

The Digital Infrastructure Audit Checklist

Twenty-seven scored checkpoints across seven layers of your stack. Score each 0, 1 or 2 and you will finish with a number out of 54 — and a ranked list of what is most likely to break first.

How to use this checklist

Most infrastructure problems are not discovered — they are announced, usually by an outage, an auditor, or a customer. This checklist is designed to find them in the ninety minutes before that happens.

Work through all twenty-seven checkpoints and score each one honestly:

SCORE	MEANS
0	Not in place, or nobody can say whether it is in place.
1	Partly in place — exists for some systems, or exists but is not verified, documented or monitored.
2	In place, documented, and verified within the last 90 days.

The single most important rule

Score what you can **prove today**, not what you believe is true. "We have backups" scores 0 until someone has actually restored one. The gap between belief and evidence is where every incident lives.

Layer 1 — Network & connectivity 4 checks

1	Documented network topology. A current diagram showing every site, VLAN, subnet, firewall and internet circuit — with the date it was last verified against reality, not against memory.	0 · 1 · 2
2	Single points of failure identified. You can name every device whose failure takes a site offline, and for each one you know the replacement lead time and whether a spare exists.	0 · 1 · 2
3	Firewall rule review. Rules have been reviewed in the last 12 months, any-any rules are justified in writing, and rules created for a project that ended have been removed.	0 · 1 · 2
4	Remote access is brokered, not exposed. No RDP, SSH or management interface is reachable directly from the internet; access is via VPN or an identity-aware proxy with MFA.	0 · 1 · 2

Layer 2 — Identity & access 5 checks

5	MFA on every administrative account. Including break-glass accounts, service-desk accounts, and the accounts your vendors use. Legacy protocols that bypass MFA are blocked.	0 · 1 · 2
6	No shared administrator credentials. Every privileged action is attributable to a named human. Shared passwords in a spreadsheet, a wiki or a chat channel score 0.	0 · 1 · 2
7	Joiner–mover–leaver process is enforced. Access is provisioned from a role definition and revoked the same day someone leaves — verified by sampling three recent departures.	0 · 1 · 2
8	Quarterly access reviews. System owners re-attest who should have access to what, and the attestation is retained. Reviews that nobody has ever failed are not reviews.	0 · 1 · 2
9	Least privilege on cloud and SaaS admin roles. You can produce a list of every global administrator across Microsoft 365, Google Workspace, AWS, Azure and your main SaaS tools.	0 · 1 · 2

Layer 3 — Endpoints 4 checks

10	Complete asset inventory. Every laptop, desktop, server and mobile device that touches company data is enrolled and accounted for, including contractor and personal devices.	0 · 1 · 2
11	Patch compliance is measured. You can state the percentage of endpoints patched within 30 days of release. "Automatic updates are on" without a compliance number scores 1.	0 · 1 · 2
12	Managed endpoint detection. EDR or equivalent is deployed, alerting to somebody whose job it is to respond, with defined hours of coverage.	0 · 1 · 2
13	Disk encryption enforced and recoverable. Full-disk encryption is on by policy and recovery keys are escrowed centrally — not held only by the user.	0 · 1 · 2

Layer 4 — Data & backup 4 checks

- | | | |
|-----------|---|-----------|
| 14 | Backups cover everything that matters. Including SaaS data — Microsoft 365, Google Workspace, Salesforce and similar are <i>not</i> backed up by the vendor in the way most people assume. | 0 · 1 · 2 |
| 15 | An immutable or offline copy exists. At least one copy cannot be deleted or encrypted by an attacker who has compromised your administrative credentials. | 0 · 1 · 2 |
| 16 | Restores are tested on a schedule. A real restore of a real system has been performed and timed in the last 90 days, and the result was written down. | 0 · 1 · 2 |
| 17 | RPO and RTO are agreed with the business. Written targets exist per system, signed off by someone outside IT, and your current capability is measured against them. | 0 · 1 · 2 |

Layer 5 — Cloud & hosting 4 checks

- | | | |
|-----------|---|-----------|
| 18 | Cloud spend is attributed. Every resource carries an owner and cost-centre tag, and someone reviews the bill monthly against expectation rather than paying it. | 0 · 1 · 2 |
| 19 | No orphaned or unmanaged resources. You have identified resources with no owner, no tags, or created outside your provisioning process — the classic source of both cost and breach. | 0 · 1 · 2 |
| 20 | Infrastructure is reproducible. Critical environments can be rebuilt from code or documented runbooks rather than from the memory of one person. | 0 · 1 · 2 |
| 21 | Public exposure is deliberate. Every publicly reachable storage bucket, database, container registry and endpoint is on a list, and each one is on that list on purpose. | 0 · 1 · 2 |

Layer 6 — Monitoring & response 3 checks

- | | | |
|-----------|--|-----------|
| 22 | You find out before your users do. Monitoring covers availability and the key business transaction, not just whether the server responds to ping. | 0 · 1 · 2 |
| 23 | Alerts route to a human with authority. There is an on-call rotation, an escalation path, and alert volume is low enough that alerts are actually read. | 0 · 1 · 2 |
| 24 | An incident response plan exists and has been rehearsed. Including who declares an incident, who talks to customers, and who can authorise taking a system offline. | 0 · 1 · 2 |

Layer 7 — Governance & continuity

3 checks

25	Vendor and licence register is current. Renewal dates, contract owners and data-processing terms for every material supplier, reviewed at least annually.	0 · 1 · 2
26	Key-person risk is documented. You can name every system where exactly one person holds the knowledge or the credentials, and there is a plan for each.	0 · 1 · 2
27	Change management is proportionate and used. Production changes are recorded with a rollback plan. A process that everyone routes around scores 1, not 2.	0 · 1 · 2

Reading your score

Add all twenty-seven scores together for a total out of 54.

SCORE	WHAT IT MEANS	WHERE TO START
45–54	Mature. Controls exist and are evidenced. Your risk is drift — controls decaying quietly between reviews.	Move from annual to continuous verification; focus on the two lowest individual scores.
32–44	Functional but uneven. The basics hold; specific layers are carrying real risk.	Fix every checkpoint scored 0 before improving anything already scored 1.
18–31	Fragile. You are likely one departure, one ransomware event or one audit away from a serious problem.	Backups with a tested restore, MFA everywhere, and the leaver process — in that order.
0–17	Critical. Assume that an incident would be materially damaging and that recovery is unproven.	Stop improvement work. Establish a recoverable backup and remove internet-exposed management access this week.

The number is less useful than the pattern

A total of 40 built from evenly-spread 1s is a very different organisation from a 40 built from mostly 2s and four hard zeros. **The zeros are the finding.** Rank them by what a failure would cost you on a Monday morning, and work that list from the top.

You have the gaps. The next question is what they cost.

The **IT Health Check Quickstart** takes the eighteen checkpoints that most reliably predict an outage or a failed audit and gives you the exact command, console path or query to verify each one — plus a findings template and a sequenced 30-day remediation plan.

atomixtechnology.com/it-health-check-quickstart · \$37

This checklist is provided for general informational purposes and does not constitute legal, regulatory or security assurance advice. Scoring is a self-assessment aid, not a certification, audit opinion or penetration test. Regulated organisations should validate findings against their applicable framework. © 2026 Atomix Technology. Distributed free; not for resale.