Enterprise Security Audit Checklist

A comprehensive, interactive framework for CISOs, security teams, and auditors.

1. Define Scope & Classification (NIST SP 800-53)

- [ ] Maintain CMDB of hardware, software, network devices, cloud services.
- [ ] Define and apply data classification levels (Public, Internal, Confidential, Regulated).
- [ ] Document VLANs, subnets, DMZs, external connections and firewall rules.
- [ ] Create system boundary and data flow diagrams; validate against architecture records.
- [ ] Identify and confirm system and data owners, stakeholders, and responsibilities.

2. Governance & Policy Review (ISO 27001:2013 Annex A)

- [ ] Catalog and verify policies (Security, AUP, BYOD, Access) with version control.
- [ ] Map policies to Annex A controls A.5–A.18; ensure procedures exist.
- [ ] Review user training records; test awareness via phishing simulations.
- [ ] Inspect audit logs and change tickets for policy enforcement.

3. Risk Assessment (CIS Controls v8)

- [ ] Conduct threat modeling using STRIDE/PASTA methodologies.
- [ ] Analyze CVE reports, scan results, and bug bounty feedback; record CVSS scores.
- [ ] Develop impact vs. likelihood matrix; categorize risks.
- [ ] Document risk treatment decisions (accept, mitigate, transfer, avoid) with owners.

4. Access Control Evaluation

- [ ] Audit identity lifecycle: provisioning, changes, deprovisioning.
- [ ] Verify MFA on all high-risk systems and admin portals.
- [ ] Review RBAC/ABAC and least-privilege configurations.
- [ ] Inspect PAM logs, session recordings, approval workflows, and service account rotation.

5. Vulnerability & Penetration Testing

- [ ] Run weekly Nessus/Qualys scans; ensure credentialed coverage.
- [ ] Perform internal/external pen tests; review scope and findings.
- [ ] Track remediation tickets and verify patch deployments.
- [ ] Collect and assess vendor SOC 2/ISO audit reports.

6. Logging, Monitoring & Detection

- [ ] Inventory log sources: OS, network, applications, cloud, security devices.
- [ ] Review SIEM correlation rules, tuning, and alert workflows.
- [ ] Conduct threat hunts; document hypotheses and results.
- [ ] Validate log retention policies and immutability safeguards.

7. Incident Response & Business Continuity

- [ ] Review IR playbooks for key scenarios; confirm contact lists.
- [ ] Run tabletop and technical exercises; capture lessons learned.
- [ ] Perform post-incident reviews; update controls and playbooks.
- [ ] Test BCP/DR plans: backups, RTO/RPO, failover procedures.

8. Reporting, Remediation & Follow-up

- [ ] Prepare executive summary with key findings and recommendations.
- [ ] Compile detailed report: evidence, screenshots, methodology.
- [ ] Create remediation roadmap: priorities, owners, deadlines.
- [ ] Schedule follow-up audits, exercises, and policy reviews.