Professional Server Hardening Audit Checklist

IT Administrator Infrastructure Security Self-Assessment

Score each item:

- **Yes = 2 points**
- **Partially = 1 point**
- **No = 0 points**

Inventory & Governance

☐ We maintain a current documented inventory of all production servers.
☐ Each server has a clearly defined business role and criticality classification.
☐ Administrative ownership is assigned for every production server.

OS Hardening

☐ Secure operating system baselines exist for Windows and/or Linux deployments.
☐ Legacy protocols and deprecated services have been disabled where possible.
☐ Unnecessary packages, features, and startup services are routinely removed.

Privileged Access

☐ Shared administrator accounts have been eliminated or minimised.
☐ Vendor access accounts are documented and periodically reviewed.
☐ MFA protects privileged remote administrative access.
☐ Service accounts are reviewed for password age and permission scope.

Patch & Vulnerability Management

☐ Critical OS and application patches are applied on a scheduled cycle.
☐ Firmware and infrastructure appliance updates are included in patch planning.
☐ Deferred vulnerabilities are formally documented with compensating controls.

Network Exposure

☐ Open ports are periodically reviewed for business necessity.
☐ Administrative interfaces are restricted to approved sources/VPN/jump hosts.
☐ Internal network segmentation limits unrestricted lateral movement.

Service & Application Reduction

☐ Installed applications are periodically reviewed and rationalized.
☐ Unauthorised software execution is restricted where possible.
☐ Deprecated vendor tools and unused agents are removed.

Monitoring & Visibility

☐ Security logs are centrally retained and reviewed.
☐ Failed login and privileged activity alerts are monitored.
☐ Service changes and endpoint security tampering generate alerts.

Backup & Recovery

☐ Backup systems use separate privileged protection.
☐ Recovery tests are performed regularly — not just backup completion reviews.
☐ Offline/offsite or immutable recovery copies exist for critical workloads.

Program Maturity

☐ Quarterly hardening reviews are scheduled and documented.
☐ Hardening checks are included in infrastructure change management.

SCORING RESULTS

40–50 Points — STRONG MATURITY

Your server environment demonstrates disciplined infrastructure security governance and above-average operational cyber resilience.

22–39 Points — MODERATE EXPOSURE

Important protections exist, but inconsistent controls and administrative drift may still leave exploitable weaknesses.

0–21 Points — HIGH VULNERABILITY

Your server infrastructure likely contains multiple avoidable compromise pathways and requires immediate hardening attention.