CYBER SIGMA

Server Security Configuration Review Workbook

PCI DSS v4.0.1 | ISO/IEC 27001:2022 | NIST CSF 2.0 | CIS Benchmarks & Controls v8.1 | UAE IA / KSA ECC | CERT-In

Client / Entity	
Device Hostname / Group	
OEM / Model / OS Version	
Serial / Asset ID	
Location / Environment	
Review Period	
Auditor	Cyber Sigma Consulting Services LLP
Reviewer	
Document Version	1.0
Classification	Confidential
Assessment Status	Draft / Final
Report Date	

Important: Example commands and console paths in this workbook are illustrative. They do not replace direct evidence from the sampled device. Mask serial numbers, public IPs, secrets and community strings in distributed reports. Prepare a separate copy for each sampled device.

1. Purpose and intended use

Use this workbook to review the secure configuration and hardening of one server (or a defined group of identical builds) at a time against an approved baseline. Duplicate the workbook or add an Asset Inventory row for each sampled host.

Collect configuration exports, policy output and CLI/registry/console evidence. Screenshots prove visible state; configuration and command output validate hidden, default and bulk settings. For each control record Pass, Fail, Partial, Not Applicable or Not Tested with an evidence reference.

The control-to-standard mappings are practical audit mappings, not a substitute for the licensed text of the standards or the formal opinion of a PCI QSA, SOC or ISO assessor.

2. Evidence capture rules

Rule	Required practice
Freshness	Capture during the audit period; show hostname and system time where possible; recollect stale evidence.
Completeness	Export full running/effective configuration and CLI/registry output; do not rely on cropped screenshots that omit context.
Authenticity	Capture directly from the sampled device or approved manager; retain native export metadata and checksum.
Confidentiality	Mask secrets, hashes, keys, community strings, serials and public IPs in the report; keep unredacted evidence in a restricted repository.
Traceability	Name files <Entity>_<Host>_<ControlNo>_<EvidenceType>_<YYYYMMDD>.<ext> and reference the evidence ID in each finding.
Two-sided proof	For 'not used' features (SNMP, Telnet, a service, encryption) obtain disabled/absent-state evidence. A management statement alone is insufficient.
Validation	Where feasible combine configuration evidence with an observed test: login failure, denied connection, log receipt or restore.

3. Assessment method and status criteria

Status	Definition	Suggested report treatment
Pass	Control is appropriately designed, configured and operating; evidence is current, complete and consistent.	Report as effective; retain evidence reference.
Partial	Control exists but is incomplete, inconsistently applied or weakly evidenced.	Raise finding with gap and remediation.
Fail	Control is absent, misconfigured or ineffective; exposure is present.	Raise finding with risk rating and remediation.
Not Applicable	Feature is genuinely absent or disabled; supported by configuration evidence.	Record rationale and disabled-state evidence.
Not Tested	Not examined this cycle.	State reason; schedule for next cycle.

4. Assessment approach

Objective: determine whether device architecture, configuration and operation enforce least privilege, minimal attack surface, strong authentication, auditability and recoverability - with evidence.

Phase	Name	Purpose	Key Activities	Outputs	Quality Gate
0	Authorization & Safety	Prevent disruption and unauthorised access.	Confirm scope, hosts, sample, read-only access, change windows and escalation.	Approved review plan and escalation matrix.	No export, login or test before written authorization.
1	Scope & Baseline	Establish the estate and the applicable hardening standard.	Reconcile inventory; confirm OS platforms, roles, data classes and the baseline per OS.	Scoped host list mapped to role, environment and baseline.	Every in-scope host mapped to owner, role and baseline.
2	Evidence Collection	Collect complete evidence without changing production.	Gather config exports, policy output, CLI/registry captures, scan and patch reports (read-only).	Evidence index with host, source, hash and date.	Exports are current, complete and reproducible.
3	Configuration Review	Assess build against the hardening baseline.	Run benchmark scans (CIS-CAT/SCAP), review services, accounts, crypto, firewall and audit policy.	Per-host control observations with drift.	No finding based on syntax alone; effective config confirmed.
4	Identity & Privilege	Validate authentication, MFA and least privilege.	Review accounts, admin membership, elevation, service accounts and remote-access controls.	Access-control observations.	Privileged access justified and evidenced.
5	Patch & Vulnerability	Assess currency and exposure.	Review patch compliance, EOL status, authenticated scan results and remediation SLAs.	Vulnerability and currency observations.	Findings validated against authenticated evidence.
6	Logging & Detection	Confirm auditability and monitoring.	Review audit policy, central forwarding, retention and detection use cases.	Logging and monitoring observations.	Central log receipt and detection confirmed, not assumed.
7	Resilience	Assess backup, recovery and time integrity.	Review backup coverage, restore tests, immutability and NTP.	Resilience observations.	At least one tested, immutable recovery path evidenced.
8	Risk Rating & Findings	Convert weaknesses into rated, actionable findings.	Score exposure, privilege, data criticality and control gaps; write condition/criteria/cause/impact.	Findings register with evidence and recommendations.	Each finding includes condition, criteria, cause, risk and recommendation.
9	Remediation & Retest	Reduce exposure and verify fixes.	Prioritise quick wins, plan changes, retest and update status.	Implemented/scheduled corrective actions and retest results.	High-risk changes peer-reviewed, tested and re-evidenced.
10	QA & Closure	Ensure consistency and management usability.	Peer review, evidence traceability, framework mapping and reporting.	Final report, baseline update and closure log.	All conclusions reproducible from evidence.

5. Control checklist

For each control record Pass, Fail, Partial, Not Applicable or Not Tested with evidence reference. Mappings are practical audit mappings.

Scope & Governance

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-SCO-01	Is every in-scope server (physical, virtual, cloud IaaS, appliance) captured in an approved inventory with owner, role, environment and data classification?	Reconcile CMDB, hypervisor/cloud console, monitoring and directory (AD/LDAP) computer objects; sample for coverage.	Approved server inventory with hostname, IP, OS/build, role, owner, environment, data class.	Unmanaged/unhardened hosts become unassessed attack surface.	ID.AM-01; GV.OC / A.5.9; A.8.1 / CIS 1.1 / 2.4; 12.5.1	Critical	_____
SRV-SCO-02	Is there an approved server hardening standard/baseline (e.g. CIS/DISA STIG derived) mandated for each OS platform in use?	Review the documented baseline, its approval, version and applicability per OS.	Signed hardening standard/build document per OS with control rationale.	Inconsistent, ad-hoc builds with undocumented exposure.	GV.PO; PR.PS / A.5.1; A.8.9 / CIS 4.1 / 2.2	Critical	_____
SRV-SCO-03	Are build, change, patch and decommission handled through change management with separation of request/approve/implement roles?	Review RACI and sample change tickets for a build and a config change.	Change records, RACI, segregation-of-duties evidence.	Unauthorised or unreviewed changes to production hosts.	GV.RR; PR.PS / A.5.3; A.8.32 / CIS 4.2 / 6.5.1; 12.5	High	_____
SRV-SCO-04	Are configuration exceptions time-bound, risk-assessed, approved and tracked to closure?	Sample the exception register against live configuration.	Exception records with risk, owner, compensating control and expiry.	Permanent, unreviewed deviations from baseline.	GV.RM / A.5.1; A.8.32 / CIS 4.1 / 2.2	High	_____

Asset Inventory & Ownership

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-INV-01	Is the OS edition, build/kernel and support/EOL status recorded and within a vendor-supported lifecycle?	Query build (winver / uname -r / cat /etc/os-release) and compare to vendor lifecycle.	OS/build report with support-end dates.	Unsupported OS receives no security patches.	ID.AM-02; ID.RA / A.8.8 / CIS 2.2 / 6.3.3	Critical	_____
SRV-INV-02	Is an authoritative software/package inventory maintained per host (installed packages, versions, agents)?	Export installed software (Get-Package / rpm -qa / dpkg -l) and reconcile to approved list.	Per-host software inventory with approval status.	Unknown/unauthorised software widens attack surface.	ID.AM-02 / A.5.9; A.8.8 / CIS 2.1 / 2.2.4; 6.3	High	_____
SRV-INV-03	Are hosts assigned to a business service and data-sensitivity tier that drives control strength?	Trace host to service catalogue and data classification.	Service map and data-classification tag per host.	Controls cannot be right-sized without context.	ID.AM-05 / A.5.12 / CIS 3.2 / 12.5.1	Medium	_____

Identity & Authentication

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-IAM-01	Are default/vendor accounts removed, renamed or disabled and their default passwords changed before production?	List local accounts (Get-LocalUser / /etc/passwd); check guest, default admin, vendor accounts.	Account listing showing disabled/renamed defaults and rotated credentials.	Default credentials are the most exploited initial-access vector.	PR.AA-01 / A.5.16; A.8.5 / CIS 5.2 / 2.2.2; 8.3.1	Critical	_____
SRV-IAM-02	Is centralised authentication enforced (AD / LDAP / IdM) with local accounts minimised to break-glass only?	Review domain join / SSSD/realmd config; enumerate local interactive accounts.	Directory-integration config and justified local-account list.	Orphaned local accounts and inconsistent controls.	PR.AA-01; PR.AA-05 / A.5.16; A.8.2 / CIS 5.6 / 8.2.1	High	_____
SRV-IAM-03	Is a strong password/passphrase policy enforced (length, complexity, history, lockout) meeting standard requirements?	Inspect policy (secpol.msc / pam_pwquality / faillock / pwpolicy) and lockout thresholds.	Password and lockout policy output.	Weak/guessable credentials enable brute-force and reuse.	PR.AA-01 / A.5.17; A.8.5 / CIS 5.3 / 8.3.6; 8.3.4	High	_____

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-IAM-04	Is multi-factor authentication enforced for administrative and remote (RDP/SSH/VPN) access to servers?	Verify MFA on jump hosts, RDP gateway, SSH (PAM/keys+OTP), or PAM solution.	MFA configuration/policy and enrolment evidence.	Single-factor admin access is trivially phished/replayed.	PR.AA-03 / A.8.5 / CIS 6.5 / 8.4.2; 8.5	Critical	_____
SRV-IAM-05	Are service/application accounts non-interactive, uniquely identified, least-privileged and credential-rotated (e.g. gMSA / vault)?	Review service accounts, logon rights, and secret-rotation mechanism.	Service-account register with logon-restrictions and rotation evidence.	Shared/static service credentials enable lateral movement.	PR.AA-01 / A.5.16; A.8.2 / CIS 5.4 / 8.6.1; 8.6.2	High	_____
SRV-IAM-06	Are inactive, terminated and stale accounts disabled/removed within policy timeframes?	Report last-logon and disabled accounts; reconcile to HR/leavers.	Stale-account report and deprovisioning evidence.	Dormant accounts are quiet persistence footholds.	PR.AA-01; ID.AM / A.5.18 / CIS 5.3 / 8.2.6	Medium	_____

Privilege & Access Control

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-PRV-01	Is administrative access least-privilege, role-based, and are day-to-day tasks performed with non-privileged accounts?	Review admin group membership (Administrators / sudoers / wheel) and privileged-role assignment.	Admin membership export with business justification per member.	Excess admins expand blast radius of any compromise.	PR.AA-05 / A.8.2 / CIS 5.4 / 7.2.2; 7.2.5	Critical	_____
SRV-PRV-02	Is privilege elevation controlled and logged (UAC / sudo with least commands / just-in-time PAM) rather than standing full root/admin?	Inspect UAC level, sudoers (NOPASSWD, command scope), JIT/PAM elevation and logging.	Elevation policy and sample elevation logs.	Standing privilege and unlogged elevation prevent accountability.	PR.AA-05; PR.PS / A.8.2; A.8.18 / CIS 5.4 / 7.2; 10.2.1.2	High	_____
SRV-PRV-03	Are file-system and share permissions restrictive, with world-writable files, weak ACLs and anonymous shares eliminated?	Scan for world-writable/SUID files (find / -perm), open shares, and sensitive-path ACLs.	Permission/ACL scan output and remediation of exceptions.	Weak permissions enable privilege escalation and data exposure.	PR.DS; PR.AA / A.8.3; A.8.4 / CIS 6.1 / 7.2.3	High	_____
SRV-PRV-04	Is remote administrative access restricted to specific admin sources/jump hosts rather than exposed to the whole network or Internet?	Review firewall/host rules for RDP(3389)/SSH(22)/WinRM and admin-source restriction.	Rule evidence limiting admin ports to bastion/management subnets.	Broad admin exposure invites brute-force and exploitation.	PR.AA-05; PR.IR / A.8.20; A.8.22 / CIS 4.6 / 1.3; 8.4	Critical	_____

Patch & Vulnerability Management

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-PAT-01	Are security patches applied within defined SLAs (e.g. critical <=14-30 days) via a managed patch process?	Review patch-management tool status (WSUS/SCCM/Intune, yum/dnf/apt, Satellite) and last-patch dates; sample missing patches.	Patch-compliance report with SLA adherence.	Unpatched hosts are exploited by commodity and targeted attackers.	ID.RA; PR.PS / A.8.8 / CIS 7.3 / 6.3.3	Critical	_____
SRV-PAT-02	Are hosts scanned regularly for vulnerabilities with authenticated scans and findings tracked to remediation?	Review scanner coverage (Nessus/Qualys/Defender), credentialed-scan config and remediation SLA.	Authenticated scan reports and remediation tracker.	Blind spots hide exploitable weaknesses.	ID.RA-01; DE.CM / A.8.8 / CIS 7.5 / 11.3.1	High	_____
SRV-PAT-03	Is third-party/application software (runtimes, middleware, agents) patched to supported versions alongside the OS?	Sample versions of Java, .NET, web/app servers, DB clients, agents vs current supported.	Application/component version report vs vendor-supported.	Vulnerable middleware is a common breach entry point.	ID.RA; PR.PS / A.8.8 / CIS 7.4 / 6.3.3	High	_____

Services & Attack Surface

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-SVC-01	Are only required services/roles/features installed and running, with unnecessary daemons disabled (minimal footprint)?	Enumerate services/roles (Get-Service / systemctl list-unit-files / chkconfig) vs role need.	Running-services list with justification; disabled-services evidence.	Every needless service is extra attack surface.	PR.PS-01 / A.8.9; A.8.19 / CIS 2.2 / 2.2.4; 2.2.5	High	_____
SRV-SVC-02	Are legacy/insecure services and protocols disabled (Telnet, FTP, rsh, TFTP, SMBv1, LLMNR/NBT-NS, LM/NTLMv1)?	Check for listeners and protocol settings (netstat/ss, SMB1 feature, LLMNR GPO, lanmanserver).	Config/scan evidence that insecure services/protocols are off.	Cleartext/legacy protocols enable interception and relay.	PR.PS; PR.DS / A.8.21; A.8.24 / CIS 2.3 / 2.2.5; 4.2.1	Critical	_____
SRV-SVC-03	Are listening network ports minimised and each open port mapped to an approved service?	Capture listeners (ss -tulpn / netstat -ano) and reconcile to approved service map.	Port-to-service mapping with approval.	Unexplained open ports indicate rogue or misconfigured services.	PR.PS; DE.CM / A.8.20 / CIS 4.4 / 1.2.5; 2.2.4	High	_____
SRV-SVC-04	Is host-based scripting / management surface controlled (PowerShell constrained language + logging, disabled macros where relevant)?	Review PowerShell execution/logging policy, WDAC/AppLocker, and script-host restrictions.	Script-control policy and logging evidence.	Living-off-the-land tooling abuses default scripting.	PR.PS; DE.CM / A.8.19 / CIS 2.3 / 2.2.4	Medium	_____

OS Hardening & Secure Configuration

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-CFG-01	Is the host built to an approved hardening baseline and is drift measured (e.g. CIS-CAT / DISA STIG / Group Policy / Ansible)?	Run a benchmark scan (CIS-CAT, SCAP, PowerSTIG) and compare score to target.	Benchmark scan result and drift report vs baseline.	Undetected drift silently reintroduces exposure.	PR.PS-01 / A.8.9 / CIS 4.1 / 2.2	Critical	_____
SRV-CFG-02	Are OS exploit-mitigation and integrity features enabled (Windows ASR/Credential Guard/LSA protection; Linux SELinux/AppArmor enforcing, ASLR, kernel hardening)?	Check Credential Guard/LSA (RunAsPPL), ASR rules; getenforce / aa-status; kernel sysctl.	Configuration evidence of enabled mitigations in enforcing mode.	Disabled mitigations ease credential theft and code execution.	PR.PS-01 / A.8.9 / CIS 5.1 / 2.2	High	_____
SRV-CFG-03	Are unnecessary local admin shares, autorun, and unauthenticated remote registry/WMI access disabled or restricted?	Check administrative shares, AutoRun policy, Remote Registry service, WMI namespace ACLs.	Config evidence of restricted remote management surfaces.	Default remote surfaces enable lateral movement.	PR.PS; PR.AA / A.8.9 / CIS 4.8 / 2.2.4	Medium	_____
SRV-CFG-04	Is disk/volume encryption enabled for data at rest where the data class or regulation requires it (BitLocker / LUKS / dm-crypt)?	Verify encryption status (manage-bde -status / lsblk + cryptsetup) and key-escrow.	Encryption status and key-management evidence.	Unencrypted disks expose data on theft/decommission.	PR.DS-01 / A.8.24 / CIS 3.6 / 3.5.1	High	_____
SRV-CFG-05	Are removable-media and external-device controls applied where policy requires (block/allow-list, read-only, encryption)?	Review device-control policy (GPO / MDM / DLP agent) and enforcement.	Device-control policy and enforcement evidence.	Uncontrolled media enables data exfiltration and malware ingress.	PR.DS; PR.PS / A.7.10; A.8.7 / CIS 10.3 /	Medium	_____

Network & Host-based Firewall

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-NET-01	Is a host-based firewall enabled with a default-deny inbound posture and only required ports allowed?	Review Windows Defender Firewall / firewalld / nftables/ufw profiles and rules.	Firewall profile export showing default-deny + justified allows.	Flat host exposure enables lateral movement.	PR.IR-01 / A.8.20 / CIS 4.5 / 1.4.1; 1.2	High	_____
SRV-NET-02	Are servers placed in appropriate network zones/segments (DMZ vs internal vs management) consistent with their role and data class?	Trace interfaces/VLANs and inter-zone rules to architecture.	Segmentation evidence and zone assignment.	Flat networks allow unrestricted lateral movement.	PR.IR-01 / A.8.22 / CIS 12.2 / 1.2; 1.3	High	_____
SRV-NET-03	Is outbound/egress traffic restricted (no unrestricted Internet egress from servers; proxy/allow-list for updates)?	Review egress rules, proxy config and DNS egress control.	Egress policy and enforcement evidence.	Unrestricted egress aids C2 and exfiltration.	PR.IR; DE.CM / A.8.20 / CIS 4.4 / 1.3.2	Medium	_____

Cryptography & Secure Protocols

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-CRY-01	Are only strong TLS versions and cipher suites enabled (TLS1.2/1.3; SSLv3/TLS1.0/1.1 and weak ciphers disabled)?	Test endpoints (testssl.sh / registry SCHANNEL / OpenSSL config) for protocol/cipher support.	TLS scan output and protocol/cipher configuration.	Weak TLS enables downgrade and interception.	PR.DS-02 / A.8.24 / CIS 3.10 / 4.2.1; 2.2.7	High	_____
SRV-CRY-02	Is remote admin over SSH hardened (SSHv2 only, no root login, key-based auth, strong KEX/MAC/ciphers, idle timeout)?	Inspect sshd_config (PermitRootLogin, PasswordAuthentication, Ciphers/MACs/KexAlgorithms).	sshd_config and effective-config evidence.	Weak SSH config enables brute-force and MITM.	PR.AA; PR.DS / A.8.5; A.8.24 / CIS 5.2 / 2.2.7; 8.3	High	_____
SRV-CRY-03	Are certificates and keys valid, from a trusted CA, adequately sized, and managed (no self-signed on prod, no expired, protected private keys)?	Enumerate certificate stores; check expiry, key length and private-key protection.	Certificate inventory with validity and key protection evidence.	Expired/weak/exposed keys break trust and confidentiality.	PR.DS-02 / A.8.24 / CIS 3.10 / 4.2.1	Medium	_____

Logging, Audit & Monitoring

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-LOG-01	Is security auditing enabled to capture logon, privilege use, account/policy changes, object access and process creation?	Review audit policy (auditpol / advanced audit GPO; auditd rules; authpriv) against baseline.	Audit-policy export and sample events.	Without audit trails, attacks are invisible and unforensicable.	DE.CM-01; PR.PS / A.8.15 / CIS 8.5 / 10.2.1	Critical	_____
SRV-LOG-02	Are logs forwarded in near real time to a central SIEM/log store separate from the host, with integrity protection?	Verify log forwarding (WEF/agent, rsyslog/journald remote) and central receipt; check tamper controls.	Forwarding config and evidence of central receipt.	Local-only logs are wiped by attackers; gaps hide incidents.	DE.CM; PR.PS / A.8.15; A.8.16 / CIS 8.9 / 10.3; 10.5.1	Critical	_____
SRV-LOG-03	Are log retention and protection sufficient (>=1 year, or per regulation, with restricted access and no clear-text secrets)?	Check retention config, storage sizing and access controls on log stores.	Retention policy and access-control evidence.	Insufficient retention defeats investigation and compliance.	PR.PS; RC.RP / A.8.15 / CIS 8.10 / 10.5.1	High	_____
SRV-LOG-04	Are host-relevant detections monitored (EDR alerts, brute-force, new admin, service changes) with defined response?	Review SIEM/EDR use cases mapped to the host and alerting workflow.	Use-case list and sample alert-to-response evidence.	Collected-but-unwatched logs do not stop attacks.	DE.AE; DE.CM / A.8.16 / CIS 8.11 / 10.4.1	High	_____

File Integrity & Change Control

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-FIM-01	Is file-integrity monitoring deployed on critical OS, config and binary paths with alerting on change?	Review FIM tooling (Defender/Tripwire/AIDE/osquery) scope and alert config.	FIM policy, monitored-path list and sample change alerts.	Silent tampering of binaries/config enables persistence.	DE.CM-01; PR.DS / A.8.15; A.8.9 / CIS 3.14 / 11.5.2	Medium	_____
SRV-FIM-02	Is application allow-listing / execution control used on high-value or fixed-function servers where feasible?	Review WDAC/AppLocker/fapolicyd policy and enforcement mode.	Allow-listing policy and enforcement evidence.	Unrestricted execution permits malware and LOLBins.	PR.PS-02 / A.8.19 / CIS 2.5 /	Medium	_____

Malware Protection

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-MAL-01	Is endpoint protection / EDR installed, running, updated and centrally managed on every server (with server-appropriate exclusions)?	Verify agent presence, definition currency, tamper protection and console enrolment.	EDR/AV status report showing coverage and update state.	Unprotected hosts are soft targets for malware/ransomware.	DE.CM-01; PR.PS / A.8.7 / CIS 10.1 / 5.2; 5.3	Critical	_____

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-MAL-02	Are anti-malware real-time protection, tamper protection and periodic scans enabled and not weakened by broad exclusions?	Review real-time/tamper settings and audit exclusion scope for over-breadth.	Protection settings and exclusion review.	Disabled protection or broad exclusions blind defences.	PR.PS; DE.CM / A.8.7 / CIS 10.1 / 5.3.1; 5.3.2	High	_____

Time Synchronisation

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-TIM-01	Are all servers synchronised to authorised, redundant time sources with drift within tolerance?	Check time config (w32tm /query / chronyc sources / timedatectl) and source trust.	Time-source config and drift/offset evidence.	Skewed clocks break log correlation, auth (Kerberos) and MFA.	PR.PS; DE.CM / A.8.15 / CIS 8.4 / 10.6.1; 10.6.2	Medium	_____

Backup & Recovery

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-BAK-01	Are servers backed up per policy, with backups tested, and at least one copy immutable/offline/off-site (ransomware-resilient)?	Review backup schedule/scope, last successful job, restore-test records and immutability/air-gap.	Backup reports, restore-test evidence and immutability configuration.	Unrecoverable data loss during ransomware/failure.	RC.RP-01; PR.DS / A.8.13 / CIS 11.2 /	Critical	_____
SRV-BAK-02	Are backup systems and media access-controlled, encrypted and monitored, with credentials separated from production admin?	Review backup console access, encryption of backups, and credential separation.	Backup access-control, encryption and monitoring evidence.	Compromised backups defeat recovery and leak data.	PR.DS; PR.AA / A.8.13; A.8.24 / CIS 11.3 /	High	_____

Boot, Firmware & Physical

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-BOOT-01	Are firmware/BIOS/BMC (iLO/iDRAC/IPMI) updated, password-protected, and management interfaces on an isolated network?	Check firmware/BMC versions, admin credentials, and BMC network placement/segmentation.	Firmware inventory, BMC credential and network-isolation evidence.	BMC/firmware compromise is stealthy and persistent.	PR.PS; PR.IR / A.7.8; A.8.9 / CIS 12.1 / 2.2.2	High	_____
SRV-BOOT-02	Are Secure Boot and (where present) TPM/measured-boot enabled, and boot order protected against unauthorised media boot?	Verify Secure Boot/TPM state (Confirm-SecureBootUEFI / mokutil / tpm2) and BIOS boot protections.	Secure Boot/TPM status and BIOS configuration evidence.	Bootkit/tamper and offline attacks bypass OS controls.	PR.PS / A.8.9 / CIS 3.6 /	Medium	_____
SRV-BOOT-03	Are physical/console access controls in place for on-prem servers (locked racks, restricted console, no auto-login)?	Review data-centre access, console/KVM restrictions and screen-lock/auto-logout policy.	Physical-access and console-control evidence.	Physical console access can bypass many logical controls.	PR.AA; PR.IR / A.7.1-A.7.4 / CIS 6.1 / 9.1	Medium	_____

Virtualisation / Hypervisor host

ID	Review Question	Test Method	Expected Evidence	Risk if Failed	NIST / ISO / CIS / PCI	Pri.	Status
SRV-VIRT-01	Are hypervisor hosts (ESXi/Hyper-V/KVM) hardened to vendor baseline with management interfaces isolated and lockdown enabled?	Review host hardening (ESXi lockdown mode, Hyper-V host config) and management-network isolation.	Hypervisor hardening and management-isolation evidence.	Hypervisor compromise exposes every hosted workload.	PR.PS; PR.IR / A.8.9; A.8.22 / CIS 12.2 / 2.2	High	_____
SRV-VIRT-02	Are hypervisor logging, patching and RBAC configured, with vMotion/live-migration and storage traffic on isolated networks?	Review host patch level, RBAC roles, syslog export, and network segregation of infra traffic.	Patch, RBAC, logging and network-segregation evidence.	Weak hypervisor governance enables broad compromise.	PR.PS; DE.CM / A.8.8; A.8.15 / CIS 12.2 / 10.2.1	Medium	_____

6. Risk scoring model

Factor	Weight	1 - Low	3	5 - Very High	Examples
Exposure	30	Internal, tightly restricted	Cross-zone / internal broad	Internet-facing or untrusted inbound	Public host, exposed RDP/SSH, DMZ server
Privilege / Account Risk	25	Standard user scope	Elevated local scope	Domain/root/admin or service credential	Local admin, domain admin, SA account
Data / Asset Criticality	20	Low-impact host	Standard business server	Sensitive data, identity, safety or OT	Domain controller, database, PACS, ERP
Exploitability	15	Hard, authenticated, no known exploit	Known issue, some conditions	Remotely exploitable, public exploit	Unauthenticated RCE, default creds
Control Gap	10	Layered compensating controls	Partial monitoring/patch gap	No logging, no EDR, unpatched, weak auth	Missing audit, no MFA, EOL OS

Weighted score = (Exposure x30 + Privilege x25 + Criticality x20 + Exploitability x15 + Control Gap x10) / 100, each factor rated 1-5, normalised to 0-100.

7. Framework mapping

Review Area	NIST CSF 2.0	ISO/IEC 27001:2022	CIS	PCI DSS v4.0.1	UAE IA / KSA ECC / CERT-In
Governance & baseline	GV.PO; GV.RR; PR.PS	A.5.1; A.5.3; A.8.9	CIS 4.1; 4.2	2.2; 12.5	1-3-3; 2-3-1
Identity & authentication	PR.AA-01; PR.AA-03	A.5.16; A.5.17; A.8.5	CIS 5.2-5.6; 6.5	8.2; 8.3; 8.4	2-2-1..4
Privilege & access	PR.AA-05	A.8.2; A.8.18	CIS 5.4	7.2	2-2-3
Patch & vulnerability	ID.RA-01; PR.PS	A.8.8	CIS 7.3-7.5	6.3.3; 11.3.1	2-10-1; 2-10-3
Attack-surface reduction	PR.PS-01	A.8.9; A.8.19; A.8.21	CIS 2.2-2.5; 4.4	2.2.4; 2.2.5	2-3-1
Cryptography & protocols	PR.DS-01; PR.DS-02	A.8.24	CIS 3.6; 3.10	3.5; 4.2.1	2-6-1; 2-6-2
Logging & monitoring	DE.CM-01; DE.AE	A.8.15; A.8.16	CIS 8.5-8.11	10.2-10.6	2-12; 2-13; CERT-In
Malware & integrity	DE.CM-01; PR.PS-02	A.8.7; A.8.9	CIS 2.5; 3.14; 10.1	5.2; 5.3; 11.5.2	2-4-1
Resilience & recovery	RC.RP-01; PR.DS	A.8.13; A.8.14	CIS 11.2; 11.3		2-8-1
Firmware, boot & physical	PR.PS; PR.IR	A.7.1-A.7.8; A.8.9	CIS 12.1	9.1	2-3-1; 2-14-1