AUTO-AUDIT · SELF-ATTESTED

T-001
SPECIMEN

ISO/IEC 42001 — Audit Report (Score 78/100)

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

78
/ 100

Verdict: Material gaps

78/100 — 2 fails, 5 warns out of 16. Risk management framework drafted but not yet operationalised.

Executive Summary

Biggest risk: No documented impact assessment for the LLM-assisted triage workflow handling user PII.

Top 3 remediations:

1. Stand up an AI Impact Assessment per Annex B.7 covering the triage LLM, with named owner + review cadence.
2. Wire a model-output sampling pipeline (≥2% weekly) into the existing observability stack.
3. Document the model retirement / rollback procedure and rehearse once per quarter.

> *This is an engine-generated Auto-Audit. Exhaustive across 16 controls. Self-attested. The Dr. Sodhi-signed edition adds named-auditor attestation, per-point deep recommendations, week-by-week action plan, and a procurement-ready auditor's letter.*

Risk Heatmap

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

Findings (5)

Q1 · 5.1 · HIGH

PASS

AI Policy

The organisation maintains a published AI Policy v2.1 dated 2026-03 with explicit ownership by the CTO and a quarterly review cadence.

Evidence cited: AI-Policy-v2.1.pdf, Board-Resolution-2026Q1.pdf

Mapping:
• AI-Policy-v2.1.pdf §1.2 → 5.1 leadership commitment

Remediation: Maintain quarterly review; surface dashboard to board.

Q2 · 6.1.2 · CRITICAL

FAIL

AI Risk Treatment

Risk register lists candidate treatments but no treatment has been formally accepted, with no owner or due date assigned for the top three identified risks.

Missing: Risk treatment plan, Acceptance signatures, Residual-risk register

Red flags: Plan to address risks later this year

Risk if unaddressed: If a model drift incident occurs before treatments are accepted, the organisation cannot demonstrate due diligence in a regulator review.

Remediation steps:
1. Assign named owner to each top-10 risk [S]
2. Draft treatment plan with effort + cost estimates [M]
3. Obtain executive sign-off and publish residual-risk register [M]

Regulator view: A lead auditor would mark this as a major nonconformity — clause 6.1.2 requires a documented, accepted treatment plan, not a roadmap.

Q3 · 8.4 · CRITICAL

FAIL

AI System Impact Assessment

No AI Impact Assessment exists for the triage LLM that processes user PII; only a generic privacy DPIA from 2024 is on file.

Missing: Impact assessment document, Affected-population analysis, Mitigations register

Risk if unaddressed: DPDP Act 2023 §10 and ISO 42001 8.4 both require impact analysis before deployment; absence here exposes the org to both regulator action and ISO nonconformity.

Remediation steps:
1. Run AIIA workshop using Annex B.7 template [M]
2. Document affected populations, harms, mitigations [M]

Regulator view: Major nonconformity. Annex B.7 template is widely accepted — gap is closeable in 4-6 weeks.

Q4 · 7.2 · MEDIUM

WARN

Competence

Two of four AI engineers hold relevant certifications; the remaining two have a training plan dated 2026-02 but no completion records yet.

Missing: Completion certificates for remaining staff

Remediation: Complete training by 2026-Q3 and attach certificates to the matrix.

Q5 · 9.1 · HIGH

WARN

Monitoring & Measurement

Observability stack captures latency and error rate but not output-quality sampling; partial coverage of clause 9.1.

Evidence cited: Observability-Runbook.pdf

Missing: Output-quality sample protocol, Weekly review minutes

Remediation steps:
1. Define ≥2% weekly sample policy [S]
2. Add quality reviewer rotation [S]

Regulator view: Minor — closeable inside the current cycle.

This Auto-Audit covers: engine-generated 16-control forensic scoring, findings, maturity profile, 30/60/90 roadmap, and likely regulator questions. Exhaustive but self-attested.

UPGRADE PATH — DR. SODHI-SIGNED EDITION

The Signed edition adds: per-finding deep recommendation (120–200 words each), week-by-week action plan with named artefacts, Stage-2 acceptance criteria, signed auditor opinion, certification-readiness verdict, and sign-off conditions — under the named attestation of **Dr. Nitnem Singh Sodhi** (ANSI & ABICB-accredited Triple-ISO Lead Auditor).