TECHNOLOGY FOR EXAMINATION SECURITY AND TRUST

TEST

A White Paper for a Secure, Resilient and Trustworthy Examination System for India

WHITE PAPER | VERSION 1.0 | SEPTEMBER 2026

"Make the security system highly available and the examination secret highly ephemeral."

FOREWORD

Examinations are among the most consequential processes undertaken by a modern state.

They determine access to education, employment, professional opportunities and public institutions. Millions of candidates invest years of effort, time and resources preparing for examinations in the belief that the process is fair.

When an examination paper is leaked, the damage therefore extends far beyond the paper itself. It affects candidates, institutions, public administration and, most importantly, confidence in merit and fairness.

The conventional response has generally been to add more controls around an existing examination process—more security personnel, more sealed packets, more surveillance and more restrictions.

The premise of this White Paper is different.

The examination process itself should be redesigned so that opportunities for compromise are reduced by architecture.

Technology now permits secure transmission of encrypted information, controlled access, authenticated devices, real-time reconciliation, machine-readable credentials, secure scanning and comprehensive audit trails. These capabilities can be combined with physical security, professional human oversight and institutional separation to create a substantially more resilient examination system.

This White Paper proposes such an architecture under the name:

Technology for Examination Security and Trust — TEST

TEST is not proposed as another examination-conducting agency. It is conceived as an independent national framework for examination security, standards, certification, technology and professional oversight.

Its central philosophy is simple:

Make the security system highly available and the examination secret highly ephemeral.

The proposal is deliberately technology-neutral. It does not depend upon inventing new technology. Much of the required technology already exists. The innovation lies principally in how these technologies, institutions and people are brought together.

Why not make the examination entirely paperless? TEST deliberately does not prescribe a fully computer-delivered model for every high-stakes examination, even though such models are well established for examinations such as the GRE and GMAT and may be entirely appropriate in many settings. India's public examination ecosystem must operate across very large candidate populations, heterogeneous geographies and widely varying institutional infrastructure. Making a computer terminal the mandatory point of delivery would introduce a different concentration of dependencies - standardised workstations at scale, assured power and connectivity, device integrity, screen-based suitability for every subject and examination format, accessibility arrangements, and equitable usability for candidates with differing levels of digital familiarity. TEST therefore remains medium-neutral. It retains paper where paper is operationally appropriate, while using digital systems to minimise the life, movement and exposure of the examination secret. An OE may choose a fully computer-delivered examination where conditions justify it; the TEST security principles should remain applicable without making that delivery model a national precondition.

KEY TO ABBREVIATIONS

OE — Organisation conducting the Examination
EA — Examination Authority
TEST — Technology for Examination Security and Trust
CAFT — Central Agency for TEST
RC — Regional Centre
TTP — TEST Technical Personnel
CTP — Centre TEST Professional
SA — Security Agency
CI — Centre In-charge
QR — Quick Response code
HSM — Hardware Security Module
OMR — Optical Mark Recognition
SEM — TEST Secure Examination Module
IAM — Identity and Access Management
MFA — Multi-Factor Authentication
PKI — Public Key Infrastructure
SIEM — Security Information and Event Management
DR — Disaster Recovery

The abbreviations above are used throughout the White Paper and its annexures.

EXECUTIVE SUMMARY

India's high-stakes examinations operate on a chain of trust extending from question preparation to the final result. The greatest structural vulnerability in the conventional model arises because the final readable examination paper must be printed, packaged, stored, transported and protected for an extended period before candidates enter the examination hall. Every additional custody point creates another opportunity for error, leakage or manipulation.

Technology for Examination Security and Trust (TEST) proposes a different architecture. Its central proposition is to redesign the process so that the examination secret remains encrypted until the last practical moment, is decrypted only in a controlled environment, is printed only after authentication, and is physically exposed only in the quantity operationally required. TEST is not another examination authority. It is a national framework for security standards, certification, technology, resilience and professional oversight.

The examination's ordinary administrative lifecycle remains with the Organisation conducting the Examination (OE) and its Examination Authority (EA). The OE determines the requirement and broad examination parameters and appoints the EA. The EA handles applications, eligibility, candidate allocation, centre allocation, hall tickets and routine candidate communication. TEST security begins after these activities have substantially concluded. The T–45 point used in the paper is an indicative planning reference, not a mandatory minimum period; an EA capable of delivering the required information earlier may do so.

At the heart of TEST is a distributed chain of trusted functions. The Central Agency for TEST (CAFT) generates the final examination paper in a protected environment. Human approvers verify it before encryption. If a paper fails approval, the architecture permits another paper to be generated without weakening the security boundary. The central paper-generation environment itself operates under a sealed-hall/no-unauthorised-device protocol, with geographically separated primary and fallback processing capability.

Encrypted examination packages are transmitted through Regional Centres (RCs) to certified examination centres. At the centre, a permanent TEST Technical Personnel (TTP) and an appropriately deployed Centre TEST Professional (CTP) perform the critical two-person controls. The TTP performs technical authentication and printing operations and undertakes decryption jointly with the designated CTP under two-person authorisation. A CTP independently scrutinises the first printed paper before bulk printing is authorised. TEST Professionals oversee the conduct of the examination process while ordinary invigilation may be performed by trained school/college personnel. The Security Agency controls physical access but does not possess cryptographic authority or routinely enter the examination hall.

TEST uses demand-based printing. A first paper is printed and verified, after which only the required quantity is printed, subject to prescribed operational redundancy. This sharply reduces unused papers, physical handling, storage and destruction. The QR-coded hall ticket provides authenticated candidate identity and carries the candidate's colour photograph; the

precise technical treatment of the photograph within or through the QR mechanism is left to the technical committee. Room allocation need not be embedded in the QR code. A local centre database can return the room assignment when the candidate is admitted, allowing room allocations to be changed without reissuing credentials.

The architecture is deliberately resilient. A full rehearsal is conducted approximately T–24, with the same secure-hall discipline as the live process. CAFT's primary and fallback environments are tested simultaneously, while RCs and centres exercise the complete generate–approve–encrypt–transmit–decrypt–print workflow. If a rehearsal fails, the failure is isolated and corrective action begins immediately, with repeat rehearsal(s) as required. By T–12, the national trust architecture must be demonstrated ready and every candidate must have a viable examination pathway. A LOCAL RED centre may be restored, reconstituted or handled through authorised redistribution; country-wide postponement should arise only from an unresolved SYSTEMIC RED condition affecting the national trust architecture. Failure management continues after T–12 for newly arising local events.

For objective examinations, the answer key is deliberately separated from the question-paper security chain. It is prepared and independently checked after the final paper is approved, with at least one hour allowed for this process, but it is not released to examination centres before the examination begins. Only after T+0 is the authorised key distributed securely to centres and loaded into the scoring environment through controlled TTP+CTP procedures. For descriptive examinations, the Evaluation Key is prepared only after the examination and shortly before evaluation. It remains an evaluation asset and need not be distributed to examination centres. Evaluation emphasises substantive knowledge and the desirable elements of an answer, while still giving appropriate weight to reasoning, expression and presentation.

Post-examination, CTPs perform the operational scanning of answer sheets under the technical supervision of the TTP. The TTP remains responsible for scanner configuration, technical integrity, answer-key loading and technical fault management; scarce technical personnel are therefore not used for repetitive scanning work. Scanned records, scores and audit data are transmitted securely to CAFT, while the corresponding physical material is reconciled, room-wise assembled and securely stored.

TEST is designed for national scale. For planning purposes, a centre ecosystem of approximately 5,000 centres, using 500-, 750- and 1,000-candidate capacity modules, provides the current working national model. One TTP is assigned to each centre, with regional redundancy. CTP deployment is based on the stricter of the candidate and room requirements, with one CTP for up to 100 candidates or three rooms. RCs must have sufficient resources not only to support centres but also to completely reconstitute at least one failed centre and redistribute its candidates if necessary. A centre failure must not automatically become a national examination failure.

TEST also changes the economics of examination security. It eliminates or substantially reduces the need to print, package, transport, store and guard examination papers for weeks. It reduces

surplus material because printing is linked to actual allocated/appearing candidates rather than the entire applicant population, subject to prescribed operational contingency. The resulting savings should be weighed against the investment required for secure technology, professional personnel, redundancy, rehearsals and audit. The real comparison is therefore the lifecycle cost and risk of the legacy physical custody chain against the reusable national infrastructure created by TEST.

TEST does not claim to make a complex national examination system foolproof. Its objective is more practical: to make unauthorised access difficult, detectable and containable; to ensure that ordinary equipment failures do not become examination emergencies; and to ensure that no single person, organisation, technology or physical location can compromise the entire examination. The proposed architecture therefore seeks to create trust not by adding controls around the old process, but by redesigning the process so that the opportunities for compromise are fundamentally reduced.

CHAPTER 1

THE EXAMINATION SECURITY CHALLENGE

A high-stakes examination is fundamentally a chain of trust in which candidates, examining organisations and the public must be confident that the question paper remains confidential, every candidate faces an equivalent test, answers are faithfully recorded and evaluated, and the declared result reflects performance rather than manipulation. Conventional systems often try to create this trust by placing successive layers of physical and administrative security around a question paper that may already exist in readable form for days or weeks. Every additional person, location, movement and period of custody creates another opportunity for leakage, substitution, coercion or error. TEST begins from a different premise: perfect security cannot be promised, but the opportunity for compromise can be radically reduced. Its objective is therefore to shorten the life of the readable secret, reduce the number of people capable of accessing it, make critical actions attributable and auditable, and contain a failure before it compromises the examination as a whole.

1.1 Why Examination Security Matters

A high-stakes examination is a chain of trust.

A candidate trusts that:

- the paper is confidential;
- the correct paper will be administered;
- all candidates will receive an equivalent opportunity;
- answers will be properly recorded;
- the examination will be evaluated fairly.

The examining institution trusts that:

- the examination process will remain secure;
- its personnel will follow prescribed procedures;
- examination material will not be compromised.

The public trusts that merit, rather than access or influence, determines the outcome.

A failure at any critical point can damage all three.

1.2 The Vulnerability of the Existing Model

The conventional examination process often involves:

Question setting → Printing → Storage → Transportation → Distribution → Examination → Collection → Evaluation

Each transition introduces people, physical movement, custody and opportunities for error or compromise.

Adding more controls at each stage can reduce risk, but cannot eliminate the structural vulnerability created by having a readable question paper exist in multiple places for prolonged periods.

1.3 The Fundamental TEST Insight

TEST begins with a different question:

Why should the final examination paper exist in readable form any earlier or in more places than absolutely necessary?

If the paper remains encrypted until shortly before the examination, is decrypted only inside a controlled environment, is printed only after authentication, and the quantity printed is based substantially on actual attendance, several traditional vulnerabilities disappear.

1.4 Security by Architecture

TEST therefore seeks to:

- minimise the number of people who can access sensitive information;
- minimise the time for which readable examination material exists;
- separate technical, physical and administrative responsibilities;
- use independent entities for separable functions;
- build redundancy into critical infrastructure;
- maintain multiple independent records of critical events;
- provide predefined fallbacks;
- preserve a complete chain of custody.

1.5 The Objective

TEST does not claim that a complex national system can be made absolutely "foolproof".

Its objective is more practical:

To make unauthorised access sufficiently difficult, detectable and contained that the examination system no longer depends primarily upon the integrity of a few individuals or the physical security of a paper packet.

CHAPTER 2

THE CURRENT EXAMINATION SYSTEM

The conventional examination lifecycle contains many sound administrative practices, but its security weakness lies in the long physical journey of the question paper. Once a final paper is prepared and printed centrally, large quantities may have to be packaged, transported, stored, guarded, redistributed and ultimately delivered to individual examination centres. The paper therefore passes through several locations and custody points while remaining a valuable readable secret. Strengthening guards, seals, storage rooms or transport arrangements can reduce individual risks, but it does not remove the underlying vulnerability created by the process itself. TEST therefore treats the problem not simply as one of inadequate security but as one of process architecture. Instead of protecting a long chain more intensively, it seeks to shorten that chain and postpone the creation of readable examination papers until they are actually required at the examination centre.

2.1 The Examination Lifecycle

A typical examination broadly involves:

1. Determination of vacancies/requirement.
2. Examination design.
3. Appointment of examination service provider.
4. Advertisement and publicity.
5. Application and eligibility processing.
6. Candidate allocation.
7. Centre allocation.
8. Hall-ticket issue.
9. Question preparation.
10. Printing/distribution.
11. Examination.
12. Collection.
13. Evaluation.
14. Result and post-examination processes.

These activities are not equally sensitive.

2.2 The Important Distinction

Routine examination administration—application processing, eligibility, candidate allocation, publicity and communication—is not necessarily part of the examination-security problem addressed by TEST.

TEST therefore does **not** seek to secure every aspect of examination administration.

The TEST security process begins at a defined point after the administrative process has substantially concluded.

2.3 The Vulnerability Window

The greatest concern arises when the final paper becomes readable and begins to move through the system.

Traditional arrangements can involve:

- multiple custodians;
- physical transportation;
- storage;
- manual distribution;
- large quantities of printed papers;
- extended periods of custody.

TEST seeks to reduce this vulnerability window radically.

2.4 Key Takeaway

The problem is not simply insufficient security.

The deeper problem is a process architecture that creates unnecessary opportunities for compromise.

CHAPTER 3

DESIGN PRINCIPLES FOR TEST

TEST is built around a small set of principles that govern every subsequent part of the architecture. The readable question paper should exist for the shortest technically practicable period; sensitive functions should be separated so that no individual or organisation controls the complete process; access should be limited by role, purpose and time; critical actions should require independent participation and leave an auditable record; predictable failures should be absorbed through redundancy rather than treated as emergencies; and technology should simplify rather than complicate the work of people at the operational level. These principles deliberately shift examination security away from dependence upon secrecy, personal integrity and physical custody alone. The architecture may be technologically sophisticated internally, but the instructions faced by a Centre In-charge, TTP, CTP, invigilator or candidate should remain simple, standardised and difficult to misunderstand.

TEST is based on a small number of principles.

3.1 Minimise the Secret

The final readable paper should exist for the shortest technically practicable period.

3.2 Separate Functions

No individual or organisation should control:

Content → Approval → Encryption → Decryption → Printing → Physical custody → Distribution

as a single chain.

3.3 Least Necessary Access

Every person, device and organisation receives only the access required for its role.

3.4 Time-Bound Access

Sensitive permissions should be:

- examination-specific;
- role-specific;
- device-specific where appropriate;
- time-bound.

3.5 Digital Isolation

Personnel involved in the most sensitive examination operations should work within controlled environments and should not carry unauthorised digital devices into the sealed areas.

3.6 Redundancy by Design

Critical equipment and functions should have appropriate redundancy.

Failure of ordinary equipment should not become an examination emergency.

3.7 Fail Securely

When something fails, it should fail in a way that protects examination integrity.

3.8 Human Verification at Critical Points

Technology should reduce dependence on people, but not eliminate human judgement where it is valuable.

The first printed examination paper, for example, should be independently checked before bulk printing.

3.9 Multiple Witnesses

Critical events should generate independently retained records.

3.10 KISS

The system should be technologically sophisticated where necessary but operationally simple where people interact with it.

Complexity should reside inside the architecture, not in the instructions given to people.

CHAPTER 4

THE TEST ARCHITECTURE

TEST does not replace the organisation conducting an examination or the Examination Authority engaged to administer it. The OE continues to determine why the examination is being held, its broad scope and required standard, while the EA handles applications, candidate administration, hall tickets and related services. TEST introduces a separate trusted security and examination-delivery architecture after these ordinary administrative functions have substantially progressed. At its operational centre is the Central Agency for TEST (CAFT), supported by Regional Centres and a network of certified examination centres. The final paper is generated and approved centrally, transmitted in encrypted form through the RC layer and converted into readable physical form only inside the Secure Hall of an examination centre at the authorised time. Permanent technical professionals, trained operational professionals, Centre In-charges, Security Agencies and certification bodies perform deliberately separated functions so that responsibility is distributed without allowing any one operational participant to control the entire chain.

4.1 TEST Is Not the Examination Authority

The proposed architecture separates:

Organisation conducting the Examination (OE)

Owns the examination.

Examination Authority (EA)

Provides examination and assessment services to the OE.

TEST

Provides the security architecture, standards, certification and professional security oversight.

Security Agency (SA)

Provides physical security.

Centre Certification Agency

Certifies infrastructure readiness.

Regional Centres (RCs)

Provide regional technical and operational coordination.

4.2 TEST Council

The TEST Council is the apex authority.

It establishes:

- standards;
- accreditation requirements;

- security policies;
- certification frameworks;
- technical standards;
- audit requirements;
- emergency authority structures.

4.3 Central Agency for TEST (CAFT)

CAFT is the permanent national executive and operational agency for the TEST architecture. It implements the standards and policies established by the TEST Council; operates the national secure technology, paper-generation, cryptographic-release and monitoring environments; coordinates RCs; maintains the permanent TEST technical cadre; and provides national examination-security command and resilience capability. CAFT does not replace the OE or EA and does not acquire academic ownership of an examination.

Within CAFT, paper generation, human approval, cryptographic control, release authority and audit shall remain functionally separated in accordance with the separation-of-capability principle.

4.4 Regional Centres

Regional Centres provide:

- technical support;
- centre monitoring;
- security coordination;
- emergency response;
- agency oversight;
- alternate regional capability.

RCs shall never become repositories of readable examination papers. Their role is to receive and forward encrypted packages, monitor centre readiness, deploy TTPs and reserves, coordinate recovery, and contain local failures at regional level.

Each RC shall maintain sufficient personnel, equipment and reserve capacity to completely reconstitute at least one failed centre and, where necessary, redistribute affected candidates to other certified centres in the same city or examination cluster.

4.5 Independent Service Providers

EA, Security Agencies and Centre Certification Agencies should be separate entities.

Their functions should not be organically combined.

Each should be accountable to TEST for the functions it performs within the TEST architecture.

CHAPTER 5

TEST SECURITY FRAMEWORK

The security framework converts the design principles into an enforceable chain of trust. TEST does not rely upon encryption alone: trusted identity, approved system configuration, secure paper generation, independent human approval, controlled cryptography, authenticated transmission, time-sensitive decryption, verified printing, physical security and protected audit records work together. Particularly sensitive functions require multi-person participation and appropriate cryptographic controls so that possession of one credential or compromise of one individual does not expose the examination paper. The Regional Centre can transport the encrypted asset without being able to read it, while the examination centre cannot decrypt it before the authorised time. The Secure Hall provides the controlled physical environment in which the digital asset finally becomes a readable examination paper. Security is therefore created by separating capability as well as responsibility, with each participant controlling only the part of the chain required for that participant's function.

5.1 The Security Chain

The principal TEST security chain is:

Trusted Identity

→ Trusted Configuration

→ Secure Paper Generation

→ Human Approval

→ Encryption

→ Secure Transmission

→ Controlled Decryption

→ Controlled Printing

→ Distribution

→ Collection

→ Scanning

→ Secure Storage

→ Audit

5.2 The Trust Core

The most sensitive TEST functions are:

1. Trusted identity.
2. Trusted time.

3. Trusted question configuration.
4. Secure paper generation.
5. Human approval.
6. Cryptography.
7. Controlled release.
8. Trusted evidence.

These functions require the strongest protection and redundancy.

5.3 Digital Isolation

At the critical examination stage, personnel entering the sealed decryption/printing environment should surrender unauthorised digital devices.

Access should be:

- authenticated;
- recorded;
- time-bound;
- physically controlled.

5.4 Physical Security

The Security Agency protects:

- premises;
- personnel;
- access;
- movement;
- examination material;
- sealed areas.

The Security Agency does not receive cryptographic authority.

5.5 Cryptographic Separation

No single individual should possess all permissions required to compromise the cryptographic chain.

Critical cryptographic functions should use appropriate:

- HSMs;
- multi-person controls;
- threshold authorisation;

- independent key-management arrangements.

Separation-of-capability principle: no single individual, pair of individuals, credential, system or operational layer shall possess all capabilities necessary to obtain, alter, prematurely release and conceal a protected examination asset. Dual control is therefore a minimum control, not a complete security model; generation, human approval, cryptographic control, release authority and audit must remain independently attributable.

CHAPTER 6

END-TO-END EXAMINATION WORKFLOW

This chapter brings the entire architecture to life by following an examination from its initial commissioning to post-examination processing. The OE determines the requirement and examination parameters and appoints the EA; the EA advertises the examination, processes applications and issues QR-enabled hall tickets. TEST then takes responsibility for the secure examination chain. Shortly before the examination, CAFT generates the final paper from the controlled question bank, obtains human approval, encrypts it and transmits it through the RCs. At the centre, authorised personnel decrypt it only at the permitted time, print and verify one complete copy, and then print the controlled quantity required for candidates. After the examination begins, the separately prepared objective answer key can enter the scoring environment; after collection, trained CTPs scan answer sheets under TTP technical supervision. Descriptive examinations follow the same secure delivery architecture but retain human evaluation against a subsequently prepared Evaluation Key. Thus pre-examination secrecy, examination-day delivery and post-examination integrity form one continuous auditable process.

During the pre-operational administrative period, the EA should provide TEST and the relevant RCs with periodic aggregate geographical demand data for capacity planning. This need not transfer candidate-level data prematurely; its purpose is to allow centre activation, reserve capacity and regional resource planning to adjust as the actual distribution of applications emerges.

This is the core worked example of TEST.

6.1 Phase A — Examination Administration Before TEST

The **OE**:

- determines the number of vacancies/candidates required;
- determines the broad scope and desired level/difficulty of the examination;
- appoints an accredited EA.

An agreement is entered into between OE and EA.

The **EA**:

- issues advertisement;
- conducts publicity;
- receives applications online and, where prescribed, physically;
- processes applications;
- conducts eligibility and administrative scrutiny;
- finalises candidates;
- allocates candidates and centres;

- prepares examination schedules;
- issues/dispatches hall tickets.

These are ordinary examination-administration functions.

They are **outside the TEST security workflow**.

6.2 TEST Security Commencement — Indicative T–45 Planning Point

TEST security and controlled examination administration begins after:

- candidate allocation is finalised;
- centre allocation is finalised;
- examination date/time are fixed;
- hall tickets have been issued/posted.

This point is designated as the indicative T–45 planning point. It is not an architectural deadline and may be shortened where the EA can securely complete and communicate the required information earlier.

The actual interval will depend on the examination, the hall-ticket delivery mechanism and candidate travel requirements. The essential requirement is that the required candidate and centre information is securely available before the TEST operational chain requires it.

6.3 QR-Coded Hall Ticket

Every hall ticket should carry:

- a secure, digitally authenticated QR code;
- the candidate's colour photograph;
- prescribed candidate/examination information.

The hall ticket should serve as the candidate's examination identity credential/photo ID.

The precise technical treatment of the photograph—whether encoded in the QR, cryptographically linked to it or implemented through another secure method—should be determined by the technical committee.

Candidate applications shall include the registered mobile number, email address and other prescribed contact information required for examination-day communication. Relevant operational data shall be securely available to the RC on a need-to-know basis.

Candidates shall be advised in advance that, in the unlikely event of a centre failure, they may be reallocated within the same city or designated examination cluster. They should check their registered email and mobile messages at approximately T–10 and thereafter until departure for the examination centre.

6.4 Centre Readiness — Two Stages

Stage 1 — Physical/Technical Readiness

To be certified at least **T–2 days**:

- infrastructure;
- secure hall;
- printers;
- certified printing capacity;
- scanners;
- power backup;
- connectivity;
- CCTV;
- shredders;
- emergency arrangements.

Stage 2 — Human Readiness

Closer to examination day:

- Centre In-charge;
- TEST Technical Personnel;
- Centre TEST Professionals;
- Security Agency;
- invigilation personnel;
- technical support.

The centre is not considered fully ready until both stages are certified.

6.5 T–24 Hours — Full System Rehearsal

A complete end-to-end rehearsal is conducted approximately one day before the examination. The same strict secure-hall/no-unauthorised-device protocol used for the live process applies. CAFT must exercise both primary and fallback environments, while the RCs and examination centres simultaneously exercise the complete operational chain.

Only the minimum test material required to demonstrate the process is printed, and all such material is destroyed under controlled conditions after the rehearsal.

The rehearsal verifies, simultaneously:

- systems;
- connectivity;
- authentication;
- encryption/decryption path;

- printing;
- scanning and objective-key loading simulation;
- communication;
- monitoring;
- contingency arrangements.

By T–12, the national trust architecture must be demonstrated ready and every candidate must have a viable examination pathway. LOCAL RED centres may continue through restoration, reconstitution or authorised redistribution; only an unresolved SYSTEMIC RED condition should threaten the country-wide examination. T–12 is a readiness gate, not the end of failure management.

If the rehearsal fails, the failure is isolated and corrective action begins immediately. The affected function is restored and the rehearsal repeated at the earliest practicable time. Repeat rehearsals may continue during the available recovery window.

6.6 T–3 Hours — Live Secure Hall Activation

The decryption and printing hall is sealed under CCTV.

Only authorised personnel enter.

They surrender unauthorised digital devices.

The Security Agency controls physical access.

The TEST Technical Personnel and authorised TEST Professionals operate within the controlled environment.

6.7 TEST Technical Personnel

Every examination centre has **one TEST Technical Personnel**, a permanent CAFT technical employee deployed through the RC.

The TTP is responsible for:

- technical authentication;
- secure package verification;
- joint decryption with the designated CTP under two-person authorisation;
- printer authentication;
- printing of the first paper;
- technical operation of subsequent printing;
- technical fault management;

The TTP does not create, edit or independently approve the examination paper or answer key.

for objective examinations, technical authentication and controlled loading of the authorised answer key after T+0, jointly with the designated CTP;

- communication with the RC; scanner/scoring configuration and technical oversight of scanning; secure transmission of technical data.

The TTP cannot independently authorise bulk printing.

6.8 Centre TEST Professionals

Centre TEST Professionals are independently recruited, trained and certified personnel.

CTP deployment shall be based on the stricter operational requirement: one CTP for up to 100 candidates or three examination rooms, with the applicable limit determining the deployment.

Their responsibilities include:

- process oversight;
- room readiness;
- distribution supervision;
- collection;
- reconciliation;
- room-wise sorting;
- operational scanning under TTP technical supervision;
- material sealing;
- adherence to TEST procedures.

One designated CTP at the centre performs the independent first-paper verification. CTPs also undertake the physical scanning operation after collection, under the technical supervision of the TTP.

6.9 First-Stage Printing

Printing begins with the mandatory first-paper check. The designated production printer first produces exactly one complete, automatically collated paper and pauses for independent scrutiny. Other printers must already have been authenticated and proven during rehearsal; live bulk output from them is permitted only after the first complete paper has been approved and remains subject to print-quality monitoring.

After the designated CTP approves the first complete set, the centre ordinarily prints an initial tranche based on the examination-specific, empirically validated planning percentage (approximately 50% may be used as the reference design assumption), subject to examination-specific instructions.

The initial tranche is held under controlled custody while candidate entry and QR authentication establish the actual room-wise attendance.

6.10 First-Paper Verification

The CTP checks:

- examination identity;
- set;
- page count;
- page sequence;
- language/version;
- format;
- printing quality;
- prescribed identifiers.

Only after successful verification is the bulk print command authorised under the prescribed two-person control.

Decrypt once. Print one. Verify independently. Then print only what is required.

6.11 Second-Stage Printing

Candidate hall-ticket QR codes are scanned at entry.

By approximately **30 minutes before examination time**, the centre has a reliable picture of:

The QR credential authenticates the candidate; room allocation is returned by the local centre database and need not be embedded in the QR code. This permits room changes without reissuing the candidate credential.

- candidates present;
- room-wise attendance;
- set allocation;
- remaining paper requirement.

The remaining quantity is calculated as:

Actual candidates present + prescribed operational contingency – usable papers already printed

Only the required balance is printed.

This substantially reduces:

- unused papers;
- paper handling;
- storage;
- destruction;
- reconciliation effort.

6.12 Distribution

Question papers are packed room-wise.

The TEST Professional verifies:

- room;
- set;
- quantity;
- custody.

The Security Agency secures physical movement.

The Centre In-charge ensures institutional cooperation.

6.13 Examination

Invigilation is performed by authorised institutional examination personnel under the Centre In-charge.

TEST Professionals oversee adherence to the prescribed examination process.

They particularly monitor:

- proper distribution;
- collection;
- material handling;
- room-wise reconciliation;
- compliance with TEST procedures.

6.14 Collection

At the end of the examination:

Answer sheets → collected room-wise

Question papers → accounted for

Unused material → reconciled

The TEST Professional verifies the count.

6.15 Scanning and Scoring

Answer sheets are scanned at the centre on the day of the examination.

The digital record includes the appropriate:

- candidate identifier;
- examination;

- room;
- set;
- answer-sheet number.

The scan is transmitted securely to the central repository.

For objective examinations, the authorised answer key is loaded only after T+0 through the prescribed TTP+CTP control. The scoring record remains linked to the answer-sheet image and answer-key version.

The scoring environment shall support question-level status controls so that a disputed or defective objective question does not hold up the remainder of the scoring process. A question may be marked VALID, WITHHELD, CANCELLED or REVISED under authorised academic control. Because the answer-sheet image, recognised response, answer-key version and scoring rule remain linked, affected scores can be recomputed without rescanning the answer sheets.

CTPs perform the operational scanning in controlled batches. The TTP configures and monitors the scanning environment, verifies technical integrity and manages technical exceptions; the TTP is not required to perform the repetitive scanning of the centre's answer sheets.

6.16 Objective Answer Key and Scoring

For objective examinations, the answer key is a separate controlled asset and is not transmitted with the question paper.

After final paper approval, the designated key setters shall receive at least one hour to prepare the objective answer key, followed by sufficient independent checking and finalisation time. The key is not released for distribution before T+0, when the examination has commenced.

The authorised key is transmitted through CAFT → RC → Centre and loaded into the scoring environment through the prescribed TTP + CTP control. The TTP provides technical oversight; the CTP participates in the controlled loading and verification process.

Scanning is performed operationally by CTPs under TTP technical supervision. The system links the candidate's image, recognised responses, answer-key version and score, providing a reproducible audit trail.

6.17 Physical Storage

After scanning:

- answer sheets;
- question papers;
- relevant examination material

are associated/stitched as prescribed, assembled room-wise, securely sealed and stored.

The digital record and physical bundle remain linked.

Physical originals should not ordinarily be opened for routine revaluation.

Exceptional opening requires authority and recorded reasons.

For descriptive examinations, no Evaluation Key is required at the examination centre. It is prepared after the examination, independently checked and frozen shortly before evaluation, and released only within the authorised evaluation environment.

6.18 The Complete Chain

OE → EA → Candidate allocation → Hall ticket → indicative TEST start → Centre readiness → T–24 rehearsal → T–12 final gate → CAFT paper generation/approval → encryption → RC → centre decryption → first print → independent verification → controlled batch printing → QR attendance/room allocation → examination → T+0 objective-key release where applicable → collection → CTP scanning under TTP supervision → physical reconciliation → secure storage → evaluation/audit

CHAPTER 7

TEST TECHNOLOGY ARCHITECTURE

TEST is not conceived as one enormous national computer system whose continuous availability is necessary for every examination activity. It is a distributed architecture of trusted functions in which CAFT, Regional Centres and examination centres perform defined roles with appropriate redundancy, interoperability and local resilience. Technology provides identity and access control, secure question-bank management, paper generation, encryption, authenticated transmission, trusted time, controlled decryption and printing, candidate verification, scanning, scoring and audit. Critical systems must have fallback capability, while centre operations should be capable of continuing through predictable failures of individual printers, networks or power sources. The purpose of the technology architecture is therefore not technological sophistication for its own sake. It is to ensure that the security rules established by TEST are enforced consistently by the system itself and that a failure in one component does not automatically propagate through the national examination network.

7.1 Technology Philosophy

TEST should be designed as a **distributed architecture of trusted functions**, not as one continuously connected national system on which every activity depends.

The architecture should provide:

- redundancy;
- interoperability;
- modularity;
- controlled degradation;
- auditability.

7.2 Critical TEST Processing

The most sensitive paper-generation and cryptographic functions should operate through two geographically separated processing environments. CAFT shall be capable of generating a second or third paper if the first generated paper fails human approval, without weakening the secure boundary.

They should have:

- the same approved data/configuration;
- independently provisioned hardware;
- independently engineered software environments;
- separate power;
- separate connectivity;

- appropriate security controls.

The secondary environment must be capable of performing the complete function if the primary becomes unavailable.

7.3 Functional Redundancy

The objective is not simply:

Two servers.

It is:

Two independently survivable systems capable of performing the same trusted function.

This protects against:

- hardware failure;
- site failure;
- software failure;
- network failure;
- common operational problems.

7.4 Trusted Time

TEST should use multiple authoritative time references.

Telecommunications infrastructure and other established time sources can provide the necessary reference, with cross-verification.

TEST need not create an unnecessarily elaborate independent national clock.

7.5 Central Secure Processing

CAFT paper-generation and cryptographic operations, together with the prescribed human-approval process, shall be conducted inside a controlled secure environment under the same no-unauthorised-device philosophy applied to the centre Secure Hall. The respective functions remain separately attributable and access shall be authenticated, recorded and subject to appropriate multi-person control.

7.6 Local Processing

Where possible, non-critical functions should tolerate temporary loss of central connectivity. For example, securely scanned answer sheets may be stored locally and transmitted when connectivity is restored. The final examination paper, however, remains subject to the prescribed controlled-release process.

For objective examinations, the technology stack shall also support delayed answer-key release after T+0, authenticated distribution and controlled loading into the scoring environment. For

descriptive examinations, it shall support secure preparation, versioning and controlled release of the Evaluation Key only after the examination.

CHAPTER 8

GOVERNANCE FRAMEWORK

Technology can enforce rules, but it cannot decide who should make those rules or who should be accountable when they are breached. TEST therefore requires an institutional governance structure centred on the TEST Council, which sets standards for security, accreditation, certification, technology, audit and professional competence. Operational roles remain deliberately separated: paper generation is distinct from paper approval; technical operation from physical security; examination administration from TEST security; and evaluation from result certification. Permanent TEST Professionals provide institutional continuity and technical competence, while the larger certified CTP pool provides trained operational capacity for examination-day deployment. Independent audit, professional certification, incident investigation and controlled software/version management ensure that the architecture itself remains subject to scrutiny. Governance therefore provides the human and institutional counterpart to TEST's technical controls: technology constrains what participants can do, while governance determines who may do it, under whose authority and with what accountability.

8.1 TEST Council

The TEST Council is the apex authority.

It is responsible for:

- standards;
- accreditation;
- certification;
- security policy;
- technology standards;
- audit;
- professional certification;
- emergency governance.

8.2 Central Agency for TEST (CAFT)

CAFT is the executive arm of the TEST architecture. The TEST Council sets standards, accreditation, policy and oversight; CAFT implements and operates the national system within those standards. CAFT commands national TEST operations, secure technology and resilience, supervises RCs and the permanent technical cadre, and operates the secure paper-generation and cryptographic-release environments subject to functional separation and independent audit.

8.3 Examination Authority

EA should be an independent professional entity.

Its services may be engaged by OEs.

EA works within TEST's security framework but does not control TEST.

8.4 OE

The OE:

- owns the examination;
- determines vacancies/requirement;
- specifies broad examination scope and difficulty;
- appoints EA;
- participates in final paper approval.

8.5 Question Bank

For examinations covered by TEST, the question bank should be developed within the approved secure process.

Where appropriate, OE may nominate **two subject experts**.

They work with at least four EA subject experts in a controlled environment to develop a controlled question bank containing not less than ten times the number of questions required, with no prescribed upper limit. The same minimum multiplicity principle shall apply, suitably adapted, to objective and descriptive examinations.

The resulting question bank is the controlled source from which the examination is generated.

The arrangement should preserve:

- OE ownership of the examination;
- EA professional assessment responsibility;
- TEST security of the process.

8.6 Final Paper Generation and Human Approval

The final paper is generated by the CAFT secure paper-generation system from the approved question-bank/process environment. Designated human approvers, including the OE's authorised representative(s) and appropriate assessment experts, review the generated paper before encryption.

The approval process is controlled, time-bound and audited. If the first generated paper is rejected, the architecture shall permit a second or, where necessary, a third paper to be generated while the approval window remains open.

The approval process is controlled, time-bound and audited.

For objective examinations, the answer key is a separate controlled asset. After final paper approval, the key setters receive at least one hour for preparation, followed by independent checking and finalisation; the key is not released to examination centres before T+0. For descriptive examinations, the Evaluation Key is prepared only after the examination and shortly before evaluation.

8.7 Security Agency

The Security Agency:

- is accredited by TEST;
- is responsible for physical security;
- secures personnel and premises;
- controls access;
- protects material movement;
- supports incident response.

It does **not** possess cryptographic authority.

8.8 Centre Certification Agency

The Centre Certification Agency certifies:

- infrastructure;
- equipment;
- secure hall;
- power;
- communications;
- physical security requirements;
- printing capacity.

It is accountable to TEST and monitored through RCs.

8.9 TEST Professional Cadre

All personnel working above the RC level in security-sensitive functions should be permanent CAFT employees serving as TEST Professionals appropriate to role.

They may be employed in categories such as:

- technology;
- cybersecurity;
- cryptography;

- operations;
- audit;
- assessment technology;
- regional management;
- resilience.

8.10 Regional Personnel

RCs should have the minimum permanent CAFT/TEST staff required for their assigned workload and resilience obligations.

For physical examination-security oversight, TEST may explore the use of specially trained Territorial Army personnel, subject to applicable legal and service provisions.

Such personnel would undergo specialised TEST training and periodic refresher training.

8.11 Centre TEST Professional Pool

Centre TEST Professionals should be:

- independently recruited;
- competitively selected;
- trained;
- certified;
- registered with TEST.

They may have regular employment elsewhere and undertake TEST assignments as additional professional work, subject to conflict-of-interest requirements.

A 20-lakh-candidate examination may require approximately 20,000 operational CTPs on the one-per-100-candidates principle, subject to the room-based deployment rule.

A national certified pool of approximately 30,000 provides useful reserve and surge capacity for a large examination ecosystem; the actual pool should scale with simultaneous examination demand.

8.12 Centre In-charge

The Centre In-charge should ordinarily be:

- the Principal/Head of the host school/college/institution; or
- a suitably senior colleague designated by the Head.

The Centre In-charge ensures cooperation of institutional personnel.

The Centre In-charge has institutional responsibility.

The TEST Professional has independent responsibility for TEST security procedures.

8.13 Separation of Duties

The four centre-level roles are deliberately distinct:

Function	Principal/CI	TTP	CTP	Security Agency
Institutional command	✓			
Decryption		✓ technical	✓ joint	
First print		✓		
First-paper verification			✓	
Bulk printing		✓	✓ approval	
Process oversight			✓	
Physical security				✓
Distribution/collection oversight			✓	✓ physical
Scanning		✓ technical oversight	✓ operation	
Incident escalation	✓	✓	✓	✓

No single participant controls the entire security chain.

CHAPTER 9

TECHNOLOGY STACK AND MARKET FEASIBILITY

Although TEST proposes a different examination architecture, it does not depend upon the invention of fundamentally new technology. Its principal components—identity management, secure databases, assessment engines, cryptography, hardware security modules, secure networking, trusted time, controlled printing, QR credentials, high-speed scanning, scoring software and audit systems—already exist in mature commercial or institutional forms. The challenge is to select, integrate and configure these technologies so that they collectively enforce the TEST security model at national scale. Wherever possible, the architecture should therefore use proven standards and interoperable products rather than proprietary dependence on a single supplier. Implementation studies and competitive procurement would determine the precise products, capacities and configurations. The feasibility question is consequently less whether the required technology exists and more whether mature technologies can be integrated, tested and operated reliably under the governance, security, timing and resilience requirements established by TEST.

TEST should use mature technology wherever possible.

9.1 Principal Technology Layers

1. Identity and access.
2. Question-bank security.
3. Assessment and paper generation.
4. Cryptography.
5. Secure networking.
6. Centre devices.
7. Printing and scanning.
8. Data and audit.
9. Monitoring and resilience.

9.2 Market Pointers

The following are **illustrative market categories, not vendor recommendations**:

TEST requirement	Existing technology category
Identity	IAM, MFA, PKI
QR credential	Digitally signed QR
Question bank	Secure content/database platforms
Paper generation	Assessment engines and secure workflow
Cryptography	HSM/PKI

TEST requirement	Existing technology category
Secure transmission	VPN/private networks/SD-WAN
Printer control	Enterprise print management
Scanning	OMR/high-speed document scanning
Security monitoring	SIEM/SOC
Audit	Immutable/WORM/append-only systems
DR	Replicated data centres/cloud/private infrastructure
Secure APIs	API gateways
AI assistance	Enterprise AI/ML platforms
Secure processing	Confidential computing

The inclusion of such technology pointers demonstrates that TEST is **not dependent upon futuristic technology**.

9.3 AI

AI may assist with:

- question quality;
- duplicate detection;
- ambiguity detection;
- statistical analysis;
- anomaly detection;
- security monitoring.

AI should not replace accountable human decision-making in critical examination matters.

9.4 QR Credentials

Secure QR technology should be used for hall-ticket authentication and attendance.

The exact technical treatment of the photograph should be determined during implementation.

9.5 Technology Principle

TEST is an integration and architecture challenge, not a technology-invention challenge.

CHAPTER 10

IMPLEMENTATION STRATEGY

A national examination-security architecture should not move directly from concept to nationwide deployment. TEST must first establish its institutional, professional and technical foundations and then prove the architecture under progressively demanding conditions before it is entrusted with high-stakes examinations at scale. The implementation philosophy is therefore prove, pilot, refine, scale and institutionalise. Early phases establish the legal and governance framework, permanent professional cadre, Regional Centres, technology platforms, certified centre network and training system. Controlled pilots then test the complete chain—including deliberate failures—under realistic examination conditions. Subsequent expansion should occur only after evidence demonstrates that paper generation, secure transmission, centre printing, candidate handling, scanning, recovery and audit can meet prescribed performance standards. National deployment is therefore the outcome of demonstrated capability rather than an assumption built into the proposal, and detailed specifications and procurement quantities should emerge from pilots and engineering studies rather than being prematurely frozen in the White Paper.

10.1 Implementation Philosophy

TEST should follow:

Prove → Pilot → Refine → Scale → Institutionalise

10.2 Phase I — Establish TEST

- Legal framework.
- TEST Council.
- Core professional cadre.
- Standards.
- Accreditation framework.
- Initial RCs.

10.3 Phase II — Build Core Technology

Develop:

- secure question-bank environment;
- paper-generation system;
- cryptographic infrastructure;
- identity;

- secure transmission;
- audit;
- monitoring.

10.4 Phase III — Build Centre Ecosystem

- Centre standards.
- Centre Certification Agencies.
- Security Agencies.
- TTP deployment.
- CTP certification.

The certified CTP pool shall be materially larger than the expected peak simultaneous deployment. CTPs constitute a trained deployable national pool rather than a permanent establishment of equal size to the peak requirement; sufficient availability reserve must therefore be maintained for absence, replacement and regional surge requirements.

- Training.

10.5 Phase IV — Controlled Pilot

A limited examination should test the **complete TEST chain**.

10.6 Phase V — Stress Pilot

Test:

- large candidate numbers;
- simultaneous activity;
- printing;
- scanning;
- network load;
- cryptography;
- RC operations;
- failure scenarios.

The stress pilot shall include adversarial recovery tests rather than only normal-load demonstrations. Without advance operational warning, at least one centre should be declared failed and the RC required to diagnose and reconstitute it within the recovery window. A separate exercise should make reconstruction unavailable and require the RC to redistribute candidates, transfer authorised incremental candidate data, update receiving-centre databases and demonstrate successful candidate notification and admission.

10.7 Phase VI — Major Deployment

Only after independent validation should TEST be deployed for a major examination.

10.8 Phase VII — Scale

The hypothetical:

20 lakh candidates / approximately 5,000 centres

should be treated as a national planning benchmark rather than necessarily the first live deployment. Centre capacity should be modular at approximately 500, 750 and 1,000 candidates, subject to physical certification.

10.9 Independent Validation

Every major stage should undergo independent:

- cybersecurity assessment;
- performance assessment;
- centre audit;
- operational review;
- red-team testing.

10.10 Professional Certification

The Centre TEST Professional cadre should be created progressively.

The basic certification programme may be designed around approximately **one week of intensive training**, followed by certification.

Specialised personnel will require additional training.

Certification should be:

- personal;
- time-bound;
- renewable;
- subject to continuing training;
- suspendable/revocable.

CHAPTER 11

BUSINESS CONTINUITY, FAILURE MANAGEMENT AND RESILIENCE

TEST assumes from the outset that equipment will fail, communications will be interrupted, personnel may become unavailable and individual centres may occasionally become unusable. Its resilience therefore comes not from pretending that such events can be eliminated but from ensuring that predictable failures remain local. Printers, scanners, power and communications have appropriate redundancy; CAFT has geographically separated capability; RCs maintain technical reserves and centre-recovery resources; and failed centres can, where necessary, be reconstructed or their candidates redistributed to available certified capacity. The full system is rehearsed before the examination so that weaknesses are discovered while there is still time to correct them. A failed centre should not automatically become a failed city, and a failed city or region should not automatically become a failed national examination. The governing objective is containment: things may go wrong without the whole examination going wrong.

11.1 Design for Failure

TEST should not merely plan for failures.

It should **engineer predictable failures out of the emergency-management system**.

11.2 Built-In Redundancy

Critical centre requirements should include normal redundancy for:

- printers;
- scanners;
- power;
- network;
- critical equipment.

A routine printer failure should therefore not be treated as a major incident.

11.3 Secure Examination Module

Each centre should have a pre-designated secure area capable of receiving a:

TEST Secure Examination Module (SEM)

The SEM would be a transportable, pre-certified secure examination facility capable of supporting essential functions if the permanent secure hall becomes unusable.

Its detailed form—containerised, modular or otherwise—should be determined during implementation.

11.4 TEST Technical Personnel

One permanent TTP at each centre provides immediate technical capability.

This significantly reduces dependence on remote assistance.

11.5 Failure Hierarchy

Level 0 — Built-in redundancy

Equipment failure handled locally.

Level 1 — Local fallback

Standby equipment/SOP/SEM.

Level 2 — Regional intervention

RC assumes coordination.

Level 3 — Security incident

TEST Security/Security Agency response.

Level 4 — TEST systemic failure

National-level continuity mechanism.

11.6 Residual Systemic Risk

Failure of the TEST trust architecture itself is qualitatively different from equipment failure.

The principal defence is:

- geographical separation;
- independent hardware/software;
- independent power/connectivity;
- functional redundancy;
- multiple authoritative records;
- controlled degradation;
- independent validation.

The final systemic-continuity design should be established through specialised technical engineering before national deployment.

TEST should not claim that this risk can be eliminated by simply duplicating servers.

11.7 Core Resilience Principle

The best failure-management system is one that prevents ordinary failures from becoming incidents.

11.8 Rehearsal Recovery and Final Gate

T–12 is the final readiness gate for the national trust architecture and for establishing a viable examination pathway for every candidate. It does not require every originally nominated centre to remain GREEN. At T–12, a local RED centre may be contained through restoration, reconstitution or authorised redistribution; only a genuinely SYSTEMIC RED condition affecting the trusted national architecture should place the country-wide examination itself at risk.

T–12 is a readiness decision point, not the end of failure management. Failures arising after T–12 continue to invoke built-in redundancy, centre fallback, RC intervention and, where necessary, local redistribution. A post-T–12 local failure should remain local unless it develops into a genuinely systemic failure.

11.9 Local Failure Containment

A failed centre shall not by itself postpone a country-wide examination. RC shall first attempt restoration or complete centre reconstitution; if the centre remains RED, its candidates shall be redistributed to available certified capacity in the city/cluster and individually notified through authorised communication channels.

Before the final run-up, each RC should maintain an examination-specific contingency capacity map showing how candidates from every activated centre could be absorbed within certified spare capacity in the city/cluster if that centre becomes unusable. The map is a planning pathway rather than an automatic reassignment and must respect receiving-centre certified capacity and reasonable geographic constraints.

Where a major local force-majeure event makes timely local absorption impossible, national continuity should still be preserved. The disruption should be contained to the smallest practicable candidate population and handled through the prescribed exceptional contingency process rather than automatically postponing an otherwise secure country-wide examination.

CHAPTER 12

COST–BENEFIT CONSIDERATIONS

The economic case for TEST cannot be judged simply by comparing the cost of new technology with the cost of printing question papers. The present system carries substantial recurring costs for advance printing, packaging, transportation, secure storage, guarding, reconciliation, surplus material and controlled destruction, as well as the much larger financial and social consequences of a compromised examination or re-examination. TEST replaces much of this long physical custody chain with reusable digital, technical and professional infrastructure, but it also introduces genuine costs for Central and Regional systems, Secure Halls, printers, scanners, communications, cybersecurity, permanent TTPs, CTP deployment, training, audit, maintenance and redundancy. The proper comparison is therefore the full lifecycle cost and risk per candidate and per examination. TEST should ultimately be adopted not because it appears technologically attractive, but only if controlled pilots and detailed feasibility studies demonstrate that its gains in security, resilience, logistics and trust justify its incremental costs.

12.1 The Correct Question

The economic question is not:

"What will TEST cost?"

It is:

"What will TEST cost compared with the economic and social cost of examination failure?"

12.2 TEST Costs

Principal cost categories include:

In addition to TEST's own infrastructure and personnel costs, the comparison must account for the legacy system's recurring costs of advance printing, packaging, weeks of secure storage, national transportation, security during transportation, and security at multiple storage centres.

- TEST organisation;
- RCs;
- technology;
- cryptography;
- cybersecurity;
- centre infrastructure;
- TTP personnel;
- CTP remuneration;

- training;
- accreditation;
- audit;
- maintenance;
- technology refresh.

12.3 Savings and Legacy-System Costs Avoided

TEST can reduce:

- printing;
- transportation;
- storage;
- physical handling;
- unused paper;
- reconciliation;
- re-examination costs;
- administrative disruption.

TEST can also substantially reduce surplus examination material because printing is linked to the candidates actually allocated/appearing at the centre, subject to prescribed operational contingency. In the legacy model, material must generally be provided against the applicant population, with contingency, and unused papers and answer sheets then require reconciliation, secure storage and destruction.

The relevant economic comparison is therefore the full lifecycle cost of the legacy physical custody chain—printing, packaging, storage, transport and security—against TEST's reusable digital and physical security infrastructure. The cost of examination failure, including re-examination, candidate travel, administrative disruption and litigation, should also be included.

12.4 Cost of Failure

A compromised examination can cause:

- re-examination;
- candidate travel;
- administrative disruption;
- delayed recruitment/admission;
- litigation;
- loss of productivity;
- loss of institutional trust.

The social cost is substantially greater than the immediate financial cost.

12.5 Shared National Infrastructure

TEST can be shared across:

- recruitment examinations;
- entrance examinations;
- professional examinations;
- government examinations;
- certification examinations;
- university examinations.

This spreads fixed infrastructure cost across a large examination ecosystem.

12.6 Cost per Candidate

The appropriate long-term measure should be:

TEST cost per candidate/examination

rather than simply the capital cost of the national platform.

As utilisation increases, the fixed cost per candidate should decline.

12.7 Detailed Feasibility Study

Before implementation, Government should establish:

- capital cost;
- operating cost;
- centre upgrade cost;
- personnel cost;
- five- and ten-year TCO;
- cost per candidate;
- cost per examination;
- avoided failure costs;
- sensitivity analysis.

CONCLUSION

TOWARDS A TRUSTWORTHY EXAMINATION SYSTEM

The central proposition of TEST is that trustworthy examinations require neither blind faith in technology nor abandonment of human judgement, but a deliberate allocation of each to the

functions it performs best. Technology can authenticate, encrypt, transmit, enforce time, print, scan, record and audit with consistency; human experts remain essential for determining examination standards, approving papers, judging academic quality and evaluating responses where judgement is required. TEST combines these strengths while reducing the long physical custody of readable question papers and separating sensitive capabilities among independently accountable participants. It does not claim that leakage, equipment failure, human error or malicious conduct can be made impossible. It proposes instead that opportunities for compromise be radically reduced, failures detected early and contained locally, and critical actions made traceable. The ultimate case for TEST must therefore rest on evidence from rigorous pilots demonstrating that the architecture can deliver greater security, fairness, resilience, scalability and public trust than the system it seeks to improve.

India does not need to choose between technology and human judgement.

It needs to use each where it is strongest.

Technology can provide:

- encryption;
- authentication;
- secure transmission;
- controlled printing;
- machine-readable credentials;
- scanning;
- audit;
- redundancy.

Human professionals provide:

- judgement;
- verification;
- accountability;
- supervision;
- response to the unexpected.

Institutional separation provides:

- independence;
- checks and balances;
- accountability.

TEST brings these together into one architecture.

Its central proposition is simple:

Do not merely secure the existing examination process. Redesign the process so that the opportunities for compromise are fundamentally reduced.

The final paper should not travel through the country as a vulnerable physical object. It should remain encrypted until the last practical moment and be generated centrally by TEST rather than at an examination centre.

It should remain encrypted until the last practical moment.

It should be decrypted only in an authenticated, physically controlled environment.

One paper should be printed and independently verified before bulk printing.

Only the quantity actually required should subsequently be printed, subject to a small prescribed operational contingency.

Every critical movement should be reconciled.

Every answer sheet should be digitally captured on the day of examination, with CTPs performing the operational scanning under TTP technical supervision.

Every important action should leave an auditable record.

And no single person, organisation, technology or physical location should be capable of compromising the entire examination.

TEST is therefore not simply a proposal for a more secure examination.

It is a proposal to create **trust by design**.

Availability of the security system.

Ephemerality of the secret.
Independence of the people.
Accountability of every action.

That is the TEST proposition.

ANNEXURES — INDEX

The detailed operating framework supporting the main White Paper is contained in the following annexures:

Annexure I — Detailed Centre Infrastructure Requirements

Annexure II — Integrated Examination Timeline and Rehearsal

Annexure III — Centre Capacity, Room, Printer and Scanner Planning

Annexure IV — Examination Authority and Candidate Information Framework

Annexure V — Secure Hall Standard Operating Procedure

Annexure VI — Security Agency Accreditation and SOP

Annexure VII — Regional Centre Standard Operating Procedure

Annexure VIII — TEST Professional Eligibility, Training and Certification

Annexure IX — Communication, Data Exchange and Information Security

Annexure X — Business Continuity, Failure Management and Resilience

Annexure XI — Post-Examination Process, Scanning, Scoring and Evaluation

Annexure XII — Governance, Audit, Oversight and Accountability

Annexure XIII — Cost, Capacity and Resource Planning

Annexure XIV — Proposed Administrative Structure for CAFT and Regional Centres

ANNEXURE I

DETAILED CENTRE INFRASTRUCTURE REQUIREMENTS

Minimum physical, technical and operational requirements for a certified TEST examination centre.

I.1 Purpose

This annexure defines the infrastructure required for certification of an examination centre. Capacity shall be certified from actual physical configuration and not from nominal institutional capacity.

Governing principle: A centre is certified for the capacity it can safely, securely and operationally support—not merely the number of seats it claims.

I.2 Centre Capacity Modules

Module	Candidates	Indicative rooms*
Small	500	~13
Medium	750	~19
Large	1,000	25

*Planning assumption: approximately 40 candidates per qualifying room. Actual capacity depends on furniture, spacing, ventilation, accessibility and safety requirements.

I.3 Required Areas

Certified examination rooms.

Separate Secure Hall for decryption and printing.

Controlled scanning/processing area.

Secure storage for examination material.

Candidate entry and verification area.

Administrative/control point for the Centre In-charge.

I.4 Secure Hall

Controlled access with two-person opening principle.

Door controlled from inside and outside.

No personal digital devices.

TEST workstation and secure communications.

Intercom with the centre and authenticated operational messaging with RC.

Power backup and environmental protection.

Space for TTP, required CTPs, printers and controlled material.

I.5 Printing and Scanning

Printers shall support required throughput and preferably automatic collation.

For planning, a 100-question objective paper is 20 pages at five questions per page.

Scanner capacity shall support the prescribed post-examination window.

Redundancy shall prevent a single equipment failure from stopping the examination.

I.6 Power, Network and Security

Primary power plus UPS and appropriate backup generation.

Primary network plus alternate connectivity and emergency communication.

CCTV/access control for prescribed sensitive areas.

Security Agency controls access to the Secure Hall and sensitive areas.

I.7 Certification

Certification shall be capacity-specific and time-bound.

Certification follows inspection, technical testing, security assessment and rehearsal.

A historically used venue is not automatically a certified TEST centre.

ANNEXURE II

INTEGRATED EXAMINATION TIMELINE AND REHEARSAL

Indicative timing assumptions for paper generation, answer-key preparation, rehearsal, printing and post-examination processing.

II.1 Timing Philosophy

T–45 is indicative only. It is not an architectural deadline. Earlier delivery of candidate information is permitted where the EA can reliably provide it.

II.2 Objective Examination

Time	Activity	Responsibility
T–3:00	CAFT secure environments activated; primary and fallback checked	CAFT
T–2:30	Final paper generated and human-approved	CAFT
T–2:30 to T–1:30	Answer key prepared; minimum one hour	CAFT
T–1:30 to T–0:30	Independent key checking and finalisation	CAFT
After paper approval	Encrypted paper transmitted to RCs/centres	CAFT / RC
Authorised time	TTP + CTP jointly decrypt paper	Centre
Immediately after	One paper printed and scrutinised	TTP / CTP
T–0	Examination begins	All centres
T+0 onward	Objective key released and securely transmitted	CAFT / RC
During examination	Key loaded and verified in scoring environment	TTP + CTP
T+End	Answer sheets collected/reconciled	Centre / CTPs
T+End onward	Scanning and scoring	CTPs under TTP oversight
T+3 indicative	Centre-level scoring/transmission substantially complete	Centre / RC

T+3 is a planning assumption, not a universal deadline; it must be validated against examination duration, scanner throughput and candidate volume.

II.3 Descriptive Examination

Stage	Activity
T–2:30	Final question paper generated and approved at CAFT
T–0	Examination begins
T+End	Answer booklets collected and reconciled

Stage	Activity
Post-examination	Scanning/digitisation begins
After examination	Evaluation Key prepared by subject experts
Before evaluation	Independent checking; Evaluation Key frozen
Shortly before evaluation	Evaluation Key released only to authorised evaluation environment
Evaluation	Digital answer books evaluated under prescribed controls

II.4 T–24 Full-System Rehearsal

CAFT exercises the secure paper-generation and encryption environments, including both primary/fallback capability, while the prescribed human-approval process is conducted by the authorised academic/OE participants within the controlled workflow.

RCs receive and forward the encrypted rehearsal package to every participating centre.

Centres decrypt in a time-controlled manner, print one paper, obtain acceptance and print the prescribed quantity.

For objective papers, a dummy answer key is prepared, checked, released only after the rehearsal examination-start point, distributed and loaded into scoring systems.

CTPs scan dummy answer material under TTP technical supervision and transmit records.

Rehearsal shall use dummy examination content only. No live examination content, live cryptographic secret or unreleased answer key shall be used during rehearsal; the process is rehearsed, not the secret.

Failures are diagnosed and rehearsal repeated at the earliest practicable time.

II.5 T–12 Final Gate

T–12 is the final readiness gate for the national trust architecture and for establishing a viable examination pathway for every candidate. Local RED centres may be contained through restoration, reconstitution or authorised redistribution. Postponement/cancellation of the country-wide examination should arise only from a genuinely SYSTEMIC RED condition that cannot be restored by T–12.

ANNEXURE III

CENTRE CAPACITY, ROOM, PRINTER AND SCANNER PLANNING

Engineering assumptions for 500-, 750- and 1,000-candidate centre modules.

III.1 National Planning Assumption

Approximately 5,000 centres is the current working national planning assumption. It is not a fixed requirement.

Module	Candidates	Indicative rooms
Small	500	~13
Medium	750	~19
Large	1,000	25

Room capacity is based on a planning assumption of approximately 40 candidates per compliant room. Primary-class furniture is not assumed suitable merely because floor area exists.

III.2 Printer Planning

A 100-question objective paper is assumed to occupy 20 pages. A 500-candidate centre therefore requires about 10,000 examination pages before prescribed operational contingency.

Printer selection shall be based on reliable throughput, recovery time, paper capacity and automatic collation.

After approval of the first complete paper, approximately 50% of allotted centre capacity is a reference design assumption for the initial print tranche, not a fixed rule. The operational percentage shall be established through pilot load testing and examination-specific throughput, attendance and contingency analysis. Candidate attendance then determines the balance print requirement, subject to prescribed operational contingency.

Manual collation shall not be normal practice.

Printer redundancy shall permit continuity after an individual printer failure.

Final printer counts shall be established through engineering tests.

III.3 Scanning

Scanning is an operational function performed by CTPs under TTP technical supervision. The TTP configures and verifies the scanner/scoring environment, handles technical failures and monitors integrity; CTPs perform the physical scanning in parallel.

III.4 CTP Planning

One CTP shall be provided for every 100 candidates or three rooms, whichever imposes the stricter requirement, with reserve capacity.

III.5 Reserve Capacity

Reserve capacity should be planned at city/cluster and RC level so a failed centre can be absorbed without national postponement.

ANNEXURE IV

EXAMINATION AUTHORITY AND CANDIDATE INFORMATION FRAMEWORK

Administrative boundary between OE/EA and TEST, including the candidate information required for contingency operations.

IV.1 Boundary

The OE decides the requirement and broad examination parameters and appoints the EA. The EA manages applications, acceptance, candidate communication and hall tickets. TEST security and administration begin after candidate allocation and hall-ticket delivery.

IV.2 EA Responsibilities

Publish advertisement and publicity.

Receive applications through approved online and physical channels.

Conduct eligibility/acceptance functions assigned under the agreement.

Maintain the authoritative candidate administrative record.

Issue hall tickets with colour photograph and machine-readable QR credential.

Transmit prescribed candidate allocation/contact data securely to TEST/RC systems.

IV.3 Candidate Contact Information

Registered mobile number.

Email address.

Other prescribed contact information.

Information needed for emergency individual communication where prescribed.

IV.4 QR and Room Allocation

The QR credential should authenticate the candidate. The room number need not be embedded in the QR. A secure local database may return the room at entry or through an approved application before the examination.

IV.5 Contingency Communication

Candidates shall be advised in advance that exceptional centre redistribution may occur and should check registered email and mobile messages at approximately T–10 and thereafter until departure.

IV.6 Redistributed Candidate Data

Receiving-centre databases shall support controlled incremental updates from RC so that redistributed candidates can enter through the normal authentication and room-allocation process.

ANNEXURE V

SECURE HALL STANDARD OPERATING PROCEDURE

Detailed procedure for the most sensitive physical environment in TEST.

V.1 Purpose

The Secure Hall is the controlled environment in which the encrypted examination package is decrypted and the first physical paper is produced.

Governing principle: The paper remains unreadable until the last practical moment and can never be freshly generated at a centre.

V.2 Access

Access limited to authorised TEST personnel and prescribed CTP participation.

Door controlled from inside and outside.

Two-person control required to defeat the locking arrangement.

Security Agency controls access from outside and does not routinely enter.

Exceptional Security Agency entry requires prescribed high-level authorisation.

V.3 Devices and Communications

No personal digital device.

Fixed intercom/equivalent with centre.

Authenticated TEST operational messaging with centre and RC.

Consumer messaging platforms are prohibited for examination-sensitive operations.

V.4 Receipt and Decryption

Encrypted package becomes available around T–2.5, subject to the examination schedule.

Decryption is time-controlled.

TTP + one CTP jointly authorise and perform decryption.

All decryption actions are separately attributable and audited.

V.5 First Print

TTP initiates printing after successful decryption.

Exactly one examination paper is printed initially.

Designated CTP checks identity, set/version, page count, sequence, language, format, identifiers and print quality.

Bulk printing is authorised only after successful verification.

V.6 Objective Answer Key

The objective key is separate from the paper. After final paper approval, key setters shall have at least one hour for preparation, followed by sufficient independent checking and finalisation.

The key is not transmitted with the paper and is not released to centres before T+0. After commencement it is securely transmitted, authenticated and loaded into the scoring environment by TTP + CTP jointly.

V.7 Centre Prohibition

No fresh examination paper may be generated at a centre. Replacement papers are generated only at CAFT through the controlled paper-generation process.

ANNEXURE VI

SECURITY AGENCY ACCREDITATION AND SOP

Physical security responsibilities before, during and after examination.

VI.1 Role

The Security Agency protects people, premises, access points and physical examination material. It does not control examination content or technical operations.

VI.2 Responsibilities

Control access to Secure Hall and prescribed sensitive areas.

Maintain perimeter and entry security.

Prevent unauthorised persons/devices entering controlled areas.

Protect physical movement of examination material.

Support emergencies without entering examination operations unless authorised.

VI.3 Accreditation

Personnel shall be identifiable and appropriately vetted.

Staffing shall match centre risk profile.

Personnel shall be trained in the boundary between physical security and examination operations.

Agency shall participate in rehearsal and incident drills.

VI.4 Incident Response

Security incidents shall be reported through the prescribed chain. Security personnel preserve the scene and evidence and do not independently open, inspect or manipulate examination material.

ANNEXURE VII

REGIONAL CENTRE STANDARD OPERATING PROCEDURE

Command, monitoring, reserve capacity, centre recovery and candidate redistribution.

VII.1 Role

The RC is the operational layer between CAFT and centres. It does not generate or decrypt examination papers.

VII.2 Responsibilities

Provide one permanent CAFT TTP to each centre and maintain reserve capacity.

Monitor centre readiness and rehearsal status.

Receive encrypted packages and forward them securely.

Provide technical and operational support.

Maintain capability to completely reconstitute at least one failed centre.

Maintain candidate contact information needed for contingency communication.

Redistribute candidates when a centre remains RED at the final gate.

VII.3 Failed Centre

A centre failure shall not by itself postpone a national examination. RC uses reserve capacity and redistributes candidates to other certified centres where feasible.

VII.4 Candidate Notification

Use email, SMS and an approved messaging channel as appropriate.

State revised centre, address, reporting instructions and help contact.

Candidates are warned in advance that this contingency is possible.

VII.5 Receiving Centre Update

RC sends an authorised incremental update to the receiving centre database. The centre verifies the update before admitting redistributed candidates.

VII.6 Regional Resources

RC resources are based on maximum simultaneous operational load and must cover TTP reserves, centre reconstruction, alternate communications and candidate redistribution.

ANNEXURE VIII

TEST PROFESSIONAL ELIGIBILITY, TRAINING AND CERTIFICATION

Personnel architecture for permanent TEST Professionals and the certified CTP pool.

VIII.1 Personnel Principle

Personnel above the centre operational layer shall be permanent CAFT employees serving as TEST Professionals appropriate to role. Government employees, teachers and PSU officers shall not form the routine permanent CAFT technical cadre.

VIII.2 Certification

Basic certification may use approximately one week of intensive training followed by certification.

Specialised functions require additional training.

Certification is personal, renewable, suspendable and revocable.

Continuing training and refresher training are mandatory.

VIII.3 TTP

Permanent CAFT technical employee; one per centre plus RC reserve.

Technical ownership of decryption, printing, scanner configuration and scoring-environment integrity.

Receipt/authentication/controlled loading of objective answer key after T+0.

Technical supervision of CTP scanning.

Troubleshooting, incident response and technical transmission verification.

VIII.4 CTP

One per 100 candidates or three rooms, whichever is stricter.

Room/process oversight, distribution and collection supervision.

First-paper scrutiny.

Room-wise reconciliation and sorting.

Physical scanning under TTP technical oversight.

Exception handling and scanning reconciliation.

VIII.5 Territorial Army

Territorial Army personnel may, subject to permissions and specialised training, supplement the regional oversight pool. This is optional and not a dependency.

VIII.6 Centre In-charge

Preferably the Principal of the host institution or a senior colleague able to secure cooperation of junior staff. The role is institutional command, not TEST technical command.

ANNEXURE IX

COMMUNICATION, DATA EXCHANGE AND INFORMATION SECURITY

Secure movement of examination, operational and candidate information.

IX.1 Information Domains

Domain	Examples	Control
Examination-sensitive	Paper, cryptographic material, objective key	Highest security
Operational/candidate	Identity, contact, allocation, attendance	Role-based access/encryption
Public	Dates, instructions, advisories	Approved public channels

IX.2 Two Logical Networks

The Examination Security Network (CAFT → RC → Centre) and Operational/Candidate Network (EA → CAFT/RC → Centre/Candidate) shall interoperate where required but remain logically separated.

IX.3 Operational Messaging

Use an authenticated TEST operational messaging platform with identity, encryption, audit trail and controlled file transfer.

No WhatsApp or similar consumer platform for examination-sensitive operations.

WhatsApp may be used, where appropriate, as one candidate-notification channel.

IX.4 Candidate Data

Candidate information is distributed on a need-to-know basis. Centre databases contain candidates allocated to the centre plus controlled contingency updates.

IX.5 Examination Package

The paper remains encrypted through CAFT → RC → Centre and is decrypted only at the authorised centre stage. RC never decrypts.

IX.6 Objective Key

The key is released only after T+0, transmitted securely and loaded only into the authorised scoring environment.

IX.7 Trusted Time

Critical systems use multiple authoritative time references with cross-verification. Time is a security parameter.

IX.8 Access and Audit

Critical transactions create protected audit records.

Access is least-privilege, need-to-know and time-bound.

Privileged accounts are individually attributable and monitored.

Access is revoked when authorisation ends.

ANNEXURE X

BUSINESS CONTINUITY, FAILURE MANAGEMENT AND RESILIENCE

Failure containment, redundancy, recovery and the T–12 final readiness gate.

Governing principle: The aim is not to claim that failure is impossible; it is to absorb predictable failures, recover quickly and contain failure at the lowest possible level.

X.1 Failure Levels

Level	Examples	Primary response
0 — Built-in redundancy	Single printer/scanner/power/network component	Local
1 — Local fallback	Secure Hall/equipment issue	Centre / SEM
2 — Regional	Centre failure/multiple equipment failures	RC
3 — Security incident	Physical/cyber compromise	CAFT / Security
4 — Systemic	TEST trust architecture failure	National continuity

X.2 Central Redundancy

CAFT shall have two geographically separated environments with the same approved data/configuration, independently provisioned hardware, independently engineered software, separate power/connectivity and the ability of the fallback to perform the critical function.

X.3 Answer-Key Failure

Preparation delay: use the controlled preparation/checking window; never release an unverified key.

Transmission failure: use alternate secure path.

Authentication failure: do not load; escalate and obtain verified package.

Loading failure: use authorised technical recovery/standby scoring environment.

Scanner failure after loading: transfer scoring without regenerating the key.

Suspected compromise: CAFT incident; revoke/replace as prescribed and preserve audit evidence.

X.4 Centre Failure

RC attempts recovery during the rehearsal window. If a centre remains RED at the final gate, candidates are redistributed to certified centres with available capacity.

X.5 T–24 to T–12

T–24 failure triggers diagnosis, correction and repeat rehearsal at the earliest practicable time. By T–12, the national trust architecture must be demonstrated ready and every candidate must have a viable examination pathway. A local RED centre is handled through recovery or

redistribution; only an unresolved SYSTEMIC RED condition should threaten the country-wide examination. Failure management continues after T–12 for newly arising local events.

X.6 No Cascade Principle

A printer failure should remain a printer failure; a centre failure a centre failure; an RC failure a regional failure. Only a genuinely systemic failure should threaten the national examination.

ANNEXURE XI

POST-EXAMINATION PROCESS, SCANNING, SCORING AND EVALUATION

Secure chain of custody for objective and descriptive examinations.

XI.1 Collection

Invigilators collect answer material room-wise.

CTPs supervise counting and reconciliation.

Unused material is separately accounted for.

Physical count is reconciled with attendance and issue records.

XI.2 Objective Papers

CTPs perform physical scanning in parallel under TTP technical supervision. The TTP configures/verifies the scanner and scoring environment and handles technical exceptions.

XI.3 Objective Scoring

The authorised key is applied by the scoring environment. CAFT receives the answer-sheet image, candidate identifier, machine-read responses, score and relevant audit information.

XI.4 Objective Audit Chain

Candidate → Answer image → Recognised responses → Answer-key version → Scoring rules → Score.

XI.5 Descriptive Papers

Descriptive answer booklets are scanned into secure digital booklets. Human evaluators retain academic judgement.

XI.6 Descriptive Evaluation Key

Prepared only after the examination and shortly before evaluation. It identifies substantive points, acceptable alternatives, mark allocation and partial-credit conditions. It is not a word-for-word model answer.

XI.7 Weighting Principle

Governing principle: Substantive knowledge and desirable points should normally carry the dominant weight. Reasoning, organisation, expression and presentation receive appropriate credit but should not normally overwhelm demonstrated knowledge unless the question specifically assesses them.

XI.8 Evaluation Consistency

TEST seeks consistency, not artificial uniformity. Competent evaluators using the same question-specific Evaluation Key should reach broadly comparable scores for substantially similar answers.

XI.9 Double Evaluation and Moderation

Where prescribed, double evaluation, statistical moderation and reconciliation shall be supported.

XI.10 Physical Chain of Custody

After scanning, answer sheets/booklets and relevant question-paper material are associated room-wise, securely sealed and stored. Routine revaluation should use the digital record; exceptional opening of originals requires authority and recorded reasons.

XI.11 Result Integrity

No result shall be altered without authenticated authority, reason, before/after values, time stamp and audit record.

ANNEXURE XII

GOVERNANCE, AUDIT, OVERSIGHT AND ACCOUNTABILITY

Oversight architecture ensuring that TEST remains independently auditable and accountable.

XII.1 TEST Council

The TEST Council is the apex authority for standards, accreditation, certification, security policy, technology standards, audit, professional certification and emergency governance.

XII.2 CAFT Executive Responsibility

CAFT is accountable for national execution of the TEST architecture and supervision of RCs, but remains subject to TEST Council standards, independent audit and the separation-of-capability controls prescribed in the White Paper. Day-to-day execution shall not be concentrated in the TEST Council itself.

XII.3 Separation of Powers

Paper generation ≠ paper approval.

Key preparation ≠ key verification.

Decryption ≠ unilateral approval.

Technical operation ≠ security approval.

Evaluation ≠ result certification.

XII.4 Independent Audit

Cybersecurity assessment.

Technology/performance assessment.

Centre and RC audit.

Operational review.

Red-team testing.

Financial/procurement audit.

XII.5 Rehearsal Audit

T–24 rehearsal records shall capture participation, timing, failures, corrective action, repeat rehearsal and final status.

XII.6 Accountability

Every critical function shall have a primary owner, backup owner, escalation authority and audit authority. Shared credentials are prohibited.

XII.7 Software and Version Control

Security/scoring software changes require testing, approval, version control and rollback capability.

Emergency changes require separate authorisation and post-event review.

Paper, answer-key, Evaluation-Key, software and configuration versions must be identifiable and auditable.

XII.8 Incident Investigation

Serious incidents shall be independently investigated to establish immediate, underlying and systemic causes. Corrective action should address the systemic cause.

XII.9 Transparency

TEST should publish architecture principles, standards, audit methodology and aggregate performance to the extent consistent with security and privacy.

ANNEXURE XIII

COST, CAPACITY AND RESOURCE PLANNING

Illustrative bottom-up planning model for national-scale TEST infrastructure and examination-specific operating cost. The figures below are engineering estimates intended to establish order of magnitude; they are not procurement quotations and must be validated through pilots, competitive procurement and utilisation studies.

XIII.1 Scope and Costing Principle

The relevant economic measure is full lifecycle cost per candidate and per examination. TEST replaces much of the long physical custody chain with reusable secure infrastructure and trained personnel. The model therefore separates reusable capital infrastructure from examination-specific recurring operating cost. Permanent CAFT/RC/TTP establishment costs, EA administrative costs and academic/evaluation costs are excluded from the recurring operating estimate below and should be assessed separately in a full feasibility study.

XIII.2 National Planning Assumptions

Reference examination: approximately 20 lakh candidates.

Activated network: approximately 5,000 certified centres using 500-, 750- and 1,000-candidate modules; 5,000 is a planning assumption, not a fixed procurement number.

Reference centre for costing: 500-candidate module, approximately 13 qualifying rooms at about 40 candidates per room.

Invigilation planning assumption: two invigilators per room for the prudent national-cost case.

CTP planning: five CTPs for the 500-candidate reference centre under the one-per-100-candidates or three-rooms rule, whichever is stricter.

Centre usage charge is assumed to include the access required for T–24 rehearsal and examination-day operations.

XIII.3 Illustrative Examination-Day Remuneration and Centre Cost

Item	Quantity	Planning rate	Reference-centre cost
Centre usage (includes T–24 access)	1	₹50,000	₹50,000
Centre In-charge	1	₹10,000	₹10,000
Lead CTP — T–24 + examination day	1	₹8,000	₹8,000
Other CTPs	4	₹6,000	₹24,000
Invigilators	26	₹3,000	₹78,000
Total before Security Agency			**₹1,70,000**

The lead CTP is costed at ₹8,000 because at least one CTP must participate both in the T–24 rehearsal and on examination day. Other deployed CTPs are costed at ₹6,000 each. These are planning honoraria, not prescribed national rates.

At 5,000 reference centres, the above centre/personnel model gives an indicative national cost of approximately ₹85 crore before specialised security, printing consumables and local contingency costs.

XIII.4 Security, Consumables and Examination-Specific Operating Cost

Recurring examination-specific head	Illustrative national estimate
Centre usage, Centre In-charge, CTPs and invigilators	~₹85 crore
Accredited Security Agency deployment, reserves and rehearsal support	₹8–10 crore
Paper, toner and controlled printing/processing consumables	₹3–5 crore
Secure communications, seals, local logistics and operating contingencies	₹3–6 crore
Indicative examination-specific recurring total	**~₹99–106 crore; prudent planning envelope ₹100–110 crore**

For an examination of 20 lakh candidates, the prudent ₹100–110 crore envelope corresponds to approximately ₹500–550 per candidate. This is a marginal examination-operating estimate and excludes permanent institutional establishment, capital amortisation, EA administration and academic/evaluation expenditure.

XIII.5 Illustrative Certified-Centre Technology Package

Centre technology component	Reference quantity	Illustrative provision
Secure TEST/CAFT workstations	2	₹1.20–1.40 lakh
High-speed duplex/collating printers	4	₹1.80–2.20 lakh
High-speed duplex scanners	3	₹1.20–1.50 lakh
Online UPS with adequate batteries	1	₹1.50–1.80 lakh
Dual-network/router/firewall equipment	As designed	₹0.40–0.60 lakh
QR/entry authentication devices	As designed	₹0.40–0.60 lakh
Secure Hall access control/CCTV/intercom	As designed	₹0.50–0.75 lakh
Secure cabinets, cabling, installation and local integration	As designed	₹0.50–0.75 lakh

The resulting reference-centre technology package is of the order of ₹7.5–9.5 lakh. Across 5,000 centres this gives an indicative gross centre-technology envelope of approximately ₹375–475 crore. Actual incremental cost may be materially lower where certified host institutions already possess compliant power backup, CCTV, networking, rooms or other reusable infrastructure.

XIII.6 CAFT, RC and National Resilience Infrastructure

The centre layer must be supplemented by CAFT primary and geographically separated fallback environments, secure question-bank and paper-generation systems, HSM/PKI and trusted-release infrastructure, national monitoring/SOC capability, secure data and audit repositories, RC infrastructure, alternate communications, regional reserve equipment and centre-reconstruction capability. Until the number and engineering configuration of RCs are fixed, an illustrative planning allowance of ₹100–150 crore is reasonable for this national/RC technology and resilience layer.

On that basis, the first-order reusable technology envelope for the national TEST ecosystem is approximately ₹500–650 crore. This is deliberately an order-of-magnitude estimate and should not be converted into procurement sanctions without pilot engineering and market testing.

XIII.7 Illustrative Capital Allocation

As a simple utilisation illustration—not an accounting depreciation rule—if reusable infrastructure of about ₹600 crore supports twenty major examination events over its initial useful/refresh cycle, the capital allocation is about ₹30 crore per event, or about ₹150 per candidate for a 20-lakh-candidate examination. Actual economics will depend heavily on utilisation, maintenance, technology refresh, shared infrastructure and the mix of examination sizes.

XIII.8 Legacy Lifecycle Cost Comparison

Legacy cost heads include advance confidential printing and packaging, secure storage for days or weeks, nationwide transportation, transport security, guarding at multiple custody points, inventory/reconciliation, surplus material and controlled destruction, and the financial and social cost of re-examination after compromise.

TEST incurs higher reusable technology, redundancy, specialist manpower, training, rehearsal and audit costs, but materially reduces the duration and extent of physical question-paper custody.

No claim is made at this stage that TEST is cheaper in every examination. The correct comparison is the full lifecycle cost and risk of the legacy model against the reusable TEST architecture, including avoided failure and re-examination costs.

XIII.9 Feasibility and Pilot Validation

Pilot procurement should validate centre hardware quantities, throughput and redundancy.

Pilot operations should record actual centre, CTP, invigilator, security, consumable and communication expenditure.

Government should separately determine permanent CAFT/RC/TTP establishment cost, centre-upgrade cost, five- and ten-year total cost of ownership, maintenance/refresh, cost per candidate/examination, avoided failure costs and sensitivity to utilisation.

The financial case should be accepted only after like-for-like comparison with the full current physical-custody lifecycle.

Governing principle: the figures in this annexure are intended to show that TEST is capable of being costed from its detailed architecture and that its apparent order of magnitude is

compatible with national-scale examination economics. Pilot evidence, not advocacy, must determine the final financial case.

ANNEXURE XIV

PROPOSED ADMINISTRATIVE STRUCTURE FOR CAFT AND REGIONAL CENTRES

Illustrative administrative and command structure for operating TEST while preserving separation of powers, professional accountability and regional resilience. Titles and sanctioned strength are indicative and should be fixed only after workload and pilot studies.

XIV.1 Institutional Relationship

Entity	Primary role
TEST Council	Apex policy, standards, accreditation, certification, oversight, emergency governance and independent assurance.
CAFT	Permanent national executive/operational agency implementing and operating the TEST architecture.
Regional Centres (RCs)	Regional command, centre readiness, TTP deployment, recovery, contingency capacity and candidate redistribution.
Examination Centres	Certified local execution under prescribed TTP/CTP, Centre In-charge and Security Agency controls.

The TEST Council should not become the day-to-day examination operator. CAFT should not become the academic owner or routine examination administrator. The OE and EA retain those functions as defined in the White Paper.

XIV.2 Proposed CAFT Command Structure

CAFT may be headed by a Director General/Chief Executive accountable to the TEST Council for implementation, operational readiness, security and performance. The precise service designations are secondary; functional separation is essential.

CAFT function/directorate	Indicative responsibility
National Examination Operations	National scheduling interface, examination activation, command centre, RC coordination and operational status.
Secure Paper Generation & Assessment Systems	Secure question-bank/process environment, paper-generation systems and assessment technology. Academic ownership remains with OE/EA experts.
Cryptography & Trusted Release	HSM/PKI, key management, time-bound release and cryptographic control, functionally separated from paper generation.
Technology, Cybersecurity & Infrastructure	Platforms, networks, IAM, SOC/SIEM, secure communications, repositories, resilience engineering and technology standards implementation.

CAFT function/directorate	Indicative responsibility
Regional Operations & Resilience	RC supervision, reserve-capacity policy, centre-reconstruction standards, contingency planning and national failover coordination.
Professional Standards, Training & Certification	Permanent technical cadre standards, TTP training, CTP certification framework, refresher training and professional discipline.
Risk, Compliance & Internal Assurance	Operational risk, control testing, incident review and compliance. Independent external audit remains answerable to the TEST Council.
Administration, Finance & Procurement	Personnel administration, finance, contracting and procurement under security-aware controls and conflict-of-interest safeguards.

XIV.3 Separation Within CAFT

Paper generation shall not carry cryptographic release authority.

Human paper approval shall remain attributable to authorised academic/OE participants and shall not be subsumed into technology operations.

Cryptographic control and trusted release shall be functionally separated from paper-generation operations.

Internal assurance may test compliance, but independent external cybersecurity, operational and financial audit shall report through the oversight arrangements of the TEST Council.

No individual or pair shall acquire the complete capability to generate, approve, release and conceal a protected examination asset.

XIV.4 Proposed Regional Centre Structure

Each RC may be headed by a Regional Director/Regional TEST Head, a permanent CAFT professional responsible for maximum simultaneous examination load in the assigned region. RC staffing should be driven by workload and recovery obligations rather than a uniform establishment formula.

RC function/cell	Indicative responsibility
Operations & Centre Readiness	Centre activation, rehearsal status, dashboards, escalation and examination-day coordination.
Technical Operations & TTP Deployment	Permanent TTP cadre deployment, technical reserves, equipment support and secure package forwarding.
Secure Communications & Systems Support	Regional secure connectivity, alternate paths, local systems support and communications resilience.
Resilience, Logistics & Contingency	Reserve equipment, SEM/reconstruction capability, city/cluster capacity map and candidate redistribution.
Professional Deployment & Training	CTP availability, reserve deployment, refresher readiness and regional training coordination.
Security/Certification Liaison & Administration	Interface with independent Security Agencies and Centre Certification Agencies, plus regional logistics and administration.

XIV.5 Personnel Categories

Category	Status
Permanent CAFT/RC cadre	National specialists, regional core staff and TTPs.
Certified deployable pool	CTPs; remunerated/deployed for examinations, with pool size materially above peak demand.
Host-institution personnel	Centre In-charge and invigilators under institutional command and TEST procedures.
Independent accredited providers	Security Agencies and Centre Certification Agencies; organisationally separate from CAFT/EA.

XIV.6 Examination-Day Command and Boundaries

National operational command flows from CAFT to RCs for TEST functions. RCs coordinate and support TTPs and TEST operational personnel at centres. The Centre In-charge commands host-institution staff; CTPs perform prescribed certified operational functions; the Security Agency commands its own physical-security personnel within the accredited scope. These lines must cooperate operationally without merging authorities that TEST deliberately keeps separate.

An RC does not generate, approve or decrypt examination papers. It receives and forwards encrypted packages, maintains readiness and recovery capability, and contains regional failures. National paper-generation and trusted-release functions remain at CAFT.

XIV.7 Incident Command

LOCAL RED events should be owned at the lowest capable level and escalated to the RC where centre recovery, reconstruction or redistribution is required. SYSTEMIC RED conditions affecting national trust architecture are escalated immediately to CAFT and the prescribed TEST Council emergency-governance authority. Incident command shall not override the separation-of-capability controls for examination secrets.

XIV.8 Staffing and Sanctioning Principle

This annexure intentionally does not prescribe sanctioned posts or government-equivalent grades. CAFT and RC staffing should be derived from maximum simultaneous examination load, number and geography of centres, required TTP reserve, cyber/operations coverage, resilience obligations and service-level targets. Pilot data should determine the final establishment, with administrative staffing kept lean relative to the permanent technical and operational capability required by TEST.

END OF ANNEXURES

To be read with the TEST White Paper. Detailed technical specifications, procurement quantities and statutory provisions remain subject to implementation studies and applicable law.