MatrixGard

INFRASTRUCTURE AUDIT, 2026 EDITION

Infrastructure Evaluation Checklist

Is your infrastructure cost-effective, secure and scalable? A 10-minute self-assessment for founders. Score each line Yes, Partly or No. No deep technical digging: if you do not know an answer, ask your team, and treat "not sure" as No.

40 questions | 8 sections of 5 | Max score 80 | About 10 minutes | Last reviewed: November 2026

How to score

Yes = 2 | Partly = 1 | No = 0

Tick one box per line. Add up each section (5 lines, so 10 points at most), then add the 8 sections.

Does a line not apply to you (for example, you do not run virtual machines)? Score it 2, so it does not pull you down.

The arithmetic

40 questions x 2 points = **80 points**.

8 sections x 10 points = **80 points**.

Score bands are on the last page.

SECTION 1 · COST

Cost visibility

Do we know where the money goes?

Score ____ / 10

	QUESTION	YES	PARTLY	NO
1.1	We can see monthly cloud cost by service and by team or product.	2	1	0
1.2	Budgets and alerts warn us before a surprise bill, not after it.	2	1	0
1.3	Idle and unused resources are found and removed on a schedule.	2	1	0
1.4	Someone acts on the provider's right-sizing recommendations at least once a quarter.	2	1	0
1.5	We know roughly what one customer, feature or environment costs us.	2	1	0

SECTION 2 · COST

Cost leaks

Where does money leak without anyone noticing?

Score ____ / 10

	QUESTION	YES	PARTLY	NO
2.1	Non-production environments shut down outside working hours.	2	1	0
2.2	Steady, always-on workloads are covered by Savings Plans, reservations or committed-use discounts.	2	1	0
2.3	Servers run on current instance generations, and Arm (AWS Graviton) has been tried where our software supports it. Example: AWS M8g runs on Graviton4.[10]	2	1	0
2.4	We count our public IPv4 addresses and release the ones we do not need. Since 1 Feb 2024 AWS charges for every public IPv4 address, in use or idle.[8]	2	1	0
2.5	Every resource carries an owner and cost-centre tag, and untagged resources are blocked or flagged.	2	1	0

SECTION 3 · SECURITY

Identity, access and secrets

Could a stolen password or leaked key take us down?

Score _____ / 10

	QUESTION	YES	PARTLY	NO
3.1	Everyone with admin or cloud-console access signs in with phishing-resistant MFA: passkeys or FIDO2 security keys, not SMS codes. NIST SP 800-63B-4 requires a phishing-resistant option at AAL2 and a phishing-resistant authenticator at AAL3.[1]	2	1	0
3.2	Least privilege: no broad admin roles for people or services, and access is reviewed at least quarterly.	2	1	0
3.3	The root or owner account is locked away with MFA and not used day to day.	2	1	0
3.4	Secrets live in a secrets manager, not in code, CI variables, wikis or chat.	2	1	0
3.5	AI and LLM API keys are in the secrets manager too, with spend limits and a rotation plan. OWASP Top 10 for LLM Applications 2025: LLM10 Unbounded Consumption.[3]	2	1	0

SECTION 4 · SECURITY

Data and workload protection

If someone gets in, how far can they get?

Score _____ / 10

	QUESTION	YES	PARTLY	NO
4.1	Data is encrypted at rest and in transit, everywhere.	2	1	0
4.2	On AWS, every EC2 instance requires IMDSv2 (the metadata token), and the account default enforces it. AWS documents how to require IMDSv2 and enforce it at account level.[2]	2	1	0
4.3	Production is on a separate network (and ideally a separate account) from dev and staging.	2	1	0
4.4	We have written rules for what data may go into AI prompts: no secrets and no customer personal data unless approved. OWASP Top 10 for LLM Applications 2025: LLM02 Sensitive Information Disclosure.[3]	2	1	0
4.5	Audit logs are on, protected from deletion, and kept long enough for our obligations. In India, CERT-In Directions require ICT logs for a rolling 180 days, kept within India.[9]	2	1	0

SECTION 5 · SECURITY

Software supply chain

Do we know what is inside what we ship?

Score _____ / 10

	QUESTION	YES	PARTLY	NO
5.1	Code and dependencies are scanned automatically in CI/CD.	2	1	0
5.2	Container images are scanned before they reach production.	2	1	0
5.3	Each release produces an SBOM (software bill of materials) that we could hand to a customer. CISA, 2026 Minimum Elements for an SBOM (29 July 2026).[4]	2	1	0
5.4	We can prove where, when and how each build artifact was produced (build provenance). SLSA v1.0 provenance.[5]	2	1	0
5.5	Patch deadlines for critical and high vulnerabilities are written down and met.	2	1	0

SECTION 6 · SCALE

Scalability

What breaks first if traffic doubles next month?

Score _____ / 10

	QUESTION	YES	PARTLY	NO
6.1	Compute and the application tier scale automatically with load.	2	1	0
6.2	We have a load-test baseline and a capacity plan for expected growth.	2	1	0
6.3	The database has a plan for read scaling, connection limits and backups.	2	1	0
6.4	Caching or a CDN sits in front of static content and heavy reads.	2	1	0
6.5	Performance is measured against service level objectives (SLOs) for the user journeys that matter.	2	1	0

SECTION 7 · SCALE

Reliability and recovery

When something fails at 2 am, what happens?

Score _____ / 10

	QUESTION	YES	PARTLY	NO
7.1	Monitoring and alerts go to a named on-call owner.	2	1	0
7.2	Backups are proven by real restore drills, not just by the backup job's success message.	2	1	0
7.3	Every deployment can be rolled back quickly.	2	1	0
7.4	Recovery time and data-loss targets (RTO and RPO) are written down for critical systems.	2	1	0
7.5	There is a written incident response process, and every incident ends with a review and tracked actions.	2	1	0

SECTION 8 · GOVERNANCE

Governance and assurance

Could we pass a customer's security review?

Score _____ / 10

	QUESTION	YES	PARTLY	NO
8.1	Infrastructure is defined as code (for example Terraform, OpenTofu or CloudFormation), and that code is the source of truth.	2	1	0
8.2	High-risk changes need a second person's approval.	2	1	0
8.3	Dev, staging and production are built the same way.	2	1	0
8.4	Every access and change to production can be traced to a person and a time.	2	1	0
8.5	We know which assurance our customers ask for (ISO/IEC 27001:2022, SOC 2) and check ourselves against it each quarter. ISO/IEC 27001:2013 certificates expired or were withdrawn after 31 October 2025 (IAF MD 26).[6] SOC 2 reports come from a CPA examination (AICPA).[7]	2	1	0

YOUR RESULT

Add it up

1. Cost visibility	_____ / 10	2. Cost leaks	_____ / 10
3. Identity, access and secrets	_____ / 10	4. Data and workload protection	_____ / 10
5. Software supply chain	_____ / 10	6. Scalability	_____ / 10
7. Reliability and recovery	_____ / 10	8. Governance and assurance	_____ / 10
Total			**_____ / 80**

0 to 39

Fix the foundations

Start with sections 3, 4 and 7: sign-in, backups and alerts. They carry the most risk for the least effort.

40 to 63

Plug the leaks

The basics are in place. Turn every Partly into a Yes, starting with the lowest-scoring section.

64 to 80

Optimise and automate

Keep it that way: automate the checks so they run without anyone remembering them.

The bands are our rule of thumb for where to start, not an industry benchmark. Any section under 6 out of 10 is worth a look, whatever the total.

Want us to go through it with you?
Free 20-minute review. We read your answers with you and name the first three fixes.

matrixgard.com/review/

SOURCES (CHECKED NOVEMBER 2026)

1. NIST SP 800-63B-4, Digital Identity Guidelines: Authentication (final, July 2025). csrc.nist.gov/pubs/sp/800/63/b/4/final
2. AWS, Modify instance metadata options (require IMDSv2). docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-IMDS-existing-instances.html
3. OWASP Top 10 for LLM Applications 2025. genai.owasp.org/llm-top-10/
4. CISA, 2026 Minimum Elements for a Software Bill of Materials. cisa.gov/sites/default/files/2026-07/2026_cisa_sbom_minimum_elements_508c.pdf
5. SLSA v1.0, Provenance. slsa.dev/spec/v1.0/provenance
6. IAF MD 26:2023, Transition requirements for ISO/IEC 27001:2022. iaf.nu/iaf_system/uploads/documents/IAF_MD26_Issue_2_15012023.pdf
7. AICPA, SOC 2 examinations. aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
8. AWS, Public IPv4 address charge (from 1 February 2024). aws.amazon.com/blogs/aws/new-aws-public-ipv4-address-charge-public-ip-insights/
9. CERT-In Directions under section 70B(6) of the IT Act, 28 April 2022. cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
10. AWS, Amazon EC2 M8g instances. aws.amazon.com/ec2/instance-types/m8g/