
FREE STARTER TOOLKIT / IDENTITY AND ACCESS

IAM Governance Checklist

Review who has access, why they need it and who owns the decision.

01

Ownership and approvals

Identify a system or data owner. Require documented approval before granting access. Record the request, business reason, approver and assigned role.

02

Least privilege and conflicting duties

Grant only the access needed for the role. Check combinations that could allow one person to initiate and approve a sensitive transaction. Document approved exceptions and review dates.

03

Joiners, movers and leavers

Link account changes to authorised personnel events. Remove old permissions when roles change. Disable departing users promptly under your policy and retain completion evidence.

04

Privileged and non-human accounts

Inventory administrator, service and emergency accounts. Assign owners, protect credentials, apply appropriate authentication and review use. Avoid shared accounts where individual accountability is required.

FREE STARTER TOOLKIT / IDENTITY AND ACCESS

IAM Governance Checklist

Review who has access, why they need it and who owns the decision.

05 Periodic access reviews

Give reviewers identity, role, privileges, employment status and business need. Record keep, modify or remove decisions with reasons. Track removals and changes to completion.

06 Monitoring and evidence

Review unusual access and privileged activity. Preserve dated approvals, review decisions, revocation evidence and exception records according to policy. Assign an owner to every unresolved action.

07 Record your next action

System: _____ Reviewer: _____
Priority gap: _____
Action owner: _____ Target date: _____
Completion evidence: _____

08 Put the checklist into practice

Download the free [CyberJA Access Review Workbook](#). Adapt this educational checklist to your organisation's scope, policies and applicable requirements.
