T-002
SPECIMEN

ISO/IEC 42001 — Signed Audit Report (Score 92/100)

Sample · 2026-05-19 · Bharat NeuroTech · NeuroCortex v2

92
/ 100

Verdict: Ready with caveats

92/100 — 0 fails, 2 warns out of 16. Audit-ready for ISO/IEC 42001 certification with minor closure work.

SIGNED BY DR. SODHI · MAY 14, 2026

Dr. Nitnem Singh Sodhi

Reviewed and signed by Dr. Nitnem Singh Sodhi, ANSI & ABICB-accredited Triple-ISO Lead Auditor (March 2025). Dr. Sodhi is the named lead auditor of record for this engagement and accepts professional responsibility for the findings, recommendations, and sign-off conditions herein.

PROCUREMENT-READY · CLAUSE-CITED · DEFENSIBLE IN STAGE-2 · CERTIFICATION-BODY-ACCEPTED

Executive Summary

Biggest risk: Documentation of output-quality sampling is partial; coverage exists but cadence is not yet formalised.

Top 3 remediations:

1. Formalise weekly output-quality sampling cadence in the Observability Runbook.
2. Add a quarterly residual-risk review to the existing risk register process.
3. Extend training matrix to include the two newly hired AI engineers (2026-Q3).

> *Reviewed and signed by Dr. Nitnem Singh Sodhi, ANSI & ABICB-accredited Triple-ISO Lead Auditor (March 2025). Procurement-ready. Adds per-finding deep recommendations, week-by-week plan, acceptance criteria, and signed auditor's letter on top of the Auto-Audit baseline.*

Risk Heatmap

	PASS	WARN	FAIL
CRITICAL	2	0	0
HIGH	1	1	0
MEDIUM	1	0	0

Findings (5)

Q1 · 5.1 · HIGH

PASS

AI Policy

AI Policy v2.1 (2026-03) signed by CTO with quarterly review. Board has accepted the policy and reviews dashboard monthly.

Evidence cited: AI-Policy-v2.1.pdf, Board-Minutes-2026-04.pdf

Mapping:
• AI-Policy-v2.1.pdf §1 → 5.1 leadership
• Board-Minutes §3 → 5.1 commitment

Remediation: Maintain cadence.

>> AUDITOR RECOMMENDATION (SIGNED)

> The AI Policy is a strong artefact and clearly satisfies clause 5.1. To convert this from a passing control into a competitive advantage at Stage-2, I would (a) extend the quarterly review minutes to include explicit board-level acceptance of residual AI risk, naming each owner, and (b) bind the policy to the SDLC by referencing it from the Change-Advisory-Board template so every model release records compliance against the policy version in force. Both moves are low-effort and immediately demonstrable. They also pre-empt the most common Stage-2 finding I see at this maturity level: 'policy exists but is not linked to operational practice'.

>> WEEK-BY-WEEK PLAN

WK	ACTION	ARTEFACT
W1	Add residual-risk acceptance section to next board minutes	Board-Minutes-2026-Q3.pdf
W2	Reference AI Policy version in CAB template	CAB-Template-v3.docx

>> ACCEPTANCE CRITERIA (STAGE-2)

[✓] Policy version field present in CAB record for last 3 releases
[✓] Board minutes show explicit AI-risk acceptance for the period

Q2 · 6.1.2 · CRITICAL

PASS

AI Risk Treatment

Risk register lists 14 risks, each with named owner, treatment, due date, and residual rating. Executive sign-off recorded 2026-04-22.

Evidence cited: Risk-Register-2026Q2.xlsx, Exec-Signoff-2026-04-22.pdf

Mapping:

- Risk-Register §all → 6.1.2 treatment
- Exec-Signoff → 6.1.2 acceptance

Remediation: Continue quarterly review.

>> AUDITOR RECOMMENDATION (SIGNED)

> Treatment plan is mature and the executive sign-off is exactly what a Stage-2 lead auditor will look for. To harden this control for surveillance audits in year 2 and year 3, formalise the residual-risk review cadence in the policy (today it is implied, not stated) and add a control-effectiveness scoring column to the register so you can trend residual risk over time. This single column converts the register from a static document into a live management instrument and is the difference between a Pass and a Pass-with-Commendation in my experience.

>> WEEK-BY-WEEK PLAN

WK	ACTION	ARTEFACT
W1	Add 'residual-risk trend' column to register	Risk-Register-2026Q3.xlsx
W4	Codify quarterly review cadence in Risk Policy §4.3	Risk-Policy-v1.2.pdf
W12	First quarterly trend review with exec	Risk-Review-2026Q3-Minutes.pdf

>> ACCEPTANCE CRITERIA (STAGE-2)

- [✓] Trend column populated for ≥1 review cycle
- [✓] Risk Policy v1.2 published with cadence clause

Q3 · 8.4 · CRITICAL

PASS

AI System Impact Assessment

AIIA dated 2026-03 covers the triage LLM, lists affected populations, harms, mitigations, and residual risk. Referenced from DPDP DPIA.

Evidence cited: AIIA-Triage-LLM-2026-03.pdf

Mapping:

- AIIA §2 → 8.4 affected parties
- AIIA §5 → 8.4 mitigations

Remediation: Re-run when model is retrained or scope changes.

>> AUDITOR RECOMMENDATION (SIGNED)

> The AIIA is well-structured and the cross-reference to the DPDP DPIA is the right architectural decision — one source of truth on impact, two views (AI and privacy). To future-proof the control, build a lightweight trigger matrix that defines when an AIIA must be re-run (model version bump, training-data domain shift, new affected population, change in jurisdiction). Without this, the next model refresh in 2026-Q4 will create a window where the AIIA is technically stale. Adding the matrix and binding it to the model registry closes that window mechanically. At surveillance audits in year 2 and year 3, the re-trigger matrix is the first artefact a Stage-2 lead auditor will ask to see — having it published and bound to the release gate turns that conversation into a five-minute confirmation rather than a finding worth chasing through change-management evidence.

>> WEEK-BY-WEEK PLAN

WK	ACTION	ARTEFACT
W2	Author AIIA re-trigger matrix	AIIA-ReTrigger-Matrix.pdf
W4	Bind matrix to Model Registry release gate	Model-Registry-Config.yaml

>> ACCEPTANCE CRITERIA (STAGE-2)

- [✓] Re-trigger matrix referenced from Model Registry config
- [✓] Latest model release shows AIIA validity check in CI log

Q4 · 7.2 · MEDIUM

PASS

Competence

Training matrix complete for all four engineers, with certificates attached. New-hire onboarding includes mandatory AI ethics module.

Evidence cited: Training-Matrix-2026Q2.xlsx

Remediation: Refresh annually.

>> AUDITOR RECOMMENDATION (SIGNED)

> Competence evidence is complete and the onboarding module is a credit-worthy addition. Two enhancements will harden this against staff turnover: (a) define a minimum certification half-life (recommend 18 months) so the matrix shows currency, not just attendance, and (b) add a 'role-criticality' column so the Stage-2 auditor sees that the most safety-critical roles carry the most current certifications. This is the cleanest way to demonstrate proportional competence at clause 7.2.

>> WEEK-BY-WEEK PLAN

WK	ACTION	ARTEFACT
W2	Add expiry + role-criticality columns	Training-Matrix-2026Q3.xlsx
W8	First refresh wave for senior engineers	Cert-Refresh-2026Q4.pdf

>> ACCEPTANCE CRITERIA (STAGE-2)

- [✓] Matrix shows expiry date for every certificate
- [✓] No safety-critical role with expired certification

Q5 · 9.1 · HIGH

WARN

Monitoring & Measurement

Output-quality sampling exists at 1.4% weekly, slightly under the documented 2% target. Reviewer rotation is informal.

Evidence cited: Observability-Runbook-v3.pdf

Missing: Formal reviewer rotation

Remediation steps:

1. Document reviewer rotation in runbook [S]
2. Raise sample rate to 2% via automated trigger [S]

Regulator view: Minor finding — does not block certification.

>> AUDITOR RECOMMENDATION (SIGNED)

> This is the only warn-rated control in the audit and it is closeable inside the current cycle. The shortfall from 2% to 1.4% is a sampling-trigger issue, not a coverage issue — there is no need to redesign the pipeline. Codify the reviewer rotation in the runbook with named primaries and backups, and add a CI-side sampling rate alert that fails when weekly coverage drops below 2%. With these two changes in place, the control moves cleanly to Pass before Stage-2 and demonstrates measurable improvement quarter-on-quarter to the surveillance auditor.

>> WEEK-BY-WEEK PLAN

WK	ACTION	ARTEFACT
W1	Document reviewer rotation in Runbook §3.4	Observability-Runbook-v3.1.pdf
W2	Add CI alert for <2% weekly sampling	ci/alerts/sampling.yaml
W4	First two weeks of audited rotation logs	Reviewer-Rotation-Log-2026-W22.csv

>> ACCEPTANCE CRITERIA (STAGE-2)

- [✓] Runbook v3.1 lists named primary + backup reviewers
- [✓] CI alert fires on synthetic <2% scenario
- [✓] Two consecutive weeks at ≥2% sampling on the live pipeline

Auditor's Letter & Sign-off

AUDITOR OPINION (SIGNED)

Based on the engine-generated forensic scoring and my independent review of the cited artefacts for the five spotlighted controls, I am satisfied that the organisation operates an AI Management System that materially conforms to ISO/IEC 42001:2023. The leadership, risk-treatment, and impact-assessment controls (clauses 5.1, 6.1.2, 8.4) are credibly evidenced and management has demonstrated ownership at the executive level.

The single warn finding at clause 9.1 (output-quality sampling) is operational, not architectural, and is closeable inside one audit cycle without re-engineering the monitoring stack. I would expect a clean Stage-2 result, contingent on the closure conditions listed below being demonstrably in place at the time of audit. There is no nonconformity that would, in my judgement, block initial certification.

CERTIFICATION READINESS

The organisation is ready to enter Stage-1 immediately and Stage-2 within 8–12 weeks of this report, subject to closure of the four conditions below. No findings rise to the level of major nonconformity.

CONDITIONS FOR SIGN-OFF (4)

1. Close the clause 9.1 sampling-rate gap (raise to ≥2% weekly with formal reviewer rotation).

2. Publish the residual-risk trend column on the risk register and demonstrate one cycle of trend data.

3. Author and adopt the AIIA re-trigger matrix and bind it to the Model Registry release gate.

4. Add certificate-expiry and role-criticality columns to the training matrix.

Notes: Reviewed against ISO/IEC 42001:2023, Annex A & B. Cross-checked with the organisation's DPDP DPIA where impact analysis overlaps.

SIGNED BY · LEAD AUDITOR OF RECORD SIGNED MAY 14, 2026 · LUCKNOW, IN

Dr. Nitnem Singh Sodhi
ISO 42001 · ISO 27001 · ISO 27701