departures can leave a different access state in each system. The review follows an identity from its authoritative source to every downstream permission it obtains.

Test the federation and provisioning boundaries

Architects document federation trusts, SSO claims, SCIM provisioning, group-to-role mappings and service-account ownership. Tests cover initial access, role changes, conflicting privileges, deprovisioning, retry behaviour, and what happens when one downstream system returns an unexpected status or remains temporarily unavailable.

Restore one accountable entitlement model

Business roles and sensitive responsibilities are related to explicit application privileges, with mutually exclusive roles where required. Changes to identity providers, synchronization jobs and legacy adapters follow the operator’s change authority, with recorded exception paths, idempotent reconciliation and rollback criteria.

Prove removal and maintainability

The final test confirms that revoked access is removed at both the identity-provider level and within downstream applications. The customer receives an entitlement matrix, integration contracts, exception register, test records and instructions to monitor and maintain the flow without relying on individual engineers.

Acceptance and handover

The customer receives a role and entitlement matrix, federation and SCIM integration specification, exception register, deployment and rollback plan, and repeatable evidence that permissions are enforced.

For a scoped assessment contact sales.advisor@deepinfosec.com.