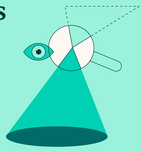
IDENTITY COMPLIANCE CHECKLIST

10 control areas

to review before your next audit



01. Identity & Access Inventory

WHAT TO REVIEW

- [ ] All privileged, human, machine, and third-party identities are accounted for
- [ ] Each has a clear owner and access scope

EVIDENCE TO HAVE READY

- [ ] Account inventories
- [ ] Entitlement reports
- [ ] Ownership records

02. Access Authorization

WHAT TO REVIEW

- [ ] Privileged access has a documented business need
- [ ] Access is approved and aligned to the user or system role

EVIDENCE TO HAVE READY

- [ ] Access requests
- [ ] Approval records
- [ ] Role definitions

03. Least Privilege

WHAT TO REVIEW

- [ ] Excess permissions and standing admin rights are identified
- [ ] Unnecessary access is removed or remediated

EVIDENCE TO HAVE READY

- [ ] Entitlement reports
- [ ] Segregation of Duties (SoD)
- [ ] Access review records
- [ ] Remediation records

04. Authentication

WHAT TO REVIEW

- [ ] MFA and other required authentication controls are applied
- [ ] Remote privileged access is appropriately protected

EVIDENCE TO HAVE READY

- [ ] MFA configurations
- [ ] Authentication logs
- [ ] Exception records

05. Privileged Credentials & Secrets

WHAT TO REVIEW

- [ ] Passwords, keys, tokens, and service credentials are controlled
- [ ] Storage, access, ownership, and rotation are defined

EVIDENCE TO HAVE READY

- [ ] Vault records
- [ ] Rotation history
- [ ] Credential access logs

06. Temporary Privileged Access

WHAT TO REVIEW

- [ ] Standing privilege is limited where appropriate
- [ ] JIT, time-bound, and emergency access expires as intended

EVIDENCE TO HAVE READY

- [ ] Approval records
- [ ] Expiration logs
- [ ] Break-glass records

07. Identity Lifecycle

WHAT TO REVIEW

- [ ] Access changes when roles or responsibilities change
- [ ] Access is removed when employees, vendors, or systems no longer need it

EVIDENCE TO HAVE READY

- [ ] Provisioning records
- [ ] Deprovisioning logs
- [ ] Role-change records

08. Access Reviews

WHAT TO REVIEW

- [ ] Access has a current owner and business need
- [ ] Review decisions and remediation are documented

EVIDENCE TO HAVE READY

- [ ] Review reports
- [ ] Certification records
- [ ] Remediation tickets

09. Logging & Monitoring

WHAT TO REVIEW

- [ ] Privileged activity can be traced to an accountable identity
- [ ] Relevant logs are protected, retained, and retrievable

EVIDENCE TO HAVE READY

- [ ] Access logs
- [ ] Session records
- [ ] Monitoring reports

10. Third-Party & Non-Human Access

WHAT TO REVIEW

- [ ] Vendors, service accounts, workloads, and AI agents have defined ownership
- [ ] Permissions are limited to their approved purpose

EVIDENCE TO HAVE READY

- [ ] Access records
- [ ] Identity inventories
- [ ] Activity logs