From Examination Crisis to Institutional Resilience: Digital Transformation, Stakeholder Management, And Strategic Decision-Making in the NEET-UG 2026 Crisis

Sanjay Vishwanath Khande[1], Dr. Avinash Kakade[2], Dr. Kirankumar P. Johare[3]
[1]*PhD Scholar, Symbiosis International (Deemed University), Pune – 412115, Maharashtra, India*
[2,3]*Symbiosis International (Deemed University), Pune – 412115, Maharashtra, India*
[3]*Maratha Vidya Prasarak Samaj, Nashik – 422002, Maharashtra, India*
doi.org/10.64643/ijirt.208377-459

***Abstract*—India's NEET-UG 2026 examination crisis exposed critical vulnerabilities in public-sector crisis management. Operational disruptions and localized paper leaks on May 3, 2026, overwhelmed traditional bureaucratic response mechanisms as decentralized digital communication outpaced official information flows, culminating in the cancellation of the examination, a federal criminal investigation, sustained student mobilizations at New Delhi's Jantar Mantar, and a full national re-examination. This study examines how public testing agencies manage high-stakes operational crises under conditions of rapid digital information escalation. Adopting an abductive, qualitative single-case design, we analyze the National Testing Agency's handling of the crisis through three triangulated documentary streams: official administrative records, statutory investigative statements, and public digital archives. Thematic analysis identifies four interlocking vulnerabilities (delayed anomaly recognition, a verification vacuum, engagement asymmetry, and an absent learning loop) that converge on a single master vulnerability: chronological lag, the interval between internal detection and transparent public disclosure.**

From these empirically derived vulnerabilities we develop the CRISP framework (Crisis Recognition, Risk Intelligence, Stakeholder Engagement, and Preparedness), a continuous capability loop in which digital governance capability functions as the connective mechanism rather than a back-office support function. The study makes three contributions: it extends the fusion view of digital strategy from the firm to crisis-governed public institutions; it specifies a digitally enabled micro-foundation for capability-based conceptualizations of organizational resilience; and it translates dynamic-capabilities theory into an operational blueprint for examination governance, specifying the organizational loci, decision rights, activation triggers, and performance indicators through which each capability can be institutionalized. Rival explanations for disclosure delay, including legal constraints arising from the concurrent criminal investigation, are explicitly examined.

***Index Terms*—Organizational Resilience; Crisis Management; Digital Transformation; Strategic Decision-Making; Dynamic Capabilities; Stakeholder Management; Public Administration.**

I. INTRODUCTION

High-stakes examinations in India are critical public institutions that hold societal trust and shape the academic futures of millions of students. The National Eligibility-cum-Entrance Test (NEET-UG) is the single gateway to undergraduate medical education, and when a security breach impacts a framework of this scale, the consequence is not merely logistical: institutional credibility itself is placed at risk. Operational failures in such settings escalate into systemic crises that minor administrative adjustments cannot resolve [9], [10].

The breakdown of the NEET-UG 2026 examination cycle offers a revelatory real-world case of this dynamic. Following the initial test administration on May 3, 2026, documented paper leaks and logistics failures triggered public concern, the cancellation of the examination and a formal criminal investigation registered by the Central Bureau of Investigation (CBI), both on May 12, 2026 [2], and a full re-examination conducted for all registered candidates on June 21, 2026 [1]. As institutional trust declined, decentralized student networks, including groups organizing under student-led banners such as the

Cockroach Janta Party (CJP), used digital platforms to coordinate public demonstrations at New Delhi's Jantar Mantar, as documented in contemporaneous public reporting. The episode demonstrates how operational errors within state agencies are rapidly amplified and reframed through horizontal communication networks that move faster than hierarchical reporting structures.

This study analyzes the NEET-UG 2026 crisis through an integrated theoretical lens combining crisis management, dynamic capabilities, and digital governance. Rather than treating the incident strictly as an examination security breach, we evaluate administrative action by mapping the intersection of organizational resilience [4], stakeholder dynamics [16], [17], and digitally enabled risk intelligence [3]. Our purpose is to build a proactive managerial framework for examination bodies forced to navigate multi-stakeholder disruptions in hyperconnected information environments.

Specifically, this paper addresses two research questions:

RQ1. How can digital governance capabilities be repurposed as a core, strategic governance mechanism, rather than a back-office tool, during high-stakes institutional crises?

RQ2. What specific administrative and logistical capabilities, including their organizational placement, decision rights, and activation triggers, are required to transition a state testing body from reactive crisis control to permanent, proactive organizational resilience?

1.1 Objectives of the Study

Consistent with these research questions, the study pursues four objectives: (1) to reconstruct the escalation dynamics of the NEET-UG 2026 examination crisis from triangulated documentary evidence (Section 4.1); (2) to identify the structural vulnerabilities in the administrative response through reflexive thematic analysis (Section 4.3); (3) to derive from those vulnerabilities a capability framework, CRISP, that repositions digital governance capability as a strategic mechanism rather than a back-office function (Sections 5.1–5.2, addressing RQ1); and (4) to operationalize that framework by specifying the organizational loci, decision rights, activation triggers, and performance indicators through which each capability can be institutionalized (Sections 5.3–5.4, addressing RQ2).

The paper proceeds as follows. Section 2 positions the study within crisis management, dynamic-capabilities, digital governance, and stakeholder scholarship, and specifies the gap at their intersection. Section 3 details the abductive single-case methodology and its validity strategy, including the treatment of rival explanations. Section 4 presents the case analysis: the escalation chronology, a stakeholder mapping, and four empirically derived vulnerability themes. Section 5 develops the CRISP framework from those themes, positions it against prior models, and operationalizes it. Section 6 discusses contributions, limitations, and future research. Section 7 concludes.

II. LITERATURE REVIEW AND THEORETICAL FRAMING

2.1 Crisis Management in Public Organizations

Organizational crises are rare but severe disruptions whose causes, consequences, and remedies are initially ambiguous, and which place the organization's viability and legitimacy at stake [10]. Public-sector crisis scholarship decomposes crisis leadership into strategic tasks of sense-making, decision-making, meaning-making, terminating, and learning [9], and emphasizes cognition, communication, coordination, and control as the operative variables of response [8].

Crisis communication research, most prominently the lifecycle tradition, structures managerial attention across pre-crisis preparation, acute response, and post-crisis learning [11], while public administration scholarship stresses that effective crisis governance requires both governance capacity and legitimacy: the ability to act and the public standing to be believed [12]. A recurring finding is the tension between agility and discipline: rigid command structures provide procedural control yet struggle in fast-moving, information-rich environments [20].

Empirically, insular hierarchical communication loops falter in hyperconnected ecosystems where public skepticism and real-time reporting can outpace official updates [8], [9].

2.2 Dynamic Capabilities and Organizational Resilience

The dynamic-capabilities perspective explains how organizations renew and recombine their competences when environments shift faster than routine operations can accommodate [5]. Teece disaggregates these into sensing (identifying threats and opportunities), seizing (mobilizing resources to respond), and transforming (continuous renewal of the organization's asset base) [6]. Although developed for firms in competitive markets, the logic transfers to public institutions confronting environmental turbulence: a testing agency that cannot sense anomalies, seize the response window, and transform its procedures is structurally fragile regardless of its routine operational competence.

Organizational resilience research runs parallel. Duchek conceptualizes resilience as a meta-capability comprising three successive stages (anticipation, coping, and adaptation) underpinned by concrete organizational routines rather than static contingency plans [4]. High-reliability scholarship similarly locates resilience in mindful anticipation and containment practices embedded in daily operations [7]. What remains underspecified in both traditions is the mechanism question for digitally mediated crises: through what concrete, technologically enabled routines do public organizations anticipate, cope, and adapt when the information environment itself is the arena of the crisis? This study addresses that micro-foundational gap.

2.3 Digital Governance Capabilities

We define *digital governance capability* as the organizational capacity to deploy digital systems for real-time sensing, verification, coordination, and public communication as an integrated element of executive decision-making, rather than as segregated technical support. The definition adapts the fusion view of digital business strategy, in which digital resources cease to be a subordinate functional strategy and become constitutive of organizational strategy itself [3], to the public-governance context, and is consistent with definitions of digital transformation as organizational change enabled by digital technologies rather than technology adoption per se [13].

E-government scholarship documents both the promise and the persistent gap between digital rhetoric and administrative reality [15], and the digital-era governance thesis argues that digital integration should reorganize the state around needs-based, joined-up processes [14]. Yet this literature centers overwhelmingly on routine service delivery. Its application to acute crisis governance, where verification speed, information asymmetry, and trust dynamics are decisive, remains thin, and crisis scholarship in turn typically treats information systems as decision support infrastructure rather than as governance capability [21]. This mutual blind spot is where the present study is positioned.

2.4 Stakeholder Management in Networked Publics

Stakeholder theory holds that organizational survival depends on managing relationships with the groups whose support the organization requires and whose interests its actions implicate [16]. Salience theory refines this: stakeholders command managerial attention as a function of their power, legitimacy, and urgency, and salience is dynamic, shifting as events unfold [17]. Governance-network scholarship adds that public problems are processed in networks of interdependent actors whose interactions no single authority controls [18], and crisis-network research shows that effective response increasingly depends on network governance capacity rather than hierarchical authority alone [19].

igitally mediated publics intensify all three insights: previously latent stakeholders can acquire power and urgency within days by self-organizing through horizontal platforms, transforming stakeholder management from periodic consultation into continuous, real-time engagement.

2.5 The Gap and the Study's Position

Each literature is individually mature, but their intersection is underdeveloped. Crisis management theorizes phases and tasks but treats technology as support infrastructure. Dynamic-capabilities and resilience research specifies capability categories but rarely their digital micro-foundations in public organizations. Digital governance research addresses routine administration, not acute institutional breakdown. Stakeholder research recognizes salience dynamics but seldom connects them to real-time crisis decision architecture. The NEET-UG 2026 crisis sits precisely at this four-way intersection, which motivates the integrated framework developed in Section 5.

III. RESEARCH METHODOLOGY

3.1 Research Design

This study adopts an abductive, qualitative single-case design focused on the National Testing Agency's (NTA) handling of the NEET-UG 2026 examination cycle. The design is abductive rather than purely inductive: analysis moved iteratively between the empirical record and prior theory (crisis management, dynamic capabilities, and digital governance) such that the CRISP framework presented in Section 5 was derived from the vulnerability themes identified in Section 4, then refined against existing theoretical categories. We report the analysis in that order to preserve the chain of evidence from data to framework [22]. Single-case methodology is appropriate where the case is revelatory or extreme and where the phenomenon under study cannot be meaningfully separated from its socio-political setting [22], [23]. NEET-UG 2026 satisfies both criteria: it compresses a documented security breach, decentralized digital mobilization, physical protest, a federal criminal investigation, and nationwide remediation into a single short and publicly documented window: an unusually complete stress test of every construct in our theoretical framing. The purposive selection of an extreme case supports analytical generalization to theory, not statistical generalization to populations [22].

3.2 Data Sources

The empirical foundation comprises three triangulated streams of publicly available documentary evidence covering the acute crisis window of May–July 2026: (1) official administrative publications, press releases, and notification circulars issued by the NTA and the Ministry of Education [1]; (2) investigative statements and press updates published by statutory bodies, including the CBI and the Press Information Bureau (PIB) [2]; and (3) documented public archives, contemporaneous reporting, and academic policy commentary evaluating ground-level student mobilization and digital responses. Triangulation across independently produced streams mitigates the single-source bias inherent in documentary research: convergence across official, investigative, and public records raises confidence in event claims; divergence was itself treated as data and interpreted as a communication gap.

The study raises no human-subjects concerns: it analyzes only publicly available institutional documents and publicly reported events, involves no interaction with individuals, and processes no personal data beyond what public authorities themselves have published.

3.3 Analytical Procedure

Documents were analyzed using reflexive thematic analysis following the six-phase protocol of familiarization, initial coding, theme construction, review, definition, and reporting [24]. Analysis was organized around three analytic categories specified a priori by the research questions: *decision nodes* (points at which the agency selected among response options), *communication gaps* (divergences between what the record shows was internally known and what was publicly disclosed, and when), and *structural vulnerabilities* (recurring organizational conditions enabling escalation). Consistent with the reflexive orientation of this approach, coding was undertaken interpretively by the authors, with themes developed and refined through iterative discussion until consensus, rather than through frequency-based codebook procedures [24]. Iterative comparison of vulnerability patterns across the three data streams produced the four aggregate themes reported in Section 4.3, each anchored to dated, documented events in the public record.

3.4 Validity Strategy and Rival Explanations

Four tactics support the credibility of the analysis. First, data triangulation across the three streams, as described above. Second, maintenance of a chain of evidence linking each theme to dated, citable documents [22]. Third, explicit examination of rival explanations for the study's central causal claim that disclosure delay reflected a capability deficit, including the possibility that delay was legally constrained by the concurrent criminal investigation; these rivals are analyzed in Section 4.4 rather than dismissed.

Fourth, bounded claim language: where the public record is silent, we claim absence of documented evidence, not absence of the underlying practice. The principal validity limitation, the absence of interview-based member checking with agency insiders, is acknowledged in Section 6.3 and motivates the future research agenda.

IV. CASE ANALYSIS

4.1 Escalation Chronology

The NEET-UG 2026 cycle illustrates the operational friction that arises when traditional public-sector decision-making encounters rapid digital communication flows. Following the initial security breaches of May 3, 2026, administrative responses relied on standard internal containment procedures. The speed of horizontal digital networks, however, outpaced official communication loops, allowing unverified reports and student concerns to diffuse rapidly and intensifying public pressure on testing authorities. Figure 1 reconstructs the escalation sequence in chronological order; documentary sources for each stage are noted in the caption.

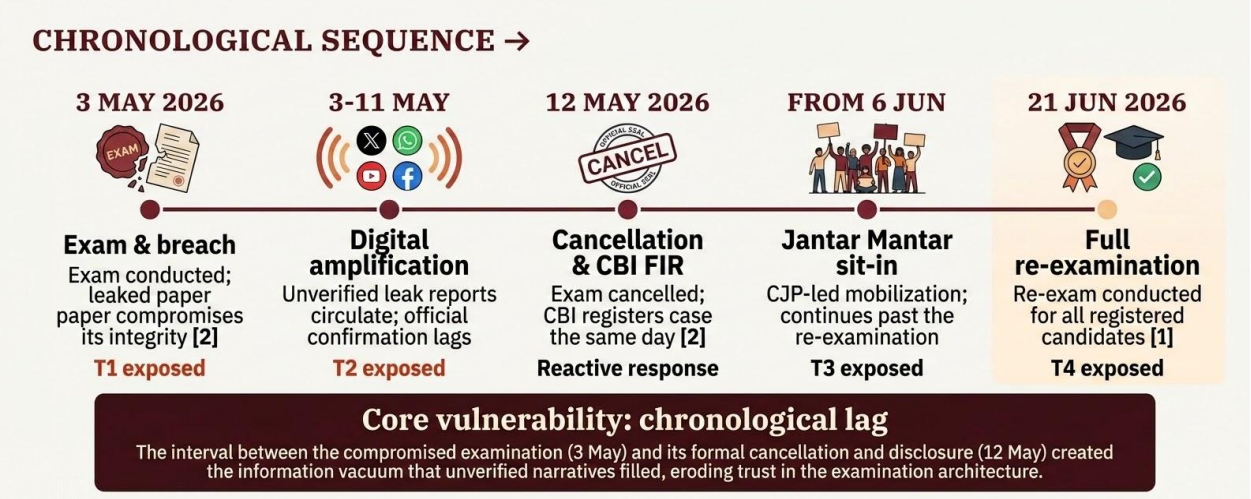

Figure 1. Escalation chronology of the NEET-UG 2026 crisis, with the vulnerability theme (T1–T4, Section 4.3) exposed at each stage. Documentary sources: official records [1], [2]; public digital archives and contemporaneous reporting.

Two features of the chronology deserve emphasis. First, nine days elapsed between the compromised examination and its formal cancellation and disclosure, a window in which unverified leak reports circulated unchecked; Section 4.3 codes this as the recognition and verification lag. Second, remediation did not end the crisis: sustained public mobilization began on June 6, 2026, after both the cancellation and the re-examination announcement, continued past the June 21 re-examination, and culminated in the Union Education Minister's resignation on July 25, 2026, as documented in contemporaneous public reporting. Technical remedy without engagement and visible learning, in other words, did not close the accountability demand.

4.2 Stakeholder Mapping

Applying the salience framework [17] to the case reveals why conventional public-relations containment failed: the crisis rapidly reordered stakeholder salience. Candidates and parents, routinely treated as passive service recipients, acquired power (network mobilization), urgency (time-critical academic futures), and legitimacy (documented breach) within days, becoming definitive stakeholders whose claims could not be deferred. Table 1 summarizes the principal stakeholders, their interests, salience trajectory, communication channels, and the institutional engagement observable in the public record.

Table 1. Stakeholder map of the NEET-UG 2026 crisis (salience categories per Mitchell et al. [17]).

Stakeholder	Primary interest	Salience trajectory	Principal channels	Observed engagement
Candidates and parents	Fair, credible examination; certainty about validity of results	Latent → definitive (power + urgency + legitimacy) within days	Social platforms; messaging networks; physical protest	Episodic official notices; no continuous two-way channel documented

Student collectives (incl. CJP)	Accountability; re-examination; systemic reform	Demanding → definitive via mobilization	Horizontal digital organizing; demonstrations	Interaction primarily via law-enforcement response, per public record
NTA / Ministry of Education	Operational continuity; institutional credibility	Focal organization	Official circulars; press releases	Hierarchical, one-way, lagged [1]
CBI / investigative bodies	Criminal accountability; evidence integrity	Dormant → dominant upon case registration	Formal releases via PIB	Formal disclosure from May 12 [2]
Media (traditional and digital)	Timely, accurate information	Continuously salient	Reporting; amplification of both official and unofficial narratives	Reactive briefings; vacuum filled by unverified sources

4.3 Thematic Findings

Analysis of decision nodes, communication gaps, and structural vulnerabilities produced four aggregate themes. Table 2 presents the theme–evidence matrix, with evidence stated at the level of dated, documented events in the public record; each theme is then elaborated.

Table 2. Theme–evidence matrix (evidence at the level of documented events in the public record). Data streams per Section 3.2: Stream 1 = official administrative records (NTA/Ministry of Education); Stream 2 = statutory investigative sources (CBI/PIB); Stream 3 = public digital archives and contemporaneous reporting.

Aggregate theme	Constituent patterns	Documented evidence base	Data streams
T1. Delayed anomaly recognition	Reliance on late-stage hierarchical reporting; anomaly surfaced to leadership via external channels; no documented early-warning monitoring	Interval between the May 3 breach and formal institutional acknowledgment in the official record [1], [2], set against earlier circulation of leak reports in public digital channels.	Streams 1, 3
T2. Verification vacuum	No authoritative real-time verification of breach scope; persistent public uncertainty; unverified narratives fill the information space	Absence of an authoritative, continuously updated scope statement in the official record between May 3 and the May 12 case registration [2], while unverified scope claims circulated publicly.	Streams 1, 2, 3
T3. Engagement asymmetry	One-way, episodic official communication vs. continuous many-to-many stakeholder communication; engagement via enforcement rather than dialogue	Episodic cadence of official notices [1] contrasted with continuous decentralized mobilization culminating in the documented Jantar Mantar demonstrations.	Streams 1, 3
T4. Absent learning loop	Remediation framed as episodic fix (re-exam); no publicly documented post-crisis evaluation or structural reform commitment within the study window	The June 21 full re-examination [1] unaccompanied, in the public record of the study window, by a published post-crisis evaluation or reform roadmap.	Streams 1, 2

Theme 1: Delayed anomaly recognition. The public record indicates that leadership-level acknowledgment of the breach trailed its circulation in digital channels. Decision nodes in this window show reliance on standard internal containment, a hierarchical reporting pathway structurally slower than the horizontal networks already carrying the information. In dynamic-capabilities terms, this is a sensing failure [6]: the organization's detection apparatus was oriented toward internal procedure rather than toward the environment in which the crisis was actually unfolding.

Theme 2: Verification vacuum. Between the breach and formal investigative disclosure on May 12 [2], no authoritative, continuously updated account of the breach's scope is observable in the official record. In an information ecosystem abhorring a vacuum, unverified narratives supplied the missing account. The vulnerability is not that rumor existed (it always will) but that the institution possessed no visible mechanism to verify faster than rumor could propagate.

Theme 3: Engagement asymmetry. Official communication remained episodic, one-way, and channel-limited while stakeholder communication was continuous, many-to-many, and platform-native. The asymmetry converted latent stakeholders into definitive ones (Table 1) and shifted the locus of accountability demands from administrative channels to the street. Where engagement occurred, the record shows it mediated substantially through law-enforcement response rather than institutional dialogue, the inverse of the legitimacy-building that crisis governance requires [12]. The mobilization, initiated on June 6, 2026 by the CJP and allied student organizations, persisted past the June 21 re-examination and culminated in the Union Education Minister's resignation on July 25, 2026: remediation without engagement did not close the accountability demand.

Theme 4: Absent learning loop. The full June 21 re-examination [1], conducted for all registered candidates after cancellation of the compromised exam, resolved the immediate distributive question but, within the study window and on the public record, was not accompanied by a published post-crisis evaluation, reform roadmap, or institutional-learning commitment. We bound this claim carefully: the absence is of documented evidence, not necessarily of internal activity.

But for a public institution whose crisis was fundamentally one of trust, undocumented learning is unavailable to the audiences whose confidence must be rebuilt: invisible adaptation forfeits its legitimacy dividend [4], [12].

The master vulnerability: chronological lag.

The four themes converge on a single higher-order pattern: the interval between internal detection and transparent public disclosure. T1 lengthens the front of the interval; T2 and T3 determine what fills it; T4 ensures its recurrence. We term this interval chronological lag and identify it as the case's core administrative vulnerability: the lag created an information vacuum, the vacuum was filled by unverified digital narratives, and the resulting narrative asymmetry, not the leak alone, is what eroded public confidence in the examination architecture.

4.4 Rival Explanations

Rival 1: Legal constraint. The strongest alternative to a capability-deficit reading is that disclosure was legally constrained: once matters proceed toward criminal investigation, agencies face genuine limits on releasing case-relevant details, and premature disclosure can compromise evidence. Three considerations bound, without eliminating, this rival. First, the lag predates the May 12 case registration [2]; legal constraint cannot explain silence in the window before formal proceedings existed.

Second, legal constraint restricts content disclosure (what is known about culprits and methods) but not process disclosure (what the agency is doing, what is verified versus unverified, when the next update will come); the observed gap extends to process communication, which investigation-sensitive agencies elsewhere routinely provide.

Third, if legal constraints were the operative mechanism, one would expect explicit communication of the constraint itself; the record does not document such meta-communication. We therefore retain the capability-deficit interpretation for process-level communication while conceding that content-level reticence after May 12 may be legally overdetermined.

Rival 2: Deliberate strategic silence. Delay might reflect a considered judgment that early disclosure would amplify panic. The record cannot exclude this, but the outcome pattern argues against its rationality as strategy: silence did not dampen amplification, it ceded the narrative. Under either reading, incapacity or misjudged choice, the prescriptive conclusion of Section 5 stands: institutions require standing capabilities that make fast, verified process disclosure the low-cost default.

Rival 3: Hierarchical clearance. Delay may have originated above the agency, in ministerial clearance requirements, rather than within it. This would relocate rather than refute the capability gap: decision rights over crisis communication are themselves an organizational design variable, and Section 5.4 addresses them explicitly.

V. THE CRISP FRAMEWORK

5.1 Derivation: From Vulnerabilities to Capabilities

Each aggregate theme identifies a structural vulnerability; each CRISP capability is the institutionalized inverse of one vulnerability. This derivation logic, capability as the mirror image of empirically observed failure, is what distinguishes the framework from an a priori checklist. Figure 2 makes the mapping explicit.

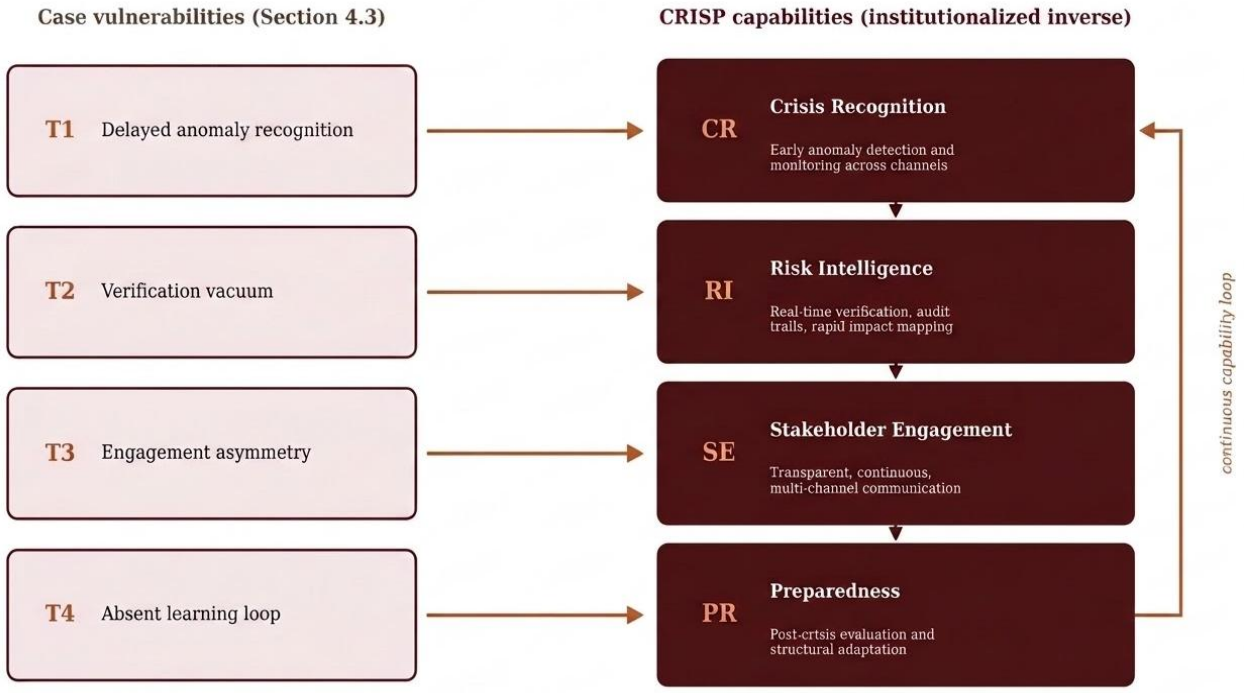

Figure 2. Derivation of the CRISP framework: each capability is the institutionalized inverse of one empirically observed vulnerability, connected as a continuous loop.

The four capabilities operate as a continuous loop rather than sequential phases: recognition feeds intelligence, intelligence disciplines engagement, engagement surfaces new signals for recognition, and preparedness upgrades all three between cycles. Digital governance capability, as defined in Section 2.3, is the connective mechanism of the loop: the means through which sensing, verifying, engaging, and learning are executed at the speed of the information environment.

This is the study's answer to RQ1: digital transformation functions as strategic governance when it constitutes the loop, and as a back-office function when it merely supports isolated stages.

5.2 Positioning Against Prior Models

CRISP is indebted to, but distinct from, four established bodies of work. Table 3 states the comparison explicitly on five dimensions.

Table 3. CRISP positioned against prior frameworks.

Dimension	Crisis lifecycle / SCCT [11]	Resilience stages [4]	Dynamic capabilities [5], [6]	CRISP (this study)
Temporal logic	Sequential phases (pre-, acute, post-crisis)	Successive stages (anticipation, coping, adaptation)	Ongoing routines (sensing, seizing, transforming)	Simultaneous, continuous loop across four capabilities
Role of technology	Communication channel/support	Largely unspecified	Enabler among resources	Constitutive governance mechanism connecting all capabilities
Unit of application	Corporate/organizational communication	Firms; generic organizations	Firms in competitive markets	Public institutions in multi-stakeholder crises
Communication	One phase/function among several	Implicit within coping	Not focal	Standing capability (SE) with specified process-disclosure discipline
Learning	Post-crisis stage	Adaptation stage	Transforming	Institutionalized loop closure (PR) with public documentation as legitimacy device

Read against dynamic-capabilities theory, CRISP can be understood as a public-sector specification of the sensing–seizing–transforming triad [6]: CR and RI operationalize sensing under crisis time-compression; SE and crisis response operationalize seizing where the resource being mobilized is public trust; PR operationalizes transforming with the added public-sector requirement that adaptation be visible to be legitimacy-restoring [12]. Read against Duchek [4], CRISP supplies the digitally enabled micro-foundation that the anticipation–coping–adaptation model leaves abstract. These correspondences are a feature, not a redundancy: the framework's claim to novelty rests on the integration and the repositioning of digital capability, not on the invention of previously unknown categories.

5.3 Operationalizing CRISP: Loci, Decision Rights, Triggers, and Indicators

RQ2 demands specificity beyond capability labels. Table 4 states, for each capability, its proposed organizational locus, the decision rights and activation triggers required for it to function at crisis speed, and illustrative performance indicators. The master indicator across the framework is the detection-to-disclosure interval (chronological lag itself), which renders the case's core vulnerability directly measurable and manageable.

Table 4. Operational specification of CRISP capabilities.

Capability	Organizational locus	Decision rights and activation triggers	Illustrative indicators
CR	Standing Examination Integrity Cell with unified view of center-level operations and digital-channel monitoring; direct reporting line to the Director-General	Authority to declare an anomaly event and convene the response protocol without prior ministerial clearance; trigger: any corroborated anomaly signal from two independent channels	Time from anomaly occurrence to internal flag; share of anomalies first detected internally vs. externally
RI	Risk-intelligence function within the Cell, with pre-	Authority to commission immediate audit-trail pulls and	Time from flag to verified scope assessment;

Capability	Organizational locus	Decision rights and activation triggers	Illustrative indicators
	authorized access to distribution logs, center audit trails, and digital forensics support	forensic verification; trigger: anomaly declaration by CR	proportion of public claims verified/refuted within 24 h
SE	Crisis communication unit with pre-approved multi-channel protocol (portal, press, platform presence) and standing legal-review fast track	Delegated authority to issue process disclosures (what is verified, what is not, next update time) without case-content clearance; trigger: verified scope assessment or 12 h elapsed, whichever first	Detection-to-first-disclosure interval; update cadence adherence; reach across stakeholder segments
PR	Post-event review board with published terms of reference; findings feed mandatory changes to the next cycle's protocol	Authority to require written management response to each recommendation; trigger: closure of any anomaly event	Share of recommendations implemented before next cycle; publication of lessons-learned report

5.4 Boundary Conditions: Delivery-Mode Adaptation

The framework's execution must adapt to the underlying test-delivery architecture. In paper-based systems, CR and RI center on physical supply-chain integrity: secure cargo transit tracking, vault infrastructure, and center-level invigilation protocols. In computer-based environments, the same capabilities shift toward cybersecurity auditing, server stress-testing, real-time telemetry monitoring, and encrypted digital identity verification. SE and PR are delivery-mode invariant.

Aligning protocols with these operational boundaries ensures targeted response to the specific failure surface of each delivery mode; technology substitution without governance transformation merely relocates the vulnerability.

VI. DISCUSSION

6.1 Theoretical Contributions

The study makes three contributions:

1. It extends the fusion view of digital strategy [3] from competitive firm strategy to crisis-governed public institutions: in the examination-governance context, digital capability is shown to be constitutive of the institution's core trust-production function, not an enabler adjacent to it.
2. It supplies a digitally enabled micro-foundation for capability-based resilience [4], specifying the concrete routines through which anticipation, coping, and adaptation are executed when the information environment is itself the crisis arena.
3. It translates the dynamic-capabilities triad [5], [6] into public-sector crisis governance, with the distinctive amendment that transforming must be publicly documented to convert adaptation into restored legitimacy [12].

Methodologically, the identification of chronological lag as a measurable master vulnerability offers a construct that future quantitative work can operationalize directly.

6.2 Practical Implications

For public administrators, the analysis yields a compact prescription: measure and manage the detection-to-disclosure interval as a first-order performance variable. The operational specification in Table 4 provides an implementable starting architecture whose principal cost is organizational redesign (decision rights, standing protocols, review discipline) rather than capital-intensive technology acquisition.

The distinction between content disclosure and process disclosure gives agencies under legal constraint a communication discipline that preserves both evidentiary integrity and public trust. For enterprise managers beyond the public sector, the mechanism transfers directly: product recalls, data breaches, and reputational crises confront firms with the same physics of horizontal information networks outpacing internal hierarchy.

6.3 Limitations

Five limitations bound the claims:

1. The single-case design supports analytical, not statistical, generalization; transfer to other testing bodies or jurisdictions is an empirical question.
2. Reliance on secondary documentary data means the analysis cannot access decision-makers' private reasoning; the rival-explanation analysis in Section 4.4 mitigates but does not eliminate this constraint.
3. Evidence is presented at the level of dated, documented events in the public record rather than as a verbatim documentary audit trail with excerpt-level citation; constructing that fuller audit trail, including systematic archiving of the digital-platform record, is a priority for the journal-length development of this work.
4. The study window covers the acute crisis phase; longer-run reform trajectories fall outside it, and the T4 finding of an absent learning loop is bound to the public record within that window.
5. The recency of the events means investigative findings may still evolve; the analysis rests only on facts documented in the official record at the time of writing.

6.4 Future Research

Three extensions follow directly. Comparative case studies across paper-based, computer-based, and hybrid assessment systems, and across jurisdictions, would test the framework's boundary conditions. Semi-structured interviews with administrators, policymakers, and student-advocacy stakeholders would adjudicate among the rival explanations of Section 4.4, particularly the locus of disclosure decision rights. Finally, quantitative operationalization of chronological lag across a panel of examination crises would permit testing of the study's central proposition: that detection-to-disclosure interval predicts trust erosion better than breach severity itself.

VII. CONCLUSION

This study set out to understand how public testing bodies can survive high-stakes operational crises in hyperconnected information environments, and what capabilities would move them from reactive control to durable resilience. Analysis of the NEET-UG 2026 crisis identified four interlocking vulnerabilities converging on a single master vulnerability, chronological lag between detection and disclosure, and derived from them the CRISP framework: a continuous loop of Crisis Recognition, Risk Intelligence, Stakeholder Engagement, and Preparedness, connected by digital governance capability functioning as a strategic mechanism rather than a back-office tool. Modern institutional resilience, the case suggests, is not built by containing crises after they break; it is built by embedding recognition, intelligence, engagement, and learning into governance before they do.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the professional support and encouragement of Mr. Pritesh Patil, Globant India Pvt. Ltd.

DECLARATIONS

Funding: This research received no external funding. Conflicts of interest: The authors declare no conflict of interest. Data availability: All documents analyzed are publicly available from the issuing bodies cited in the references.

AI DECLARATION

The authors acknowledge the use of AI-assisted tools (Google Gemini and Anthropic Claude) for language refinement, structuring, narrative flow enhancement, and revision support during the drafting and revision process. All research design, data collection, analysis, framework development, and conclusions are the authors' own. The authors have reviewed and edited all content for accuracy and are responsible for the final manuscript and its contents.

REFERENCES

[1] National Testing Agency, “Conduct of re-examination for National Eligibility-cum-Entrance Test [NEET (UG)] 2026,” Ministry of Education, Government of India, 2026.

[2] Press Information Bureau, “CBI registers case in alleged paper leak in NEET-UG 2026,” Ministry of Home Affairs, Government of India, May 12, 2026.

[3] A. Bharadwaj, O. A. El Sawy, P. A. Pavlou, and N. Venkatraman, “Digital business strategy:

Toward a next generation of insights," MIS Quarterly, vol. 37, no. 2, pp. 471–482, 2013.

[4] S. Duchek, "Organizational resilience: A capability-based conceptualization," Business Research, vol. 13, no. 1, pp. 215–246, 2020.

[5] D. J. Teece, G. Pisano, and A. Shuen, "Dynamic capabilities and strategic management," Strategic Management Journal, vol. 18, no. 7, pp. 509–533, 1997.

[6] D. J. Teece, "Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance," Strategic Management Journal, vol. 28, no. 13, pp. 1319–1350, 2007.

[7] K. E. Weick and K. M. Sutcliffe, Managing the Unexpected: Sustained Performance in a Complex World, 3rd ed. Hoboken, NJ, USA: Wiley, 2015.

[8] L. K. Comfort, "Crisis management in hindsight: Cognition, communication, coordination, and control," Public Administration Review, vol. 67, no. s1, pp. 189–197, 2007.

[9] A. Boin, P. 't Hart, E. Stern, and B. Sundelius, The Politics of Crisis Management: Public Leadership Under Pressure, 2nd ed. Cambridge, U.K.: Cambridge University Press, 2017.

[10] C. M. Pearson and J. A. Clair, "Reframing crisis management," Academy of Management Review, vol. 23, no. 1, pp. 59–76, 1998.

[11] W. T. Coombs, Ongoing Crisis Communication: Planning, Managing, and Responding, 5th ed. Thousand Oaks, CA, USA: SAGE Publications, 2019.

[12] T. Christensen, P. Lægreid, and L. H. Rykkja, "Organizing for crisis management: Building governance capacity and legitimacy," Public Administration Review, vol. 76, no. 6, pp. 887–897, 2016.

[13] I. Mergel, N. Edelmann, and N. Haug, "Defining digital transformation: Results from expert interviews," Government Information Quarterly, vol. 36, no. 4, Art. no. 101385, 2019.

[14] P. Dunleavy, H. Margetts, S. Bastow, and J. Tinkler, Digital Era Governance: IT Corporations, the State, and E-Government. Oxford, U.K.: Oxford University Press, 2006.

[15] M. J. Moon, "The evolution of e-government among municipalities: Rhetoric or reality?" Public Administration Review, vol. 62, no. 4, pp. 424–433, 2002.

[16] R. E. Freeman, Strategic Management: A Stakeholder Approach. Boston, MA, USA: Pitman, 1984.

[17] R. K. Mitchell, B. R. Agle, and D. J. Wood, "Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts," Academy of Management Review, vol. 22, no. 4, pp. 853–886, 1997.

[18] E. H. Klijn and J. Koppenjan, Governance Networks in the Public Sector. London, U.K.: Routledge, 2016.

[19] N. Kapucu and Q. Hu, Network Governance: Concepts, Theories, and Applications. New York, NY, USA: Routledge, 2020.

[20] J. R. Harrald, "Agility and discipline: Critical success factors for disaster response," The Annals of the American Academy of Political and Social Science, vol. 604, no. 1, pp. 256–272, 2006.

[21] B. Van de Walle and M. Turoff, "Decision support for emergency situations," Information Systems and e-Business Management, vol. 6, no. 3, pp. 295–316, 2008.

[22] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed. Thousand Oaks, CA, USA: SAGE Publications, 2018.

[23] K. M. Eisenhardt, "Building theories from case study research," Academy of Management Review, vol. 14, no. 4, pp. 532–550, 1989.

[24] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.