CYBER & TECH ARCHITECTURE

Enterprise Security Architecture Review Checklist

A 20-point self-assessment across identity, segmentation, data protection, detection, and governance — score yourself honestly, then fix your weakest section first.

How to score: for each item, score 0 (not in place), 1 (partially / informally in place), or 2 (fully in place and verified). Add your section subtotals. Your **lowest-scoring section is your real constraint** — a strong average hides a weak section that attackers will find first.

Zero Trust & Identity

Every user and device is authenticated per-session, not per-network-perimeter	**0 1 2**
Multi-factor authentication is enforced for all privileged accounts	**0 1 2**
Identity provider enforces least-privilege role assignments, reviewed quarterly	**0 1 2**
Service accounts and machine identities are inventoried and rotated on a schedule	**0 1 2**
Section subtotal (out of 8)	

Network Segmentation

Production, staging, and corporate networks are segmented with enforced east-west controls	**0 1 2**
Micro-segmentation is applied around crown-jewel data stores	**0 1 2**
Remote access runs through a Zero Trust Network Access (ZTNA) gateway, not a flat VPN	**0 1 2**
Segmentation boundaries are tested with an internal red-team exercise at least annually	**0 1 2**
Section subtotal (out of 8)	

Data Protection

Sensitive data is classified and tagged at creation, not retroactively	**0 1 2**
Encryption at rest and in transit is enforced by policy, not by individual engineer discretion	**0 1 2**
Data loss prevention (DLP) controls cover the top 3 exfiltration paths (email, cloud storage, endpoint)	**0 1 2**
Backup integrity is verified with a real restore test at least twice a year	**0 1 2**

Section subtotal (out of 8)

Monitoring & Detection

Centralized logging covers identity, network, endpoint, and cloud control-plane events	**0 1 2**
Detection rules are mapped to a named framework (e.g. MITRE ATT&CK), not ad hoc	**0 1 2**
Mean time to detect (MTTD) is measured and tracked over time	**0 1 2**
Alert fatigue is actively managed — false-positive rate is reviewed monthly	**0 1 2**

Section subtotal (out of 8)

Governance & Response

A documented incident response plan exists and has been tabletop-tested in the last 12 months	**0 1 2**
Architecture decisions are reviewed against a written reference architecture, not tribal knowledge	**0 1 2**
Third-party and vendor access is time-boxed and logged, not standing	**0 1 2**
Executive leadership receives a security posture readout at least quarterly	**0 1 2**

Section subtotal (out of 8)

Reading Your Score

Total Score	Verdict
0–14	Foundational gaps — architecture is largely ad hoc; start with identity and segmentation before anything else.
15–26	Partial coverage — controls exist but aren't verified or consistently enforced across the environment.
27–33	Solid baseline — most controls are in place; focus on the lowest-scoring section, not the average.
34–40	Mature — shift focus from building controls to proving and measuring them (tabletop tests, red-team validation, metrics).

Max possible score: 40 (20 items × 2)

Want a second set of eyes on this?
This self-assessment tells you where you stand. If your lowest-scoring section needs real remediation planning, the Architect Track programs at Cyber & Tech Architecture start with a scoped architecture review — see the current Founding Tripwire pricing on the site for the fastest way in.