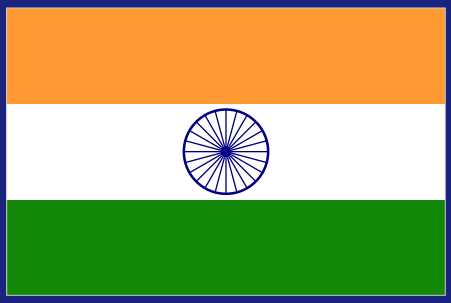

Securing India's National Examinations

A Zero-Trust Reference Architecture to Prevent Paper Leaks, Protect Merit, and Rebuild Public Trust

Roshan Trivedi, CIAM

PAM Product Owner · Identity & Access Management · Cybersecurity Architecture

Version 2.0 · 24 July 2026 · Classification: Public — Policy Discussion

"Every paper leak is preventable — if we design systems that expect failure."

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion
Author: Roshan Trivedi, CIAM | PAM Product Owner, Identity & Access Management

» **Read the full document online: roshantrivedi.co.in/secure-india-exams**

Contents

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

FOREWORD

Foreword

India conducts the largest and highest-stakes examinations in the world. For millions of young Indians, a single examination determines access to medicine, engineering, public service, and social mobility. When a question paper leaks, the damage is not limited to one examination — it corrodes the founding promise of meritocracy on which public trust in the state rests.

This document is an independent, non-commercial policy proposal. It does not critique any individual or institution. Instead it argues a single technical thesis: that examination integrity should not depend on humans reliably following rules under pressure, but on an architecture designed — cryptographically and procedurally — to make compromise structurally difficult and immediately detectable. The approach draws on established disciplines of Zero Trust security, Privileged Access Management, and modern cryptography, and aligns with India's own legal and standards framework: the DPDP Act 2023, CERT-In Directions 2022, the IT Act 2000, and the Public Examinations (Prevention of Unfair Means) Act 2024.

It is offered freely to the Government of India, the Ministry of Education, the National Testing Agency, CERT-In, the National Informatics Centre, and to the public, in the hope that it contributes to a national conversation whose time has come.

— Roshan Trivedi, CIAM

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

EXECUTIVE SUMMARY

Executive Summary

India's national examinations serve over 60 lakh candidates each year across more than 5,000 centres. Recurrent paper leaks — most visibly the NEET-UG 2024 controversy affecting 24 lakh candidates — reveal that procedural safeguards alone cannot protect examination integrity. The estimated cost of a single NEET-scale cancellation is ₹700–1,250 crore, before accounting for the immeasurable erosion of public trust.

This proposal presents a four-pillar Zero Trust architecture: (1) Identity & Access, enforcing biometric verification and zero standing privileges for every actor; (2) a Secure Content Lifecycle, encrypting papers from AI-assisted authoring through geo-fenced, time-locked decryption; (3) a 24×7 National Examination Security Operations Centre with AI-driven anomaly detection; and (4) Managed Exam Infrastructure hardening all 5,000 centres. It further specifies a formal threat model and risk register, AI-specific security controls, a standards compliance matrix, business continuity and assurance frameworks, and detailed breach-response playbooks.

The total programme cost is ₹1,419 crore over three years — ₹79 per candidate per year, less than five percent of the current examination fee. It breaks even on the prevention of a single cancellation.

60L+	5,000+	₹1,419 Cr	₹79	0
candidates/yr	centres	3-yr budget	per candidate/yr	target leaks

A Hindi (□□□□□□) executive summary is available in the online edition:
roshantrivedi.co.in/secure-india-exams

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 1

1. The Problem — Why India's Examinations Are Vulnerable

India operates the world's largest examination infrastructure. A single paper leak cancels an examination for millions of candidates and delivers a devastating signal: that merit does not decide outcomes. Procedural controls have repeatedly failed because they depend on humans reliably following rules under pressure. Only architecture-level security provides reliable, testable protection.

1.1 India's Examination Scale

Examination	Candidates (2024)	Centres	Stakes
NEET-UG	24.06 lakh	~4,750	Only gateway to MBBS/BDS in India
JEE Main	11.68 lakh	500+	Gateway to IITs, NITs, IIITs
CUET-UG	13.48 lakh	313 cities	Central university admissions
UGC-NET	9+ lakh	300+	Lectureship & PhD eligibility
UPSC CSE	~13 lakh	72	IAS, IPS, IFS civil services
SSC / Banking / Railways	5+ crore	Thousands	Government employment

1.2 Root Causes of Leaks

Root Cause	Why Current Controls Fail
Insider Threat	Officials with standing access leak papers for gain. No SOP stops a trusted insider who already holds access.
Physical Custody Failure	Papers transported without cryptographic protection can be opened and photographed mid-transit, undetected.
Weak Digital Controls	Poor access controls permit unauthorised bulk downloads — undetected without continuous monitoring.
Impersonation	Proxies sit exams using forged credentials; without biometric verification, centres cannot confirm identity.
No Centralised Monitoring	Without an SOC, anomalous access the night before an exam — a classic pre-leak signal — goes undetected.
Procedural, not Architectural	Security that relies on humans following rules under pressure fails predictably. Architecture is the only reliable fix.

The NEET-UG 2024 controversy affected 24 lakh candidates, triggered a Supreme Court intervention, and cost an estimated ₹700–1,250 crore. The full three-year programme proposed here costs ₹1,419 crore — it pays for itself by preventing a single cancellation.

1.3 The Economic Cost of Inaction

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Cost Category	Estimate (₹ Crore)	Notes
Re-examination logistics	150–250	Centre hiring, staff, paper, printing, transport
Candidate travel & accommodation	200–400	Millions of families absorbing repeat costs
Academic year delay	300–500	Colleges at partial capacity; delayed intake
Legal & judicial process	50–100	SC hearings, RTI responses, investigations
Mental health & societal impact	Unquantified	Erosion of meritocracy narrative
Total (single NEET-scale event)	700–1,250+	Conservative estimate
3-year security programme (this proposal)	1,419	Break-even on one prevented incident

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 2

2. Security Architecture — Four-Pillar Zero Trust

Four mutually reinforcing pillars, unified by a National Examination Security Operations Centre, designed so that a paper leak becomes structurally impossible — not merely procedurally prohibited. The design aligns with NIST SP 800-207 (Zero Trust Architecture).

> *No user, device, session, or network is trusted by default. Every access request is authenticated, authorised, and logged — regardless of network location or seniority. This applies to ministers, paper setters, and support staff equally.*

Pillar 1 — Identity & Access (Zero Trust)

Biometric verification, zero standing privileges, and just-in-time access for every person who touches an examination. No account — including administrator accounts — holds permanent access. All access is time-limited, dual-authorised, and auto-revoked. A Privileged Access Management (PAM) platform vaults all privileged credentials with full session recording and re-authentication every 15 minutes.

Pillar 2 — Secure Content Lifecycle

Papers are encrypted from AI-assisted authoring through Hardware Security Module (HSM) vaulting to geo-fenced, time-locked decryption at the exam hall. Decryption requires three simultaneous conditions: correct GPS location, authorised time window, and two administrators authenticating together. Digital watermarking embeds a unique invisible identifier (centre ID, session, batch) in every copy, so a leaked photo is traced to its source centre within minutes.

Pillar 3 — Threat Detection & Security Operations

AI-driven User & Entity Behaviour Analytics (UEBA) establishes behaviour baselines for every user. A 24×7 National Exam-SOC runs SIEM/SOAR with 20 pre-built response playbooks executing automatically in under two minutes, plus continuous dark-web and social-media monitoring for paper content.

Pillar 4 — Managed Exam Infrastructure (MEI)

Every centre is hardened with certificate-enrolled cameras, metal detectors, signal management, and an immutable digital chain of custody. Each has a dedicated encrypted network, a local HSM cache, and GPS tamper detection. Computer-vision proctoring augments human invigilation at Tier A centres.

2.1 AI-Assisted Paper Creation Workflow

Questions are created through a secure, AI-augmented process with mandatory human oversight at every gate. Paper setters work in physical isolation on air-gapped terminals — no personal devices, no internet, no external communication. (Detailed AI security controls appear in Section 6.)

Stage	Control
1. AI Generation	AI proposes a question pool strictly from the approved, version-controlled syllabus corpus.
2. SME Review	Subject experts review, reject, or edit each AI-proposed question; no question is accepted unaltered without review.
3. Approval Gate	Minimum two subject experts digitally sign each accepted question using NE-PKI certificates.
4. Moderation	A senior examiner checks balance, difficulty, and clarity of the assembled paper.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Stage	Control
5. Encryption	The HSM encrypts and signs the final paper immediately upon assembly.
6. Vaulting	The encrypted paper enters the NIC national digital vault; access is logged and alerted.

2.2 Centre Security by Tier

Control	Tier A (Urban, 500)	Tier B (District, 2,000)	Tier C (Rural, 2,500)
Network	Dedicated MPLS	VPN + LTE failover	VSAT satellite primary
Endpoints	Locked-down terminals, EDR, signed OS	Same	Same
Local HSM cache	Yes	Yes	Yes
Camera enrollment	Full certificate-based	Full	Full
AI proctoring	AI-assisted + human	Human primary	Human primary
Power backup	4-hour UPS + generator	2-hour UPS	2-hour UPS
GPS tamper device	Yes	Yes	Yes

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 3

3. The Examination Lifecycle — Creation to Destruction

Every step from the moment a question is generated to the moment all copies are destroyed is secured, logged, and — where safe — automated. No step can be performed by a single person without a witness and an immutable log entry.

3.1 Pre-Exam Security Timeline

Day	Milestone	Actions
D-60	SME Isolation Begins	Paper setters enter isolation. Devices surrendered. Air-gapped terminals only. No external communication.
D-45	AI-Assisted Paper Creation	AI generates pool; SMEs review, edit, digitally sign; multi-layer moderation; final paper encrypted into HSM.
D-30	Centre Pre-Inspection	NTA teams inspect all centres for MEI compliance; non-compliant centres decertified and replaced.
D-21	Invigilator Duty Assignment	Randomised centre assignments generated; invigilators told exam date only, not centre.
D-14	Encrypted Paper Distribution	Encrypted files distributed to regional vaults via certificate-authenticated channels; custody hash at every hop.
D-7	Police Coordination Activated	State police briefed; cyber cells on standby; flying-squad routes assigned; CERT-In duty officer notified.
D-3	Building Lockdown	Centre sealed; only pre-enrolled identities may enter; CCTV continuous recording begins.
D-1	Hardware Health Check	All terminals, biometric devices, cameras, and networks verified; HSM local cache loaded; SOC confirms readiness.
D-1 (night)	Invigilator Centre Reveal	Invigilators receive centre assignment via encrypted notification; must report at T-2 hours.

3.2 Exam-Day Protocol

Time	Event	Actions
T-4h	SOC Heightened Readiness	All analysts on shift; real-time dashboard live; CERT-In duty officer confirmed.
T-2h	Candidate Arrival	Biometric verification at gate; QR admit scan; fingerprint + face match; metal-detector sweep; signal management active.
T-30m	Decryption Window Opens	Geo-fence confirmed; time window authorised; two administrators authenticate; paper decrypts; watermark confirmed.
T-0	Exam Commences	Computer-vision proctoring active; human invigilators monitoring; police at perimeter.
End	Answer-Sheet Collection	Dual-authorised collection; digital chain of custody; on-site scanning; sealed sheets GPS-tracked.

3.3 Paper Vaulting — Where Papers Live at Each Stage

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Stage	Location	Protection	Access Control
Authoring	Air-gapped NTA terminal	No network; device certificate; encrypted local storage	SME biometric + PAM
Post-signing (master)	NIC National HSM Vault (primary + DR)	HSM-encrypted; FIPS 140-2 L3; M-of-N key ceremony	DG NTA + 2 custodians
Regional distribution	Regional NIC Secure Vault (4 regions)	AES-256-GCM; regional key fragment	Regional NTA officer
Centre cache	Centre HSM local cache device	Encrypted; geo-locked; time-locked	Two admins + geo-fence + time window
Post-exam (digital)	NIC archive vault	7-year WORM retention; hash verified	Legal/RTI access only; dual authorised
Physical copies	Centre vault → shredding facility	Tamper-evident seal; GPS-tracked transport	Dual-authorised shredding within 24h

3.4 Police & Flying-Squad Coordination

When	Action
D-7	District SP briefed with all centre locations; state cyber cells on standby.
Exam day	Police at perimeter of every centre; plain-clothes officers near Tier A centres.
Real-time	SOC has direct radio contact with centre police officer; any SOC alert triggers police response.
Flying squads	NTA flying squads make surprise inspections at 10% of centres; may replace any invigilator without notice.
Cyber cells	State cyber cells monitor WhatsApp/Telegram; FIR within 2 hours of confirmed leak with watermark evidence.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 4

4. Identity & Access — Every Person, Every Device, Verified

Students, teachers, invigilators, and surveillance devices all hold verified, audited digital identities. No anonymous access; no standing privileges. This section specifies exactly which documents are required and how each identity class is created, enrolled, and deployed.

4.1 Student Digital Identity — Documents Required

Document	Purpose	Verification Method
Aadhaar Card	Primary identity anchor	UIDAI API real-time check
Class 10 / 12 Marksheet	Eligibility confirmation	DigiLocker pull from issuing Board
Category Certificate	Reservation eligibility	Issuing authority digital stamp
Passport photograph	Visual identity	AI face-quality check + liveness detection
Mobile number	OTP-based 2FA	Telecom KYC verification
Email address	Communication channel	Verified via OTP
Signature	Consent & legal declaration	Stored and matched at exam hall

4.2 Student Enrollment Process

Step 1: Online Application + Aadhaar Verification. Candidate submits form; Aadhaar verified against UIDAI in real time; name and DOB must match exactly.

Step 2: Document Upload + AI Verification. Marksheets pulled from DigiLocker; photo checked for quality, liveness, and consistency with Aadhaar photo.

Step 3: Biometric Enrolment Centre Visit. For high-stakes exams: candidate attends an enrolment centre; fingerprints + iris captured and linked to the Examination Identity Number (EIN).

Step 4: Digital Admit Card Issued. Time-limited digitally-signed QR (valid 24h before exam) with encrypted biometric reference; cannot be forged or transferred.

Step 5: Exam Hall Entry. QR scanned at gate; fingerprint matched; face verified by AI camera; seat assigned by randomised system on exam morning only.

4.3 Subject Matter Expert (Teacher) Selection & Isolation

Criterion	Requirement
Experience	Minimum 10 years teaching or research experience in subject
Qualification	Postgraduate or doctoral qualification in subject
Conduct	No prior disciplinary action or criminal conviction
Conflict of interest	Not related to any registered candidate; not employed by coaching institutions
Geography	Not from the same state as any exam centre for the paper
Selection method	Randomly drawn from NTA's encrypted National Examiner Registry
Identity confidentiality	Known only to DG NTA + one Oversight Board member

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Criterion	Requirement
Isolation	Personal devices surrendered; live-in secure facility; air-gapped terminal; CCTV + screen recording throughout
Legal commitment	Confidentiality agreement with ₹1 crore penalty clause

4.4 Invigilator Selection & Randomised Deployment

When	Action
D-21	Notified on duty (exam date only — centre unknown)
D-1 (8 PM)	Encrypted notification reveals centre assignment for the first time
Exam day T-2h	Report to assigned centre; biometric authentication at gate
During exam	Rotated between halls randomly under flying-squad direction
Any time	Flying squad may replace any invigilator without notice

> *The principle of surprise: an invigilator who does not know their centre cannot pre-negotiate access or arrange prohibited assistance. Randomisation is a security control, not an administrative choice.*

4.5 Camera & Device Enrollment

Control	Detail
Device certificate	Each CCTV, biometric reader, and terminal issued a unique device certificate from NE-PKI
Authenticated streaming	Streams TLS-encrypted and source-authenticated; unauthenticated streams blocked and alerted
Tamper detection	Cover, power loss, or movement triggers immediate SOC alert; offline >2 min triggers police notification
Anti-spoof	Feeds checked for looping signatures and static-image patterns
Retention	Footage retained in encrypted WORM storage for 90 days
Recertification	Device certificates expire annually; centres recertify before each exam season

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 5 · NEW

5. Threat Model & Risk Register

A security architecture is only credible if it is derived from an explicit threat model. This section enumerates the adversaries, their objectives and capabilities, the attack surface, a STRIDE analysis, and a scored risk register mapping every major risk to its controlling mechanism and residual exposure.

5.1 Adversary Personas

Adversary	Motivation	Capability	Primary Vector
Malicious insider (paper setter / admin)	Financial gain, coercion	High — legitimate access	Exfiltrate content they can access
Organised leak syndicate	Profit (sell papers/proxies)	High — funded, persistent	Bribe insiders; impersonation rings
External cyber attacker	Profit, notoriety, disruption	Medium–High	Exploit systems, phishing, malware
Nation-state actor	Strategic disruption of institutions	Very high	Supply chain, zero-days, persistence
Opportunist candidate	Personal advantage	Low	Devices, impersonation, copying
Compromised vendor	Varies (often unwitting)	Medium	Supply-chain implant, weak update

5.2 STRIDE Threat Analysis

STRIDE Category	Example Threat	Primary Mitigation
Spoofing	Proxy candidate; forged admit card; fake camera feed	Biometric + liveness; signed QR; device certificates + anti-spoof
Tampering	Paper altered in transit; log manipulation	HSM signing; immutable WORM audit log; hash chain of custody
Repudiation	Insider denies accessing a paper	PAM session recording; non-repudiable digital signatures
Information Disclosure	Paper leak; PII exposure	AES-256-GCM; ZSP; geo/time-locked decryption; watermarking
Denial of Service	Exam-day system outage; network attack	Local HSM cache offline mode; DR failover; DDoS protection
Elevation of Privilege	Admin escalates to key access	Zero standing privileges; JIT + dual authorisation; M-of-N keys

5.3 Risk Register (Top Risks)

Likelihood (L) and Impact (I) scored 1–5; Inherent = L×I before controls; Residual = expected level after the controls in this architecture are in place.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

ID	Risk	L	I	Inherent	Key Control	Residual
R1	Insider leaks pre-exam paper	4	5	20 (Critical)	ZSP, PAM, watermarking, UEBA	6 (Medium)
R2	Paper intercepted in distribution	3	5	15 (High)	End-to-end encryption, hash custody	3 (Low)
R3	Candidate impersonation	4	4	16 (High)	Biometric + liveness at gate	4 (Low)
R4	Cyber intrusion into exam systems	3	5	15 (High)	Zero Trust, SOC, segmentation	4 (Low)
R5	AI paper-tool manipulated	3	5	15 (High)	Air-gap, human gates, output validation (§6)	3 (Low)
R6	Biometric data breach	2	5	10 (High)	Encryption, DPDP controls, no export	3 (Low)
R7	Exam-day system outage	3	4	12 (High)	Local cache offline mode, DR, UPS	4 (Low)
R8	Supply-chain compromise (HSM/vendor)	2	5	10 (High)	SBOM, sovereign sourcing, audit (§9)	4 (Low)
R9	Physical breach at centre	3	3	9 (Medium)	MEI, police, signal mgmt, CCTV	3 (Low)
R10	Collusion (multiple insiders)	2	5	10 (High)	Separation of duties, M-of-N, red team	4 (Low)

5.4 MITRE ATT&CK Alignment

Detection playbooks in the Exam-SOC are mapped to MITRE ATT&CK tactics — Initial Access (phishing, valid accounts), Persistence, Privilege Escalation, Defense Evasion, Credential Access, Collection, and Exfiltration. Each SOAR playbook references the specific technique IDs it detects and the automated response it triggers, enabling measurable detection coverage and gap analysis during red-team exercises.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 6 · NEW

6. AI-Specific Security & Model Governance

Because this architecture uses artificial intelligence both to assist paper creation and to power proctoring and anomaly detection, AI itself becomes an attack surface. A modern security review will expect these risks to be addressed explicitly. This section defines the AI threat taxonomy, the controls, and a governance model.

6.1 AI Threat Taxonomy & Controls

AI Threat	Description	Control
Prompt injection	Malicious input steers the paper-generation model to leak or bias output	Air-gapped model; sanitised, templated prompts; no free-text external input; output validation
Training-data poisoning	Corrupted syllabus corpus biases generated questions	Signed, version-controlled corpus; integrity hashing; human SME review of every question
Model theft / extraction	Adversary copies the model to predict question patterns	On-premise sovereign hosting; no public API; access via PAM; query-rate monitoring
Adversarial examples	Crafted inputs fool proctoring / face match	Presentation-attack detection; ensemble models; human override
Deepfake impersonation	Synthetic face/voice defeats biometric	Liveness detection; multi-modal biometrics (fingerprint + iris + face); challenge-response
Hallucinated / flawed questions	Model invents incorrect or out-of-syllabus questions	Mandatory dual-SME approval; moderation gate; no unreviewed question is ever used
Data leakage via model	Model memorises and emits sensitive content	No PII in training; differential-privacy techniques; output filtering

6.2 Human-in-the-Loop is Mandatory

No AI output — a question, a proctoring flag, or a risk score — is ever actioned autonomously where it affects a candidate. AI accelerates and assists; humans decide. A generated question cannot enter a paper without two subject experts' digital signatures; a proctoring flag cannot exclude a candidate without human confirmation; an anomaly score triggers review, not automatic penalty.

6.3 AI Model Governance Framework

- **Model registry:** every model version is registered, signed, and traceable, with an approved-use record.
- **Model risk assessment:** each model undergoes bias, fairness, robustness, and adversarial testing before deployment.
- **Explainability:** proctoring and anomaly models must provide human-readable justification for every flag.
- **Sovereign hosting:** all models run on Government of India (MeghRaj / GI Cloud) or NIC infrastructure — no foreign cloud, no external LLM API.
- **Continuous red-teaming:** the AI paper tool is adversarially tested each cycle for prompt injection and leakage.
- **Audit logging:** every prompt, output, and human decision is logged immutably for post-exam audit.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

- **Kill switch:** AI assistance can be disabled instantly, reverting to a fully manual, human-only workflow.

> *Principle: AI must never become a single point of failure or an unaccountable authority. Every AI capability in this architecture has a manual fallback and a mandatory human decision gate.*

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 7

7. Governance & Authority

A three-tier governance structure with clear accountability at each level, independent oversight, and mandatory public transparency. No single official — including the Director General of NTA — holds unilateral authority over examination content or security controls.

7.1 Authority Structure

Body	Members	Authority	Cadence
National Examination Security Council (NESC) — proposed	MoE Secretary (Chair), DG NTA, DG NIC, DG CERT-In, retired SC judge, 2 independent experts	Final policy authority; approves architecture changes; reviews audits	Quarterly + emergency
Programme Steering Committee	DG NTA (Chair), NIC Programme Director, CERT-In representative	Operational decisions; budget releases; vendor approvals	Monthly
Technical Working Group	Lead architects (NTA+NIC), SOC lead, PAM admin	Technical design, configuration, playbook revisions	Weekly
State Security Coordinator	State officer liaising with NTA and district police	Centre compliance; local police coordination	Per exam cycle
Independent Oversight Board	2 academics, 1 retired IPS, 1 civil-society rep, 1 student rep	Watchdog; reviews annual audit; publishes transparency report	Annual

7.2 Full Examination Audit Lifecycle

Audit Type	Timing	Auditor	Scope
Centre inspection	D-30	NTA inspection team	MEI compliance, physical security, device certification
System readiness	D-1	Exam-SOC	All systems green, HSM health, connectivity
Real-time monitoring	Exam day	Exam-SOC	All centres, systems, and access events
Post-exam debrief	Within 4 hours	SOC + NTA ops	Incidents, near-misses, custody completeness
Chain-of-custody audit	Within 7 days	NTA Internal Audit	Every event in the immutable log verified
Independent security audit	Annual	CERT-In empanelled / NABCB auditor	ISO 27001 surveillance; full system review
Red / purple team	Bi-annual	External independent team	Full compromise attempt using real TTPs
Parliamentary transparency	Annual	Independent Oversight Board	Public KPI + incident summary

7.3 Data Classification

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Class	Examples	Controls
Top Secret	Question papers (pre-exam)	HSM-only; dual auth; zero standing access
Secret	Biometric data; PAM recordings	Encrypted; PAM-controlled; no export
Confidential	Candidate PII; staff identity	Encrypted; DPDP consent required
Internal	SOC logs; audit trails	Encrypted; 7-year WORM retention
Public	Schedules; results; policies	Digitally signed; integrity-verified

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 8 · NEW

8. Standards & Legal Compliance Matrix

A government evaluation committee will ask a single decisive question: is this auditable against recognised standards and Indian law? This section maps the architecture, control by control, to the frameworks and statutes that govern it — demonstrating that the proposal is not merely sound engineering but a certifiable, legally-compliant system.

8.1 NIST Cybersecurity Framework 2.0

CSF 2.0 Function	How This Architecture Satisfies It
Govern	NESC, Steering Committee, Oversight Board; documented policy, roles, and RACI (§7, §11)
Identify	Threat model, risk register, asset & data classification (§5, §7.3)
Protect	Zero Trust, PAM, HSM/PKI encryption, MEI hardening, ZSP (§2, §4)
Detect	UEBA, SIEM, dark-web monitoring, 24×7 Exam-SOC (§2)
Respond	SOAR playbooks, breach-response scenarios, CERT-In notification (§10)
Recover	BCP/DR, backups, rollback checklist, re-examination protocol (§9, §10)

8.2 ISO/IEC 27001:2022 Annex A Themes

Control Theme	Coverage in This Proposal
Organisational (A.5)	Governance structure, policies, supplier security, threat intelligence
People (A.6)	SME/invigilator vetting, background checks, security awareness training, NDAs
Physical (A.7)	MEI, building lockdown, CCTV, secure vaults, equipment disposal (shredding)
Technological (A.8)	Access control, cryptography, logging, monitoring, secure development, data leakage prevention

8.3 Indian Legal & Regulatory Alignment

Instrument	Obligation	How It Is Met
DPDP Act 2023	Lawful processing of personal & biometric data	Consent at registration; purpose limitation; minimisation; 6-hour breach notice; erasure at 3 years; DPIA (§9)
CERT-In Directions 2022	6-hour cyber-incident reporting; log retention	SOAR auto-notification; 180-day+ log retention; ICT clock sync
IT Act 2000	Legal validity of e-records & signatures	NE-PKI digital signatures; non-repudiation; Sec. 43A reasonable security
Public Examinations (Prevention of Unfair Means) Act 2024	Criminalises leaks & organised cheating	Watermark forensics + immutable logs provide court-admissible evidence for prosecution
Aadhaar Act & UIDAI regs	Lawful, minimal Aadhaar use	Authentication-only (no storage of Aadhaar number beyond token); UIDAI-compliant APIs

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Compliance is designed-in, not bolted-on. Every control traces to a standard or statute, so the system is certifiable (ISO 27001), auditable (CERT-In empanelled), and produces court-admissible evidence under the 2024 Act.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 9 · NEW

9. Resilience, Supply Chain, Assurance, Privacy & Inclusion

This section closes the remaining grey areas that experienced reviewers probe: what happens when systems fail, how the supply chain is trusted, how the system is independently proven secure, how privacy is protected in law and practice, and how every eligible candidate — including persons with disabilities — is included without weakening security.

9.1 Business Continuity & Disaster Recovery (BCP/DR)

System	RTO	RPO	Resilience Measure
Paper decryption at centre	0 (no downtime tolerated)	0	Local HSM cache works offline; backup HSM device per centre
National HSM vault	< 15 min	0	Active-active primary + DR site; M-of-N key recovery
Exam-SOC	< 5 min	< 1 min	Redundant SOC (hot standby) in second region
Identity / biometric service	< 10 min	< 5 min	Cached templates at centre; queued sync on recovery
Network (per centre)	< 5 min	N/A	VPN + LTE + VSAT failover by tier

Backups follow a 3-2-1 strategy (three copies, two media, one off-site, all encrypted). DR drills are conducted quarterly with documented recovery-time evidence reported to the Steering Committee.

9.2 Supply-Chain & Vendor Security

- **Vendor risk tiering:** vendors handling exam content or crypto are Tier-1 and undergo the deepest due diligence and continuous monitoring.
- **SBOM:** a Software Bill of Materials is required for every component; known-vulnerability scanning is continuous.
- **Sovereign sourcing:** HSMs, PKI, and hosting are procured to Indian standards (STQC / Common Criteria), avoiding foreign backdoor risk; Make-in-India preferred via GeM.
- **Secure updates:** all firmware/software updates are cryptographically signed and staged through test before production.
- **No vendor lock-in:** open standards (PKCS#11, SAML/OIDC, STIX/TAXII) preserve portability and auditability.

9.3 Security Assurance & Independent Testing

Assurance Activity	Cadence	Performed By
Vulnerability assessment & pen-test (VAPT)	Quarterly + pre-exam	CERT-In empanelled auditor
Red / purple team exercise	Bi-annual	Independent external team
Responsible-disclosure / bug bounty	Continuous	Public researchers (scoped)
Configuration & patch compliance	Monthly	NIC operations + SOC

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Assurance Activity	Cadence	Performed By
ISO 27001 certification & surveillance	Annual	NABCB-accredited certifier
STQC / Common Criteria evaluation	Per procurement	STQC, Govt. of India

9.4 Privacy by Design & DPIA

A Data Protection Impact Assessment (DPIA) is mandatory before processing begins and is refreshed annually. Privacy is engineered in: data minimisation (only what is needed), purpose limitation (biometrics used only for exam identity), storage limitation (biometric templates deleted three years post-exam), consent at registration, and data localisation within India. A Data Protection Officer is accountable to the Oversight Board, and candidates may exercise DPDP rights (access, correction, erasure) through a published process.

9.5 Accessibility & Inclusion (Without Weakening Security)

Candidate Need	Accommodation	Security Preserved By
Persons with disabilities (Divyang)	Scribes, extra time, assistive tech, accessible seating	Scribes are pre-registered, biometrically enrolled, and vetted like invigilators
Low-connectivity / rural	VSAT satellite; offline HSM cache mode	Same cryptographic controls apply; sync on reconnect
Language diversity	Multi-language papers & interface	Each language variant separately watermarked and version-controlled
Low digital literacy	Assisted registration at Common Service Centres	Assisted sessions logged; identity still Aadhaar-verified

9.6 Security Maturity Roadmap

Level	Stage	Milestone
1 — Initial	Today	Procedural controls; no continuous monitoring
2 — Managed	End of Phase 1	SOC live; PAM & HSM deployed; pilot centres
3 — Defined	End of Phase 2	Standardised controls across 2,500 centres; watermarking universal
4 — Quantified	End of Phase 3	All 5,000 centres; measured KPIs; ISO 27001 certified
5 — Optimising	Year 4+	Continuous red-teaming; post-quantum crypto; predictive threat intel

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 10

10. Breach Response & Rollback

Security architecture cannot guarantee zero incidents — it guarantees a structured, fast, documented response that limits damage, preserves evidence, and restores integrity. These playbooks cover human insiders, external attackers, and automated / AI or system failures.

> *Core principle: detect first, contain second, investigate third, communicate fourth. No single person may suppress or delay breach response. The Exam-SOC duty officer can suspend any session, revoke any credential, and isolate any system without prior escalation approval.*

10.1 Incident Severity Classification

Severity	Description	Response	Decision Authority
P1 — Critical	Confirmed leak; HSM compromise; biometric breach; active attacker	< 5 min (auto-contain)	SOC duty officer (auto) + DG NTA
P2 — High	Suspected leak; credential theft; camera outage; UEBA risk > 85	< 15 min	SOC Tier-2 + NTA security head
P3 — Medium	Single-centre connectivity failure; device tamper; suspicious login	< 30 min	SOC Tier-1 analyst
P4 — Low	Individual anomaly; failed logins below threshold	< 2 hours	SOC alert queue

10.2 Universal 5-Phase Response

1. Detect (UEBA/SIEM alert or human report) → **2. Contain** (isolate system/session/user before investigating) → **3. Eradicate** (remove threat; rotate credentials) → **4. Recover** (restore clean state; verify integrity) → **5. Review** (root-cause analysis; remediate; publish lessons).

10.3 Scenario 1 — Confirmed Paper Leak (Insider)

Step	Action	Owner	Target
1	SOAR suspends suspect sessions; PAM credentials revoked; recordings preserved	SOC (auto)	T+0
2	Watermark extraction identifies source centre and batch	SOC forensics	T+5m
3	Notify DG NTA, MoE security cell, CERT-In duty officer	SOC duty officer	T+10m
4	Police escalation; FIR initiated with watermark evidence	NTA legal + police	T+15m
5	Decision gate: rotate question pool or halt exam?	DG NTA + MoE	T+20m
6	CERT-In incident report submitted (6-hour mandate)	SOC	T+6h
7	Root-cause analysis & remediation plan	Technical Working Group	14 days

10.4 Scenario 2 — External Cyber Attacker

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Step	Action	Owner	Target
1	SIEM detects anomaly; SOAR isolates affected network segment	SOC (auto)	T+0
2	Centres switch to offline local-HSM cache mode	NIC network	T+5m
3	CERT-In cyber cell engaged; threat intel shared	SOC + CERT-In	T+10m
4	HSM integrity verified; key rotation if any doubt	NIC custodians	T+15m
5	Forensic snapshot before remediation; TTPs mapped to ATT&CK	NIC forensics	T+1h
6	Clean rebuild from verified images; full credential rotation	NIC operations	T+4h

10.5 Scenario 3 — System / AI Failure (Rollback)

Situation	Rollback Action	Max Delay
Centre HSM fails	Switch to backup HSM; regional vault re-pushes; emergency split-key decryption (DG NTA + MoE together)	90 min
Geo-fence won't resolve	SOC verifies GPS independently; issues one-time 30-min token (two-analyst approval)	60 min
Biometric system compromised	Halt biometric admission; revert to manual admit + photo; P1 escalation; UIDAI notified	Immediate
AI paper tool suspected manipulated	Kill switch to full manual workflow; regenerate from clean corpus under SME control	Per cycle
AI proctoring mass false positives	Disable AI; human invigilators take over; flags logged for post-exam review	Immediate

10.6 Continuation vs. Cancellation Framework

Situation	Decision	Authority
Leak before exam starts (confirmed)	Cancel; rotate questions if pool available; else reschedule	DG NTA + MoE Secretary
Leak after exam > 50% complete	Continue; enhanced monitoring; full statistical analysis	DG NTA
Single centre disrupted	Cancel that centre only; re-exam affected candidates	DG NTA
Central outage > 2 hours on exam day	Delay max 3 hours; if unresolved, reschedule	DG NTA + Programme Director
Insider access, no leak evidence	Continue; suspect suspended; results held pending forensics	DG NTA
Attacker present, no paper accessed	Continue in offline mode; results held until forensics complete	DG NTA + CERT-In

10.7 Post-Incident Rollback Checklist

Immediate (0–24h): rotate all compromised credentials; take forensic snapshots before any change; lock evidence chain of custody; notify CERT-In within 6 hours; issue factual candidate communication; brief MoE and NESC.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

Short-term (1–14 days): complete root-cause analysis; draft and approve control-gap remediation; red-team re-test the exploited vector; initiate legal proceedings; announce re-examination if required; engage an independent auditor to verify remediation.

> *Transparency requirement: within 30 days of any P1/P2 incident, the Independent Oversight Board must publish a non-sensitive public incident summary. Concealing a breach is itself a governance failure — incident records are immutable and independently auditable regardless of NTA or MoE preference.*

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion
Author: Roshan Trivedi, CIAM | PAM Product Owner, Identity & Access Management

SECTION 11

11. Implementation, Budget, RACI & KPIs

A phased 36-month programme across 5,000 centres, with a transparent budget, clear accountability, and measurable success metrics with go/no-go gates between phases.

11.1 Three-Phase Roadmap

Phase	Timeline	Key Deliverables	Budget (₹Cr)
1 — Foundation	Months 1–6	Exam-SOC live; PAM deployed; HSM/NE-PKI established; UEBA baselines; 200-centre pilot; training	385
2 — Core Deployment	Months 7–18	Encrypted distribution; universal watermarking; biometric enrolment (80%); MEI for 2,000 centres; AI proctoring at 500; dark-web monitoring	539
3 — Full Scale	Months 19–36	All 5,000 centres on MEI; rural VSAT; 100% biometric; post-quantum crypto; ISO 27001; standing red team	495

11.2 Budget by Line Item

Budget Line	Ph 1	Ph 2	Ph 3	Total (₹Cr)
National Exam-SOC	80	40	20	140
HSM / PKI infrastructure	60	30	20	110
PAM platform	30	10	5	45
SIEM / SOAR	40	20	10	70
UEBA platform	25	10	5	40
Biometric enrolment & devices	20	60	40	120
MEI — Tier A (500 centres)	75	0	0	75
MEI — Tier B (2,000 centres)	0	240	0	240
MEI — Tier C (2,500 centres)	0	0	250	250
Computer-vision proctoring	0	50	30	80
Rural VSAT connectivity	0	0	50	50
Training & change management	15	20	10	45
Audits & red team	5	10	10	25
Contingency (10%)	35	49	45	129
TOTAL	385	539	495	1,419

₹79 per candidate per year — under 5% of the current exam fee. Annual operating cost from Year 4: ₹210 crore. Break-even: one prevented NEET-scale cancellation.

11.3 Key Performance Indicators

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

KPI	Baseline	Year 1	Year 3
Paper leak incidents / year	3–5	≤ 1	0
Exam cancellations due to leaks	1–2 / year	0	0
Mean time to detect anomaly	Unknown	< 30 min	< 5 min
Staff with zero standing privileges	0%	80%	100%
Centres at MEI baseline	0%	20%	100%
Papers with digital watermark	0%	100%	100%
Biometric false rejection rate	N/A	< 0.5%	< 0.1%
System uptime on exam day	~95%	99.5%	99.9%
Staff trained in security awareness	0%	70%	100%
Annual independent audit completed	No	Yes	Yes

11.4 RACI Matrix

R Responsible · **A** Accountable · **C** Consulted · **I** Informed

Activity	MoE	NTA	NIC	CERT-In	Centres	Auditors
Define security policy	A	R	C	C	I	I
Architecture design	C	A	R	C	I	C
Deploy HSM / NE-PKI	I	C	A/R	C	I	C
Operate Exam-SOC	I	A	R	C	I	I
Respond to cyber incidents	I	A	R	R	C	I
Centre MEI deployment	I	A	R	I	R	C
Annual security audits	A	C	C	C	C	R
SME selection & isolation	I	A/R	C	I	I	I
Police coordination	C	A	I	C	R	I
Public transparency report	A	R	I	I	I	C

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

SECTION 12

12. Glossary & References

12.1 Glossary

Term	Definition
Aadhaar	India's national biometric identity system (UIDAI); 12-digit ID backed by fingerprint and iris.
AES-256-GCM	Advanced Encryption Standard, 256-bit, Galois/Counter Mode — confidentiality + integrity.
BCP/DR	Business Continuity Planning / Disaster Recovery — keeping services running and recovering after failure.
CERT-In	Indian Computer Emergency Response Team — national cyber incident authority under MeitY.
CRYSTALS-Kyber/Dilithium	NIST post-quantum standards (FIPS 203/204) for key exchange and digital signatures.
DPDP Act 2023	Digital Personal Data Protection Act — India's primary data-protection law.
DPIA	Data Protection Impact Assessment — structured privacy-risk analysis required before processing.
EIN	Examination Identity Number — unique ID for every actor, linked to Aadhaar.
Exam-SOC	National Examination Security Operations Centre — 24×7 monitoring facility.
Geo-fencing	Virtual geographic boundary; decryption permitted only inside the authorised area.
HSM	Hardware Security Module — FIPS 140-2 L3 device holding keys that never leave in plaintext.
JIT / ZSP	Just-In-Time access / Zero Standing Privileges — no permanent access; all access temporary.
MEI	Managed Exam Infrastructure — the mandatory security baseline for every centre.
NE-PKI	National Examination Public Key Infrastructure — dedicated certificate hierarchy.
PAM	Privileged Access Management — governs and records privileged user access.
SBOM	Software Bill of Materials — inventory of components for supply-chain assurance.
SIEM / SOAR	Security Information & Event Management / Orchestration, Automation & Response.
STRIDE	Threat-modelling taxonomy: Spoofing, Tampering, Repudiation, Info disclosure, DoS, Elevation.
UEBA	User & Entity Behaviour Analytics — AI baselining that flags anomalies.
VAPT	Vulnerability Assessment & Penetration Testing.
VSAT	Very Small Aperture Terminal — satellite connectivity for rural centres.
Zero Trust	'Never trust, always verify' — every request authenticated and authorised regardless of location.

12.2 References

1. National Testing Agency. Annual Report 2023-24. nta.ac.in

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion
Author: Roshan Trivedi, CIAM | PAM Product Owner, Identity & Access Management

2. NIST. SP 800-207: Zero Trust Architecture. 2020.
3. NIST. FIPS 203 (ML-KEM) & FIPS 204 (ML-DSA). 2024.
4. NIST. Cybersecurity Framework 2.0. 2024.
5. ISO/IEC 27001:2022. Information Security Management Systems.
6. MeitY. CERT-In Directions under Sec. 70B(6), IT Act 2000. April 2022.
7. MeitY. Digital Personal Data Protection Act 2023.
8. Ministry of Education. National Education Policy 2020.
9. Ministry of Education. Public Examinations (Prevention of Unfair Means) Act 2024.
10. Supreme Court of India. WP (Civil) No. 552/2024 — NEET-UG 2024.
11. NIST. AI Risk Management Framework (AI RMF 1.0). 2023.
12. OWASP. Top 10 for Large Language Model Applications. 2023.
13. MITRE. ATT&CK Framework for Enterprise. attack.mitre.org
14. MITRE. ATLAS (Adversarial Threat Landscape for AI Systems).
15. National Informatics Centre. GIPKI Framework & MeghRaj (GI Cloud). nic.in
16. UIDAI. Aadhaar Authentication API. uidai.gov.in
17. Trivedi, Roshan. Securing India's National Exams — Zero-Trust Reference Architecture. 2026.

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion

"Every paper leak is preventable — if we design systems that expect failure."

Roshan Trivedi, CIAM
PAM Product Owner | Identity & Access Management | Cybersecurity Architecture

linkedin.com/in/roshan-trivedi · github.com/trivediroshan1-ui
x.com/roshi_007 · instagram.com/roshi_007 · fb.com/share/1Jsv6psuJB

Read the interactive version online:
roshantrivedi.co.in/secure-india-exams

© 2026 Roshan Trivedi, CIAM · Public — Policy Discussion
Author: Roshan Trivedi, CIAM | PAM Product Owner, Identity & Access Management