Network Security Audit Checklist

Version: 1.0 | **Author:** VarnaAI (varnaai.com) | **License:** Free for commercial use

---

Audit Information

Field	Value
Audit ID	NSA-**-**
Audit Date	**/**/_____
Auditor	
Scope	
Standards Referenced	[ ] ISO 27001 [ ] PCI DSS [ ] NIS2 [ ] CIS Controls [ ] NIST CSF

---

1. Perimeter Security

#	Check	Status	Evidence/Notes
1.1	Firewall deployed at all internet entry points	[ ] Pass [ ] Fail [ ] N/A	
1.2	Default deny rule in place (inbound and outbound)	[ ] Pass [ ] Fail [ ] N/A	
1.3	DMZ architecture separates public-facing services	[ ] Pass [ ] Fail [ ] N/A	
1.4	IDS/IPS deployed and signatures current (<7 days)	[ ] Pass [ ] Fail [ ] N/A	
1.5	Web Application Firewall (WAF) on public web apps	[ ] Pass [ ] Fail [ ] N/A	
1.6	DDoS protection in place	[ ] Pass [ ] Fail [ ] N/A	
1.7	No direct internet access from internal networks	[ ] Pass [ ] Fail [ ] N/A	
1.8	DNS filtering/security configured	[ ] Pass [ ] Fail [ ] N/A	
1.9	Email gateway with anti-spam/anti-phishing	[ ] Pass [ ] Fail [ ] N/A	
1.10	SSL/TLS inspection on outbound traffic	[ ] Pass [ ] Fail [ ] N/A	

---

2. Internal Segmentation

#	Check	Status	Evidence/Notes
2.1	Network segmented into security zones	[ ] Pass [ ] Fail [ ] N/A	
2.2	VLANs implemented with inter-VLAN filtering	[ ] Pass [ ] Fail [ ] N/A	
2.3	Server, user, and management networks separated	[ ] Pass [ ] Fail [ ] N/A	
2.4	PCI cardholder data environment (CDE) isolated	[ ] Pass [ ] Fail [ ] N/A	

2.5	IoT/OT devices on separate network segment	[ ] Pass [ ] Fail [ ] N/A	
2.6	Guest Wi-Fi isolated from corporate network	[ ] Pass [ ] Fail [ ] N/A	
2.7	Microsegmentation for critical applications	[ ] Pass [ ] Fail [ ] N/A	
2.8	East-west traffic monitoring in place	[ ] Pass [ ] Fail [ ] N/A	

---

3. Access Control

#	Check	Status	Evidence/Notes
3.1	Network device access via SSH only (no Telnet)	[ ] Pass [ ] Fail [ ] N/A	
3.2	Management interfaces on dedicated OOB network	[ ] Pass [ ] Fail [ ] N/A	
3.3	Multi-factor authentication for network device admin	[ ] Pass [ ] Fail [ ] N/A	
3.4	RADIUS/TACACS+ for centralized authentication	[ ] Pass [ ] Fail [ ] N/A	
3.5	Role-based access control (RBAC) configured	[ ] Pass [ ] Fail [ ] N/A	
3.6	Default credentials changed on all devices	[ ] Pass [ ] Fail [ ] N/A	
3.7	Password complexity requirements enforced	[ ] Pass [ ] Fail [ ] N/A	
3.8	802.1X (NAC) for endpoint authentication	[ ] Pass [ ] Fail [ ] N/A	
3.9	VPN with MFA for remote access	[ ] Pass [ ] Fail [ ] N/A	
3.10	Privileged access management (PAM) for network admin	[ ] Pass [ ] Fail [ ] N/A	

---

4. Monitoring and Logging

#	Check	Status	Evidence/Notes
4.1	Centralized log management (SIEM) deployed	[ ] Pass [ ] Fail [ ] N/A	
4.2	All firewall logs forwarded to SIEM	[ ] Pass [ ] Fail [ ] N/A	
4.3	All switch/router logs forwarded to SIEM	[ ] Pass [ ] Fail [ ] N/A	
4.4	NTP synchronized across all network devices	[ ] Pass [ ] Fail [ ] N/A	
4.5	Log retention meets compliance requirements (90+ days)	[ ] Pass [ ] Fail [ ] N/A	
4.6	Alerting configured for critical events	[ ] Pass [ ] Fail [ ] N/A	
4.7	NetFlow/sFlow collection for traffic analysis	[ ] Pass [ ] Fail [ ] N/A	
4.8	Failed login attempts monitored and alerted	[ ] Pass [ ] Fail [ ] N/A	
4.9	Configuration change detection enabled	[ ] Pass [ ] Fail [ ] N/A	
4.10	Regular log review process documented	[ ] Pass [ ] Fail [ ] N/A	

---

5. Vulnerability Management

#	Check	Status	Evidence/Notes
5.1	Network device firmware current (within 1 major version)	[ ] Pass [ ] Fail [ ] N/A	
5.2	Known vulnerabilities patched within SLA	[ ] Pass [ ] Fail [ ] N/A	
5.3	Quarterly vulnerability scans performed	[ ] Pass [ ] Fail [ ] N/A	
5.4	Annual penetration test performed	[ ] Pass [ ] Fail [ ] N/A	
5.5	Unused services disabled on all devices	[ ] Pass [ ] Fail [ ] N/A	
5.6	SNMP v3 only (v1/v2c disabled)	[ ] Pass [ ] Fail [ ] N/A	
5.7	Unused ports administratively shut down	[ ] Pass [ ] Fail [ ] N/A	
5.8	Network device hardening baseline applied	[ ] Pass [ ] Fail [ ] N/A	

---

6. Resilience and Recovery

#	Check	Status	Evidence/Notes
6.1	Network device configs backed up (automated, daily)	[ ] Pass [ ] Fail [ ] N/A	
6.2	Backups stored off-device and encrypted	[ ] Pass [ ] Fail [ ] N/A	
6.3	Redundant firewalls (HA pair) for critical paths	[ ] Pass [ ] Fail [ ] N/A	
6.4	Redundant switches/routers for critical paths	[ ] Pass [ ] Fail [ ] N/A	
6.5	Disaster recovery plan includes network restoration	[ ] Pass [ ] Fail [ ] N/A	
6.6	DR plan tested within last 12 months	[ ] Pass [ ] Fail [ ] N/A	
6.7	Network topology diagram current (<6 months old)	[ ] Pass [ ] Fail [ ] N/A	
6.8	Change management process documented and followed	[ ] Pass [ ] Fail [ ] N/A	

Audit Summary

Category	Pass	Fail	N/A	Score
Perimeter Security (10)				/10
Internal Segmentation (8)				/8
Access Control (10)				/10
Monitoring and Logging (10)				/10
Vulnerability Management (8)				/8
Resilience and Recovery (8)				/8

TOTAL (54)				**/54**

Overall Grade: ____

Grade	Score	Meaning
A	90-100%	Excellent — minor improvements only
B	75-89%	Good — some gaps to address
C	60-74%	Fair — significant improvements needed
D	40-59%	Poor — major security risks present
F	<40%	Critical — immediate remediation required

Sign-Off

Role	Name	Signature	Date
Auditor			
IT Manager			
CISO / Security Lead			
