

Observability Maturity Scorecard

A practical 25-point assessment for identifying monitoring blind spots, incident-readiness gaps, unnecessary telemetry cost, and the highest-priority improvements.



Use this scorecard with engineering, platform, SRE, operations, security, and leadership stakeholders. Score current evidence, not intended future capability.

Organization: _____

Assessment owner: _____

Date: _____

How to use the scorecard

Score every statement from 0 to 4. Select the score that best reflects consistent, demonstrated practice across business-critical services. If evidence varies widely, use the lower score and record the variance as an improvement opportunity.

Score	Meaning	Evidence standard
0	Not present	No reliable practice or evidence
1	Ad hoc	Occasional, person-dependent, or undocumented
2	Developing	Partly implemented but inconsistent across services
3	Defined	Documented, broadly adopted, and measurable
4	Optimized	Continuously reviewed and tied to operational outcomes

Interpretation

Total	Maturity level	What it usually indicates
0-25	Reactive	Visibility is fragmented and incident response depends heavily on individuals.
26-50	Developing	Useful practices exist, but coverage, ownership, and standards remain inconsistent.
51-75	Defined	Core practices are established and increasingly connected to service outcomes.
76-90	Managed	Observability is governed, measurable, and routinely informs engineering decisions.
91-100	Optimized	Continuous improvement connects telemetry, cost, reliability, and business priorities.

1. Telemetry coverage and quality	0	1	2	3	4
1. We can identify the health of every business-critical service and dependency.	☐	☐	☐	☐	☐
2. Metrics, logs, traces, and events are collected according to defined diagnostic needs.	☐	☐	☐	☐	☐
3. Telemetry includes useful service, customer, transaction, and deployment context.	☐	☐	☐	☐	☐
4. Teams can correlate signals across applications, infrastructure, networks, and third parties.	☐	☐	☐	☐	☐
5. Telemetry quality, cardinality, retention, and collection failures are actively governed.	☐	☐	☐	☐	☐
DOMAIN SCORE					____ / 20

2. Detection, alerting, and incidents	0	1	2	3	4
1. Alerts represent actionable conditions with a named owner and documented response.	☐	☐	☐	☐	☐
2. Critical incidents are detected before or close to the point of customer impact.	☐	☐	☐	☐	☐
3. Teams can move from detection to probable cause without manually searching many tools.	☐	☐	☐	☐	☐
4. Escalation paths, incident roles, and communication expectations are consistently followed.	☐	☐	☐	☐	☐
5. Post-incident learning produces measurable monitoring or reliability improvements.	☐	☐	☐	☐	☐
DOMAIN SCORE					____ / 20

3. Service objectives and ownership	0	1	2	3	4
1. Critical services have clearly identified technical and business owners.	☐	☐	☐	☐	☐
2. SLIs measure outcomes that users and business stakeholders actually experience.	☐	☐	☐	☐	☐
3. SLOs or equivalent reliability targets guide prioritization and release decisions.	☐	☐	☐	☐	☐
4. Dashboards distinguish system activity from customer-impacting service health.	☐	☐	☐	☐	☐
5. Engineering and leadership review reliability performance on a regular cadence.	☐	☐	☐	☐	☐
DOMAIN SCORE					____ / 20

4. Tooling, architecture, and cost	0	1	2	3	4
1. Each observability tool has a defined purpose, owner, and lifecycle decision.	☐	☐	☐	☐	☐
2. The organization understands telemetry volume, retention, and cost by team or service.	☐	☐	☐	☐	☐
3. Duplicate collection and low-value telemetry are identified and reduced.	☐	☐	☐	☐	☐
4. The architecture can evolve without unacceptable vendor lock-in or migration risk.	☐	☐	☐	☐	☐
5. Tool and data costs are evaluated against detection, diagnosis, and business value.	☐	☐	☐	☐	☐
DOMAIN SCORE					____ / 20

5. Governance, skills, and continuous improvement	0	1	2	3	4
1. Observability standards are documented and embedded in service delivery practices.	☐	☐	☐	☐	☐
2. Teams have the skills and access required to investigate production behavior safely.	☐	☐	☐	☐	☐
3. New services inherit baseline telemetry, alerting, dashboards, and ownership controls.	☐	☐	☐	☐	☐
4. Observability gaps are tracked as operational risks with accountable owners.	☐	☐	☐	☐	☐
5. The observability roadmap is reviewed against incidents, costs, growth, and business priorities.	☐	☐	☐	☐	☐
DOMAIN SCORE					____ / 20

Results and priority roadmap

Transfer each domain score below. The total score provides a maturity baseline; the lowest domain and highest-risk services should guide the first improvement cycle.

Domain	Score
Telemetry coverage and quality	____ / 20
Detection, alerting, and incidents	____ / 20
Service objectives and ownership	____ / 20
Tooling, architecture, and cost	____ / 20
Governance, skills, and improvement	____ / 20
TOTAL	____ / 100

Top three operational risks

1. _____
2. _____
3. _____

Action roadmap

Translate the assessment into a small number of owned, measurable improvements. Prioritize risk reduction and learning before large tool migrations.

30-day actions

- 1. _____
- 2. _____
- 3. _____

60-day actions

- 1. _____
- 2. _____
- 3. _____

90-day actions

- 1. _____
- 2. _____
- 3. _____

Decisions or support required from leadership

- 1. _____
- 2. _____
- 3. _____

Need an independent assessment?

Observability Africa helps organizations identify visibility gaps, alerting and incident-response weaknesses, avoidable telemetry cost, and the practical improvements that matter most.

Request an Observability Audit

observabilityafrica.org/observability-audit/

Vendor-neutral guidance for resilient digital infrastructure across Africa and resource-constrained environments.