THE BHARAT NATIONAL RESILIENCE INDEX (BNRI)

A National Framework for Measurable Security, Safety, and Systemic Continuity Compliance

Bharat Assets Protection Institute
(B.A.P-I)

THE BHARAT NATIONAL RESILIENCE INDEX (BNRI)

A National Framework for Measurable Security, Safety, and Systemic Continuity Compliance

Doctrinal Framework and Measurement Guideline

Dr. Padmalochan Dash
Bharat Assets Protection Institute (B.A.P-I)

"धैर्यम् एव राष्ट्रस्य प्राणः"

Resilience is the life-breath of the Nation.

About the Author

Dr. Padmalochan Dash is a national security expert and the Founding Director of the Bharat Assets Protection Institute (B.A.P-I). He holds an MA and MPhil in South and Southeast Asian Studies, and an MPhil and PhD in Internal Security (Homeland Security), with over eighteen years across teaching, research, industry consultancy, institution-building, and social philanthropic engagement. He writes extensively on politics, diplomacy, and international affairs, specialising in internal security governance, critical infrastructure protection, strategic manufacturing, and supply chain resilience. His published work includes the conceptualisation of the Bharat National Resilience Index (BNRI), the Bharat National Resilience Ecosystem (BNRE), the BAP-I Twelve-Cluster Securitisation Model, and the Prahari framework. Through B.A.P-I, he advances a research agenda that repositions critical infrastructure protection and sectoral resilience as the third pillar of India's comprehensive national security.

Publication Details

Published by: Bharat Assets Protection Institute (B.A.P-I)
Year of Publication: 2025 Edition: First
Contact: bharatassetsprotection@gmail.com
Web: www.bharatassetsprotection.org

Contents

Contents

Contents

Section

ABSTRACT

India's critical infrastructure has matured into an interdependent cyber-physical ecosystem in which disruptions cascade across sectors at a pace that outstrips conventional response architectures. No unified resilience metric exists; governance remains fragmented and recovery uneven. The Bharat National Resilience Index (BNRI) is proposed as a statutory instrument to quantify resilience as a measurable systems property, integrating threat assessment, zero-tolerance compliance, adaptive governance, and defence-in-depth engineering within a single national framework. Through all-hazards consequence mapping and structured public–private coordination, BNRI converts resilience from reactive crisis management into anticipatory continuity governance. It lays the technical and policy groundwork for harmonised regulation, enforceable accountability, and sustained service integrity across India's critical sectors (Dash, 2025, May 31).

Keywords: Critical Infrastructure Protection (CIP), Bharat National Resilience Index (BNRI), Bharat National Resilience Ecosystem (BNRE), Cyber-Physical Systems, Adaptive Risk Governance, Defence-in-Depth, Zero-Tolerance Compliance, Public–Private Integration, Continuity Modelling, All-Hazards Framework, Legal and Regulatory Harmonisation, Critical Infrastructure Protection Act (CIPA), National Critical Infrastructure Authority (NCIA), BIPCARD, SOMA, RAS, Prahari

INTRODUCTORY OVERVIEW

The Bharat National Resilience Index (BNRI) marks a decisive departure from fragmented crisis management toward a unified, empirically governed system of national continuity. It is conceived as both policy doctrine and engineering standard; a measurable instrument that institutionalises resilience as a quantifiable state function across India's strategic, infrastructural, and governance domains (Dash, 2025, May 31).

Its doctrinal premise is threefold: resilience must be legally enforceable, technically auditable, and dynamically recalibrated. The framework integrates multi-domain audits, telemetry-based data ingestion, digital-twin simulations, and predictive analytics to yield an empirically derived national resilience score. The National Critical Infrastructure Authority (NCIA) serves as apex enforcement body; the BNRI Assessment and Accreditation Council (BNRI-AAC) provides technical certification; and the Resilience Assessment and Synchronisation bureau (RAS) administers scoring independently (Dash, 2025, Jan. 30).

India's power grids, ports, logistics corridors, and data networks now operate as a single cyber-physical organism; interlinked through algorithms, control systems, and human oversight. A malware intrusion at an airport, a flood in Assam, or a data-centre failure in Mumbai can trigger cascading failures across this interdependent web. Protection models that confine themselves to shielding individual assets are no longer adequate; what is required is the engineered capacity to absorb, adapt, and restore essential functions under compound stress (Rinaldi, Peerenboom & Kelly, 2001; Dash, 2025, Jul. 1).

BNRI proposes a composite methodology, integrating resilience metrics, digital-twin simulations, and sector-wise continuity assessments; to effect the transition from reactive defence to predictive, adaptive governance. At the strategic level, it functions simultaneously as governance protocol and foresight engine, mirroring the logic of adaptive regulation set out in the OECD's Compendium of Good Practices on Quality Infrastructure (OECD, 2024). This positions the BNRI within the national security doctrinal arsenal. It is not a military instrument, but as a civil-defence multiplier enabling foresight-based governance, resilience scoring, and public accountability.

I. DOCTRINAL FOUNDATION

1.1 Conceptual Definition

The **Bharat National Resilience Index (BNRI)** is a statutory measurement-and-compliance system that quantifies, audits, and enforces resilience, safety, and security across India's critical infrastructure, strategic manufacturing, supply chains, and governance lifelines. It converts resilience from a policy aspiration into mandatory, inspectable obligations; graded, penalised, and incentivised (Dash, 2025, May 31).

BNRI is operated under the **National Critical Infrastructure Authority (NCIA)** with accreditation by the **BNRI Assessment and Accreditation Council (BNRI-AAC)** and field-level execution by certified **Resilience Audit Bodies (RABs)**. Within the wider Bharat National Resilience Ecosystem (BNRE), RAS administers scoring independently of BIPCARD's governance directorate, while Prahari provides the dedicated operational force for field-level protection and compliance verification (Dash, 2025, Jan. 30; Dash, 2025, Dec. 25).

BNRI functions simultaneously as **(a)** a regulatory instrument; statutory audits, inspections, disclosure, sanctions, and incentives; and **(b)** a knowledge architecture; data lake, digital twins, cascade models, and foresight analytics. Covered systems must withstand disruption, localise failure, recover within codified MTTR limits, and maintain essential services under compound stress; physical, cyber, environmental, and socio-political.

The framework reconciles statutory enforcement with adaptive intelligence. Its foundation rests on four measurable parameters; preparedness, mitigation, response, and recovery; corresponding to the resilience function **Rc = f(P, M, Ra, Rr)** as articulated in the Resilience Measurement Index (Fisher et al., 2010; Argonne National Laboratory, 2013). BNRI thereby establishes a doctrinal shift from protection-by-design to continuity-by-compliance, an evolution consistent with CISA's Infrastructure Resilience Planning Framework (CISA, 2022, Aug.).

1.2 Measurement Logic and Formulae

BNRI expresses national resilience as a composite function: **Rc = f(P, M, Ra, Rr)** where **P** denotes preparedness (training frequency, planning coverage, resource readiness), **M** denotes mitigation (protective investments, redundancy ratios, preventive controls), **Ra** denotes response (detection time, containment efficiency, operational uptime during incident), and **Rr** denotes recovery (MTTR, reconstitution rate, post-event learning cycle). Each parameter is scored on a 0–100 scale using normalised, weighted indicators derived from statutory audits, regulator filings, and accredited third-party reports. The composite score is aggregated through a weighted geometric mean to prevent any single indicator from dominating the result.

The operational computation model is:

BNRI_Score = [Σ(Wi × Si^norm)] × K_comp × (1 − C_cascade) × C_crit

where **Si^norm** denotes indicator values (0–100) after min–max normalisation and evidentiary validation; **Wi** denotes codified weights aligned to the ten BNRI dimensions; **K_comp ∈ [0,1]** is the compliance gate multiplier, which drops with overdue audits, late disclosures, or critical non-conformances; **C_cascade ∈ [0,1]** is the cascade-exposure penalty derived from interdependency stress tests and digital-twin simulations; and **C_crit ≥ 1** is the criticality uplift for Tier-A national lifelines, which

tightens scoring thresholds and amplifies identified deficits. The mathematical rationale and derivation logic for each modifier are set out in Appendix A.

Indicator categories are classified as Binary (0/1) for presence of certified security systems or redundancy switches; Ordinal (1–5) for maturity of response protocols; and Continuous (0–100) for quantitative operational metrics such as MTTR and uptime percentage. Documented scoring logic is publicly released by NCIA under CIPA Schedule-II.

Table 1. Domain-to-Metric Map (Representative)

Domain	Primary Objectives	Representative Measurable Outputs
Critical Infrastructure	Continuity, defence-in-depth, MTTR compliance	BNRI Class, MTTR (P95), redundancy %, red-team pass rate
Strategic Manufacturing	Tech sovereignty, IP and export-control assurance	Secure-by-design %, IP breach rate, dual-use compliance index
Supply Chain & Logistics	Traceability, rerouting agility, stockpile integrity	% traceable consignments, reroute TTR, spoilage/stock-out P95
Technology Sovereignty	Indigenous R&D continuity, knowledge retention	Research succession %, indigenisation ratio, secure-by-design certification
Comprehensive National Security	COOP, cyber integrity, crisis communications	COOP test pass %, CERT MTTD/MTTR, incident disclosure SLA
Global Engagement	Cross-border exposure, mutual aid readiness	Equivalence score, FDI resilience index, MoU compliance rate

1.3 System-of-Systems View

India's resilience posture is a network property. Failure in a Tier-A node, such as a grid substation, a core router, or an RTGS switch, propagates into logistics, water, health, finance, and governance services within minutes. BNRI evaluates both sectoral strength and interdependency resilience, making cross-sector cascade exposure a scored, reportable metric. The Dependency-Interdependency Matrix developed in the CIP research programme provides the analytical substrate for this assessment (Dash, 2025; Rinaldi, Peerenboom & Kelly, 2001; Ouyang, 2014).

1.4 Data Provenance and Integrity

All data streams entering the BNRI originate from authorised entities; regulators, accredited RABs, and government-certified operators. Self-reported data are admissible only when validated by a registered verifier under NCIA. Conflict-of-interest declarations and random re-audits safeguard integrity. Loss of sovereignty continuity is defined as any event causing prolonged (> 72 h) nationwide disruption of essential functions or degradation of governance capability beyond tolerance bands set by NCIA; breach of these thresholds triggers mandatory escalation and review.

1.5 Federal Alignment

The framework recognises the constitutional concurrency between Centre and States. Each State Resilience Cell collects local data and coordinates with NCIA through a unified protocol, mirroring the Centre–State coordination architecture prescribed under

BIPCARD's State CIP Coordination Cells (Dash, 2025, Jan. 30). State utilities, municipal networks, and private operators are measured under common national indicators while retaining operational autonomy.

1.6 Global Alignment

BNRI Construct	OECD / CISA Equivalent	Primary Function
Preparedness (P)	Prevention / Readiness (NIPP, 2013)	Pre-incident capability
Mitigation (M)	Protection / Risk Reduction (OECD, 2025, Jun. 19)	Infrastructure hardening
Response (Ra)	Consequence Management (CISA IRPF, 2022, Aug.)	Real-time operational control
Recovery (Rr)	Restoration / Adaptation (Sendai Framework, 2015)	Post-event reconstitution
BNRI Composite	Resilience Index (Ganin et al., 2016, Jan. 19)	Evidence-based governance

1.7 Compliance Doctrine

- **Zero-tolerance baseline:** Minimum mandatory controls; MFA coverage, patch SLAs, OT-IT segmentation, incident reporting ≤ 24 h; codified under CIPA Schedule-II.
- **Enforcement:** Sanctions for non-compliance; Resilience Credits and procurement/FDI preferences for high performers; codified under CIPA Schedule-III.
- **Transparency:** Public BNRI grades (A–E) for lifeline operators; confidential technical annexures for sensitive assets.
- **Standards equivalence:** Interoperable with ISO/IEC 27001:2022, UNDRR Sendai priorities, NATO infrastructure resilience principles, and allied certifications.
- **Audit chain of custody:** Digitally signed evidence packs; verifiable data lineage in the BNRI Data Lake; reproducible scoring.

1.8 Critical Analytical Consolidation

The Doctrinal Foundation constitutes the intellectual and regulatory nucleus of India's national resilience architecture. It converts resilience into a measurable, enforceable, and evolvable construct; anchored in law, supported by data, and operationalised through audit-based computation. The BNRI Grid enables data convergence; the BNRI Scale provides quantified comparability; the BNRI-AAC institutionalises accountability and learning; and RAS administers measurement independently of governance direction (Dash, 2025, Jan. 30).

Three interlocking imperatives sustain this foundation: (i) Quantification of Governance; every obligation carries a numerical score; (ii) Institutional Embedding; NCIA enforces centrally while BNRI-AAC standardises technical validation through accredited RABs; and (iii) Dynamic Legality; annual recalibration and post-incident re-scoring embed adaptability into law. If these conditions remain institutionally assured, BNRI will constitute the world's first statutory resilience calculus, integrating law, engineering, data science, and security doctrine into a single measurable continuum of national safety, security, and systemic continuity.

II. STRENGTHS OF THE PROPOSED BNRI FRAMEWORK

BNRI represents a doctrinal inflection point for India's national security architecture. It converts resilience from a normative aspiration into a measurable obligation of governance; what the OECD terms governance through measurement (OECD, 2025, Jun. 19).

2.1 Doctrinal Innovation; Statutory Resilience Calculus

BNRI addresses India's long-standing enforcement deficit by establishing a legal calculus of resilience. Prior approaches treated continuity and safety as advisory. BNRI transforms them into codified obligations under CIPA; enforceable through inspection powers, statutory benchmarks (MTTR ≤ codified thresholds), 24-hour incident disclosure, and structured incentive–penalty loops. This reflects the structured resilience governance model that CISA articulates in the IRPF (CISA, 2022, Aug.).

A minimum three-year rolling cycle governs measurement: annual audits, mid-term reviews, and triennial re-benchmarking. Every cycle encompasses data collection and validation, auditing and scoring, and policy feedback and recalibration. Indicators are re-weighted after each national incident review; institutionalising learning and preventing score stagnation.

Metric	Definition / Function
Enforcement Index (EI)	Weighted composite of inspection coverage, penalty realisation, and disclosure timeliness
MTTR P95 Compliance	95th-percentile mean-time-to-recovery benchmark across Tier-A lifelines
Recidivism Rate	Percentage of repeat non-conformances post-audit cycle; targeted for year-on-year reduction

2.2 Tiered Architecture; Proportionality by Systemic Significance

India's infrastructure exhibits asymmetric criticality. A uniform regulatory load would either cripple smaller operators or leave national lifelines under-secured. BNRI's Tier-A/B/C framework introduces proportional governance calibrated to systemic significance (Guo et al., 2021).

- **Tier A:** National lifelines; digital-twin stress testing, AI-anomaly grids, statutory MTTR, red-team cadence. Annual audits; semi-annual stress-tests.
- **Tier B:** Regional infrastructures; annual integrated audits, MFA/patching SLAs, compound-crisis drills. Biennial audits.
- **Tier C:** Foundational entities; minimum cyber hygiene, training, and reporting baselines. Triennial audits with randomised sampling.

Classification criteria: (i) economic criticality (GVA share ≥ 1%), (ii) population served ≥ 10 lakh, (iii) cross-sector dependency index ≥ 0.6, (iv) recovery time sensitivity ≤ 48 h. An entity meeting all four criteria falls within Tier-A; any two, Tier-B; otherwise, Tier-C. Reclassification is mandated every five years or upon significant structural change. The quantitative tiered model **BNRI_Tiered = α(Tier A) + β(Tier B) + γ(Tier C)**, where

$\alpha > \beta > \gamma$, allocates regulatory density in proportion to systemic risk; its derivation is set out in Appendix A.

2.3 Regulatory–Research Dualism

BNRI fuses compliance with learning. Audit data feed policy intelligence and enable adaptive regulation; mirroring the supervisory intelligence cycle in financial and cyber-security domains (CISA, 2022, Aug.; OECD, 2024). RABs rotate lead auditors every two cycles and undergo peer review by BNRI-AAC. Audit data processed within the NRDG are used by research partners including B.A.P-I to generate annual Resilience Insight Notes; peer-reviewed analytical briefs that translate compliance patterns into policy signals. This architecture responds to UNDP's observation that resilience governance must evolve through evidence loops and institutional learning, not enforcement alone (UNDP India, 2023).

Performance Indicator	Function
Learning Velocity Index (LVI)	Ratio of closed recommendations to new findings per quarter
Forecast Accuracy	Precision of anomaly prediction vs. actual events
Closed-Loop Rate	Share of mitigations verified by telemetry validation

2.4 Global Relevance; Interoperable, Not Imitative

BNRI positions India as a normative innovator rather than a standards-taker. Reciprocity clauses and standards mapping (ISO/IEC 27001:2022, UNDRR Sendai, EU NIS2, Australia SOCI Act 2018) provide cross-border interoperability without dependency. Equivalence certification allows mutual audit recognition, reducing compliance friction for international trade and financing (OECD, 2025, Jun. 19; Guo et al., 2021).

Criterion	Description	Transfer Mechanism
Legal adaptability	CIPA-style statutory anchor	Model Law template exchange via MoUs
Metric compatibility	ISO 22301/31000 alignment	Cross-walk tables and joint benchmarks
Data interoperability	API schema for resilience data	Shared metadata standards (UNDRR compliant)
Capacity building	Training for audit agencies	BNRI–B.A.P-I International Training Hub
Reciprocity	Recognition of BNRI certificates	Mutual acknowledgement under QUAD/UNDRR

2.5 Analytical Consolidation

The four structural strengths address distinct deficit vectors; legal, structural, epistemic, and diplomatic; while generating an adaptive, measurable, and exportable national standard.

BNRI Strength	Analytical Output	Impact Vector	Residual Risk if Absent
Doctrinal Innovation	Statutory compulsion from normative guidance	Enforcement and accountability	Policy rhetoric without execution
Tiered Architecture	Proportional control density by systemic criticality	Efficiency and equity	Regulatory overreach or under-protection

BNRI Strength	Analytical Output	Impact Vector	Residual Risk if Absent
Regulatory–Research Dualism	Predictive feedback embedded in compliance loops	Continuous learning and foresight	Static regimes and audit fatigue
Global Relevance	Rule-shaping role in international resilience governance	Diplomatic standing and market access	Isolation from global assurance markets

Three measurable technical effects follow: **(i) Compliance Velocity Gain (CVG)**; average audit-closure cycles reduce as automation, tiered obligations, and integrated dashboards compress remediation timelines; **(ii) Predictive Governance Index (PGI)**; foresight accuracy improves as the BNRI Data Lake and digital-twin simulations enable pre-emptive mitigation rather than post-incident reaction; **(iii) Global Equivalence Ratio (GER)**; the degree to which BNRI controls map onto international resilience frameworks provides measurable interoperability. Derivation and calibration methodology for CVG, PGI, and GER are detailed in Appendix A.

BNRI creates a quantified incentive ecosystem: Tier-A entities scoring ≥ 85 become eligible for Resilience Credits and priority procurement; Tier-B entities scoring ≥ 75 qualify for regulatory fee reductions; Tier-C entities below 60 enter mandatory remediation under NCIA supervision.

III. CONCEPTUAL ENHANCEMENTS AND META-DESIGN

BNRI must evolve as both statutory mechanism and dynamic analytical system; an instrument that learns, recalibrates, and anticipates. It is not a rigid index but a living computational framework that fuses policy, technology, and foresight into measurable resilience (Yang et al., 2024; Guo et al., 2021).

3.1 Computational Architecture and Model Governance

BNRI's analytical engine operates through a federated computational stack:

Layer	Function	Module
Data Ingestion	Validated audit telemetry, IoT feeds, incident logs	NCIA Secure Ingest Gateway (S-SIG)
Feature Store	Structured indicators (P, M, Ra, Rr)	BNRI Indicator Vault
Modelling Core	Anomaly detection, risk forecasting	Adaptive Resilience Model (ARM)
Explainability Layer	Interpretable results for policy review	Transparent Analytics Interface (TAI)
Policy Output Layer	Dashboards, alerts, governance actions	BNRI Decision Console

All AI/ML components operate under a Human-in-the-Loop protocol: model outputs require analyst confirmation before regulatory consequence. BNRI-AAC maintains an Algorithm Registry recording model versions, validation scores, and bias tests. Model drift is checked quarterly; explainability metrics are mandatory for high-impact decisions. This follows the OECD's trustworthy-AI-for-governance principle (OECD, 2025, Jun. 19).

3.2 Simulation and Stress-Testing Doctrine

BNRI institutionalises a **National Resilience Simulation Protocol (NRSP)** managed by NCIA. Scenario families: cyber-physical (OT/SCADA breach), supply-chain disruption, maritime and undersea failure, CBRN-e incident, and climate-induced infrastructure shock. Tier-A entities conduct bi-annual digital-twin stress-tests; Tier-B annual; Tier-C biennial. Each test yields three indices; containment latency, recovery efficiency, and adaptation gain. At least 25% of tests must be witnessed or replayed by accredited auditors. This mirrors CISA's emphasis on iterative, data-informed recovery planning (CISA, 2022, Aug.) and the UNDRR's Global Methodology for Infrastructure Resilience Review (UNDRR & CDRI, 2025, Apr. 24).

3.3 Compliance–Incentive Mechanism

BNRI embeds a dual-channel motivation model: a fiscal channel (Resilience Credits redeemable against licence fees or procurement preference) and a reputational channel (public publication of BNRI class status). This aligns with the OECD's finding that linking performance incentives to resilience outcomes enhances voluntary alignment with national security goals (OECD, 2025, Jun. 19).

BNRI Score	Oversight Cycle	Regulatory Posture	Fiscal/Market Instruments
< 60	Emergency; re-audit ≤ 6 months	Penalties; mandatory CAP	Ineligible for credits/procurement
60–84.9	Annual oversight	Standard regime; moderated penalties	Limited credits; conditional procurement
≥ 85	Biennial oversight	Relief and self-attest add-ons	Full credits; insurance/credit discounts; priority

3.4 National Resilience Data Grid (NRDG)

The NRDG functions as the nation's fusion layer; aggregating incident reports, audit telemetry, and simulation outputs from ministries and operators into a sovereign data backplane under NCIA. Data governance: classification (Public, Restricted, Secret) with retention periods; AES-256 encryption at rest and TLS 1.3 in transit; role-based access management with audit logs immutable for ten years; aggregate sectoral scores published annually while raw data remains protected. The NRDG also generates early-warning signals for systemic stress; automatic threshold alerts prompt NCIA and state cells to trigger corrective protocols.

Service KPIs: Ingestion Latency; Coverage %; Data Quality Index (DQI); Lineage Completeness; Availability/Uptime.

3.5 Temporal Adaptability

Temporal adaptability is codified through a mandatory Annual BNRI Review Conference co-hosted by NCIA and B.A.P-I. Incident after-action reports and international benchmarking feed indicator recalibration directly. A five-year Strategic Resilience Re-Baseline updates weights, thresholds, and sectoral coverage. Drift detection monitors indicator distributions and forecast residuals; model review includes backtesting and k-fold validation before weight updates; post-incident re-scoring is triggered by severity/impact thresholds. UNDP notes that resilience frameworks lose validity when they fail to evolve with emergent risks (UNDP India, 2023); BNRI makes evolution a statutory requirement.

3.6 International Reciprocity Clause

Cross-certification with UNDRR, ISO 22301/31000, and QUAD-aligned frameworks occurs through memoranda of understanding signed by NCIA. Each MoU specifies mutual recognition of audit methodology, data interchange protocols, and joint review frequency. Control-to-control mapping produces an **Equivalence Score** = mapped BNRI controls accepted abroad / total mapped controls. The derivation is detailed in Appendix A.

3.7 Analytical Consolidation

The five enhancements create a closed governance loop: computation renders resilience quantifiable; incentives lift performance beyond minima; data fusion supplies real-time evidence; temporal updates keep the model valid; reciprocity externalises credibility. Remove any one element and the system degrades: without computation, non-comparability; without incentives, plateaued compliance; without NRDG, blind spots; without recalibration, model drift; without reciprocity, trade and finance friction.

Policy sufficiency targets: Coverage ≥ 95% Tier-A assets scored quarterly, ≥ 85% Tier-B annually. DQI ≥ 0.9; Evidence Confidence Level ≥ 0.95 for Tier-A indicators. Re-score within T+30 days for severe incidents; annual model update published with Version ID. Equivalence Score ≥ 0.75 with at least two allied regimes in Year-1.

Computation-layer outputs: Data Completeness Index (DCI), Evidence Confidence Level (ECL), Weight Stability Coefficient, Tier-wise Score Variance, and Reproducibility Checksum for every published score.

IV. SCOPE AND PURVIEW; THE 6×4 OPERATIONAL DOMAIN MATRIX

BNRI's statutory coverage spans **six operational domains**, each assessed through **four cross-cutting measurement parameters**; forming a 6×4 matrix that constitutes the macro-level architecture of national resilience measurement. The twelve BAP-I cluster specifics (Section IX) provide granular sectoral classification within this framework.

The Four Cross-Cutting Measurement Parameters

- **Critical Dynamics and Resilience Parameters:** Threat modelling, vulnerability indexing, MTTR/MTTD benchmarks, redundancy ratios, cascade-exposure coefficients, and digital-twin stress-test results; the quantitative backbone of BNRI scoring.
- **Ecosystem Intelligence:** Real-time telemetry, anomaly detection, predictive analytics, inter-agency data fusion, OSINT integration, and early-warning signal generation; the foresight and situational-awareness layer.
- **National Resilience Data Grid:** Federated data architecture connecting Central Fusion Nodes, Sectoral Resilience Nodes, and State Resilience Cells under a sovereign data backplane managed by NCIA.
- **Ecosystem Resilience:** Adaptive capacity, post-disruption recovery intelligence, institutional learning loops, simulation-to-implementation conversion ratios, social resilience readiness, and transformative recovery capability.

4.A Critical Infrastructure

Energy grids, water and sanitation, transport (rail/road/port/aviation), communications and digital networks, finance and payments, health and emergency services, judicial/governance platforms, and digital infrastructure including data centres, SCADA systems, and AI command layers. Failure at a single Tier-A node propagates immediate cross-sector cascades; ICS/SCADA and core ICT stacks are simultaneously targetable, demanding fused cyber-physical governance (Dash, 2025, Jul. 1).

Mandatory baselines: OT/IT segmentation with unidirectional guards; MFA and patch SLAs; MTTR benchmarks codified per asset class; digital-twin stress drills; red-team cadence; 24-hour incident disclosure; immutable off-network backups. Redundancy ratios ≥ 2:1 for Tier-A utilities; service availability > 99.95%.

BAP-I Cluster Coverage: Cluster 1 (Critical Sectors) and Cluster 9 (Digital Revolution & Critical Automation).

4.B Strategic Manufacturing

Defence–aerospace corridors, semiconductor foundries, quantum research clusters, MEMS fabrication, nuclear assets, heavy and core industries, and the commercial-industrial complex. Disruption creates multi-year economic and capability gaps; cleanroom/precision fragility introduces single points of failure.

Mandatory baselines: Design-for-resilience; IP vaulting and export-control gates; supplier due diligence; cleanroom continuity; tamper-evident logistics; secure data rooms. Domestic sourcing ratio ≥ 60%; critical input redundancy ≥ 1.5×; validated continuity plans for Category-A plants.

BAP-I Cluster Coverage: Cluster 6 (Business Innovation) and Cluster 12 (Commercial-Industrial Complex).

4.C Supply Chain

National freight corridors, ports and airports, warehousing, cold-chain networks, border trade corridors, ICDs, intermodal terminals, and blue-water maritime infrastructure including undersea cable systems and port-inland logistics continua. Corridor or port outages magnify into nationwide stock-outs; temperature excursions destroy value and may endanger public health; trade and customs systems are software-defined chokepoints (OECD, 2024).

Mandatory baselines: End-to-end traceability (RFID/serialisation); temperature telemetry with alerts; reroute playbooks and stockpile policies; bonded-area security; API resilience; blockchain-verified cargo tracking for Tier-A corridors. Corridor uptime ≥ 95%.

BAP-I Cluster Coverage: Cluster 2 (Logistics & Supply Chain) and Cluster 3 (Blue-Water Infrastructure).

4.D Technology Sovereignty

The nexus of indigenous technological capability, research-to-resilience pipelines, and the knowledge infrastructure that underwrites long-term national self-reliance. Semiconductor ecosystems, quantum and MEMS fabrication, defence-grade R&D, AI/ML development pipelines, universities and national laboratories, and the entire

range of indigenisation and deep-tech autonomy. Disruption here weakens current capability and, more critically, future strategic agency (UNDP India, 2023).

Mandatory baselines: Knowledge retention and succession capacity under crisis; IP security and sovereign control of critical know-how; research continuity planning; secure-by-design certification for indigenous technology; dual-use governance safeguards; cybersecurity hardware and encryption stack indigenisation targets.

BAP-I Cluster Coverage: Cluster 4 (Research to Resilience) and Cluster 5 (Indigenisation & Technology Sovereignty).

4.E Comprehensive National Security

Internal security management, disaster dynamics and eco-protection, corporate governance and social security linkages, counter-terrorism, CBRN-e preparedness, hybrid-threat convergence, and continuity of governance. Not confined to external defence; it encompasses defence infrastructure resilience, defence manufacturing and supply chain security, the internal security apparatus, sectoral resilience, and the social contract: pensions, welfare, ESG-driven risk governance. Governance failure compounds every other domain (Dash, 2025, Jan. 30).

Mandatory baselines: Fusion intelligence and nationwide alerting; COOP exercises; CBRN-e detection; immutable backups for crown-jewel systems; failover communications (multi-bearer); annual joint disaster-cyber drills; 24×7 command audits; climate adaptation standards; governance transparency and continuity of social transfers.

BAP-I Cluster Coverage: Cluster 7 (Corporate Governance & Social Security), Cluster 10 (Disaster Dynamics & Eco-Protection), and Cluster 11 (Internal Security Management).

4.F Global Engagement and Collective Resilience

External economic posture, transnational supply chain resilience, overseas Indian enterprise continuity, international logistics capacity, diplomatic resilience of supply routes, multilateral framework alignment, and strategic investment diversification. Indian-controlled offshore assets, corporate presence abroad, and global value chain integration function as buffers, redirection channels, or surge networks in crisis, thereby extending resilience from a domestic construct into a transnational one.

Mandatory baselines: Exposure assessment to hostile jurisdictional interference; continuity arrangements with overseas partners; cross-border mutual aid protocols; alignment with UNDRR, ISO, QUAD, and allied frameworks; FDI/SEZ/EEZ governance; trusted-vendor certification; equivalence and mutual recognition agreements.

BAP-I Cluster Coverage: Cluster 8 (Global Partnership).

4.G The 6×4 Matrix; Integrated Summary

Domain	Critical Dynamics	Ecosystem Intelligence	National Resilience Data Grid	Ecosystem Resilience
Critical Infrastructure	MTTR, redundancy, cascade indices	SCADA telemetry, CERT feeds	Central Fusion Node, sectoral nodes	Recovery velocity, simulation conversion
Strategic Manufacturing	Yield continuity, IP breach rate	Supply chain intelligence	Industrial resilience node	Reconstitution capacity

Domain	Critical Dynamics	Ecosystem Intelligence	National Resilience Data Grid	Ecosystem Resilience
Supply Chain	Traceability %, reroute TTR	Predictive logistics analytics	Corridor monitoring, customs API	Rerouting agility, stockpile integrity
Technology Sovereignty	R&D continuity, indigenisation ratio	Horizon scanning, foresight cells	Knowledge retention data	Research succession, secure-by-design
National Security	COOP pass %, CBRN-e coverage	Fusion intelligence, OSINT	MHA/NDMA/CERT feeds	Social resilience, climate adaptation
Global Engagement	Cross-border exposure	Diplomatic risk intelligence	International data interchange	Mutual aid readiness, FDI resilience

Each cell produces measurable indicators that feed the BNRI computation layer, are scored against the ten foundational dimensions (Section VIII), contextualised through the seven India-specific perspectives (Section VIII-B), and disaggregated across the twelve BAP-I cluster specifics (Section IX).

V. BNRI CORE MEASUREMENT PILLARS

BNRI's measurement foundation rests on four interlinked pillars; Safety and Security Integrity, Operational Continuity and Redundancy, Compliance and Governance Assurance, and Systemic Interdependency and Adaptability. Each is independently auditable yet derives significance only through interaction with the others. The weighting; 30% + 25% + 25% + 20%; reflects empirical resilience-impact evidence (Yang et al., 2024; Guo et al., 2021) and the OECD's position that foundational protection and institutional compliance must together constitute at least half of any national-resilience scoring system (OECD, 2025, Jun. 19).

5.A Safety and Security Integrity (30%)

The protective baseline; measuring the ability of assets and systems to prevent, detect, and contain physical or cyber compromise within the same operational cycle (CISA, 2022, Aug.).

Dimension	Measurement Focus	Illustrative Metrics	Evidence Sources
Physical Protection	Barrier integrity, surveillance, intrusion response	Access-control uptime %, CCTV coverage %, response-force latency	Security audit logs, SOC records
Cyber Defence	Endpoint, network, OT/IT segmentation maturity	MFA compliance %, patch-window SLA %, red-team pass rate	CERT-In reports, internal audits
Integrated Access Control	Identity federation, credential isolation	Privilege escalation detection %, account rotation days	IAM telemetry, access logs

Benchmarks: Physical Intrusion Control Index (PICI) ≤ 0.05; Cyber Detection Latency (CDL) ≤ 15 min for Tier-A; Red-Team Audit Pass Rate (RAPR) ≥ 85%; MFA Coverage ≥ 98%. Safety Integrity Index (SII) ≥ 85 for Tier-A; < 70 triggers NCIA inspection.

5.B Operational Continuity and Redundancy (25%)

Quantifies the capacity of systems to sustain essential functions during disruption and restore normalcy within statutory thresholds (Petit & Verner, 2016, Oct. 2).

Dimension	Measurement Focus	Illustrative Metrics	Evidence Sources
Backup & Failover	Backup isolation, periodicity, test success	Backup integrity %, failover test pass %, MTTR (h)	DR logs, restore reports
Modularity & Resilience Design	Hot-swappable architecture, redundancy	Redundancy %, alternate routing %, critical spares index	Engineering schematics, inventory
Digital Twin & Simulation	Predictive failure modelling	Simulation frequency, scenario coverage %, validation accuracy	Simulation reports

Benchmarks: MTTR ≤ 48 h for Tier-A (≤ 4 h for critical substations); Redundancy Ratio ≥ 1.5×; Digital-Twin Test Frequency ≥ 2/year for Tier-A; Service Uptime Index ≥ 99.5%.

5.C Compliance and Governance Assurance (25%)

Institutional resilience is as decisive as engineering resilience. This pillar embeds governance quality, statutory adherence, and audit transparency into measurable parameters (OECD, 2024).

Dimension	Measurement Focus	Illustrative Metrics	Evidence Sources
Statutory Adherence	Compliance with CIPA schedules and BNRI directives	Audit score %, inspection compliance %, NC closure rate	NCIA audit records, RAB certificates
Audit Frequency & Transparency	External vs internal audit ratio, report publication	Audit cycle (days), disclosure timeliness, transparency index	Disclosure logs, compliance portals
Governance Integration	Board oversight, risk committee effectiveness	Committee meeting frequency, policy update lag	Board minutes, policy registers

Benchmarks: Audit Compliance Rate ≥ 95%; Unannounced Inspection Success ≥ 70%; Regulatory Response Latency ≤ 30 days; Transparency Score ≥ 90%. Every third audit cycle replicated by independent secondary RAB (inter-rater reliability ≥ 0.8). CAS ≥ 90 → regulatory relief; CAS < 60 → penalty band.

5.D Systemic Interdependency and Adaptability (20%)

Infrastructure does not fail in isolation; it fails in chains. This pillar measures adaptive cross-sector resilience and the capacity to absorb systemic stress (Guo et al., 2021; Rinaldi, Peerenboom & Kelly, 2001).

Dimension	Measurement Focus	Illustrative Metrics	Evidence Sources
Cross-Sector Resilience	Dependency modelling, mutual-aid protocols	Interdependency stress-test index, cascade latency (min)	NRDG analytics, stress-test outputs
Adaptive Governance	Foresight planning frequency, feedback integration	Adaptive planning rate %, post-incident policy update lag (days)	NCIA reviews, policy revision trackers
Learning Loops & Re-scoring	Use of AARs for model update	BNRI re-scoring cycle time, lesson-implementation rate %	After-action reports, re-scoring logs

Benchmarks: CSSI ≥ 2 exercises/year for Tier-A; Adaptive Planning Rate ≥ 80%; Inter-operability Audit Score ≥ 0.75; Learning-Loop Cycle Time ≤ 90 days.

5.E Composite Scoring Mechanism

For each operator *i*: **$BNRI_i = (0.30 \times S_1) + (0.25 \times S_2) + (0.25 \times S_3) + (0.20 \times S_4)$**. This yields operator-, sector-, and national-level indices published to the BNRI Grid dashboard and used for regulatory ranking and fiscal incentive allocation. Weights may be re-baselined every five years through the Annual BNRI Review Conference. The rationale for this weighting structure is set out in Appendix A.

Pillar	Symbol	Weight (%)	Primary Index Variables
Safety & Security Integrity	S_1	30	SII (MFA %, red-team rate, MTTD)
Operational Continuity & Redundancy	S_2	25	MTTR, redundancy %, digital-twin frequency
Compliance & Governance Assurance	S_3	25	CAS (audit score %, inspection rate)
Systemic Interdependency & Adaptability	S_4	20	ISTI, APR

VI. LEGAL AND INSTITUTIONAL EMBEDDING

The institutional legitimacy of BNRI depends on codification within a statutory regime. Embedding BNRI as Pillar-II of the Critical Infrastructure Protection Act (CIPA) situates it within India's emerging security legislation; alongside cyber-physical protection, disaster governance, and national continuity mandates (Dash, 2025, Jul. 1).

6.1 Statutory Basis; BNRI as Pillar-II of CIPA

Only statute can impose baseline parity across States, sectors, and private operators. Statutory chain-of-custody and data-lineage provisions make scores judicially defensible.

- **Schedule-II (Metrics and Methods):** Indicator catalogue, normalisation rules, model governance SOP.
- **Schedule-III (Sanctions and Incentives):** Penalty bands, Resilience Credits, procurement/FDI preferences.
- **Schedule-IV (Recalibration):** Annual and post-incident re-scoring; model versioning.
- **Schedule-V (Reciprocity):** Equivalence and mutual recognition with allied standards.

Mandatory publications: National Resilience Report (annual, tabled in Parliament), post-incident re-score bulletins, and NCIA directions.

6.2 Enforcement Authority; Institutional Roles

- **NCIA (apex):** Central rule-making, inspections, sanctions/relief, national dashboard.
- **BNRI-AAC:** Technical authority; accredits RABs, governs scoring models, administers appeals.
- **RAS:** Independent audit bureau; administers BNRI scoring, conducts scheduled and surprise audits, issues tiered certifications (Dash, 2025, Jan. 30).
- **Sector regulators:** Domain-specific checks (Power, Telecom, Finance, Health, Transport).

- **State Resilience Cells:** Federal data collection and joint inspections.
- **RABs:** Independent, licensed Resilience Audit Bodies; provide audits and evidence packs.
- **Prahari:** Dedicated multi-domain operational force for field-level protection and compliance verification (Dash, 2025, Dec. 25).
- **Operators:** Implement controls, report incidents, execute Corrective Action Plans (CAPs).

6.3 Penalty–Incentive Framework

BNRI Score Band	Oversight Cycle	Sanctions / Relief	Market Instruments
< 60 (Class-V/D)	Emergency; re-audit ≤ 6 months	Monetary penalties; suspension windows; CAP with milestones	Ineligible for govt procurement/credits
60–84.9 (Class-III/IV)	Annual oversight	Standard sanction regime; moderated penalties on improvement	Limited credits; conditional procurement
≥ 85 (Class-I/II)	Biennial oversight	Relief (select self-attestation); fewer routine inspections	Resilience Credits, insurance/loan discounts, procurement priority

6.4 Enforcement Lifecycle

Six sequential stages govern enforcement:

- **Step 1; Risk Signal/Trigger:** Audit finding, telemetry anomaly, incident, or complaint.
- **Step 2; Notice and Fact-Finding:** Joint NCIA/RAB/Regulator investigation.
- **Step 3; Corrective Action Plan (CAP):** Time-bound milestones with evidence requirements.
- **Step 4; Re-Audit and Verification:** Evidence packs; data-lineage check.
- **Step 5; Decision:** Sanction (penalty, suspension, publication) or Relief (reduced cadence, credits).
- **Step 6; Publication and Lessons:** BNRI re-score; model recalibration; public summary where non-sensitive.

6.5 Metrics, Assurance, and Due Process

- **Timeliness:** Time-to-Enforcement (TtE) ≤ 30 days from critical NC; Time-to-CAP Approval ≤ 10 days.
- **Quality:** RAB Quality Score (peer review, sampling errors, evidence defects); Appeal Reversal Rate ≤ 5%.
- **Coverage:** ≥ 95% Tier-A assets certified annually; ≥ 85% Tier-B.
- **Transparency:** Public grade summaries; protected technical annexures for sensitive assets.
- **Due process:** Right to respond; independent BNRI-AAC Appeals Board; judicial review under CIPA.

6.6 Interlocks with Other Law and Standards

- **Data and Cyber:** Harmonised with IT Act 2000 (amended 2008)/CERT-In directions, ISO/IEC 27001:2022.
- **Continuity and Safety:** Mapped to ISO 22301, Factories Act, Environmental Protection Act.
- **Disaster Governance:** Integrated with NDMA/DM Act 2005; Sendai alignment for international reporting.
- **Trade and Finance:** Public procurement rules and insurance/credit pricing policies recognise BNRI grades.

6.7 Analytical Consolidation

The legal backbone (CIPA + BNRI Pillar-II) creates coercive power; the institutional mesh (NCIA/BNRI-AAC/RAS/BIPCARD/Regulators/States/RABs/Prahari) delivers operational capacity; the penalty-incentive economy converts scores into behaviour. This triad constitutes a governance machine, not a checklist. RACI clarity reduces appeal reversal and audit latency, strengthening both deterrence and fairness.

VII. BNRI ECOSYSTEM: INSTITUTIONAL, FUNCTIONAL, AND STATUTORY DESIGN

BNRI is operationalised within the **Bharat National Resilience Ecosystem (BNRE)**; a doctrine positioning critical infrastructure protection and sectoral resilience as the third pillar of India's national security, alongside territorial defence and diplomatic security (Dash, 2025, Jan. 30).

7.1 The BNRE Institutional Architecture

Component	Full Name	Function
BIP-CARE	Bharat Infrastructure Protection & Critical Assets Resilience Enactment	Unified legislative foundation (CIPA)
BIP-CARP	Bharat Infrastructure Protection & Critical Assets Resilience Programme	Phased implementation framework
BIPCARD	Bharat Infrastructures Protection & Critical Assets Resilience Directorate	Apex governance body under the National Security Council
SOMA	Sectoral Operators, Managers, and Authorities	Mandatory multi-stakeholder coordination platform
RAS	Resilience Assessment & Synchronisation	Independent audit bureau administering the BNRI
Prahari	Dedicated Multi-Domain Operational Force	Field-level protection, cyber-physical rapid response, simulation exercises
BNRI	Bharat National Resilience Index	Twelve-domain measurement instrument with statutory consequences

Closed Governance Loop: BIPCARD sets standards → Prahari implements → RAS audits compliance and scores BNRI → findings feed back to BIPCARD for policy revision → SOMA coordinates all stakeholders around updated priorities (Dash, 2025, Jan. 30).

7.2 BIPCARD; Apex Governance Directorate

BIPCARD operates under the National Security Council with statutory jurisdiction across all twelve BAP-I strategic sectoral clusters. Five sub-structures:

- **Inter-Ministerial CIP Committee:** Cross-ministry policy alignment.
- **State CIP Coordination Cells:** Federal coherence and Centre-State interoperability.
- **Intelligence Fusion Centre:** Integrated threat feeds from RAW, IB, NTRO, CERT-In, and DIA.
- **Exclusive Zone Protection Directorates:** Defence, nuclear, maritime, SEZ, space, and border infrastructure.
- **Twelve BAP-I Sector Cluster Desks:** National standards translated into sector-specific compliance.

7.3 BNRI Grid; National Resilience Operating Network

- **Central Fusion Node:** Hosted by NCIA; integrates audit data, analytics, and live telemetry from Tier-A/B systems.
- **Sectoral Resilience Nodes:** Within each critical ministry; responsible for sector-level BNRI reporting.
- **State Resilience Cells:** Mirror nodes at state level for federal participation and decentralised accountability.
- **BNRI Data Lake:** Sovereign repository of audit records, incident reports, and simulation outputs.

7.4 BNRI Scale; National Measurement Framework

BNRI Class / Tier	Score Band	Designation	Meaning
Class-I / A+	90–100	National Gold Resilience Standard	Fully compliant; mentor institution
Class-II / A	75–89	Advanced Resilience Certified	High maturity; MTTR thresholds sustained
Class-III / B	60–74	Compliant & Functional	Statutory minima met; moderate redundancy
Class-IV / C	40–59	Conditional / Transitional	Improvement required; fragile interdependencies
Class-V / D	Below 40	Non-Compliant / High Risk	Critical deficits; mandatory audit and possible sanction

7.5 BNRI-AAC; Assessment and Accreditation Council

Statutory, autonomous body under CIPA; accredits RABs, certifies operators annually, administers appeals, publishes the annual National Resilience Index Report, and collaborates with B.A.P-I and technical institutions to evolve metrics, AI models, and audit protocols. Analogous to NABL or BIS but focused exclusively on resilience.

7.6 Class–Tier Regulatory Linkages

Class/Tier	Oversight Cycle	Audit Frequency	Penalty / Incentive
Class-I / A+	2-year re-certification	Annual self-audit + biennial NCIA review	Tax credit + govt contract eligibility
Class-II / A	1-year re-certification	Annual NCIA audit	Priority access to resilience grants
Class-III / B	Annual	NCIA + RAB joint audit	Standard compliance regime
Class-IV / C	6-month re-evaluation	Quarterly follow-ups	Penalty + mandatory capacity-building
Class-V / D	Immediate	Emergency oversight	Sanction + suspension if non-rectified

VIII. BNRI ASSESSMENT FRAMEWORK; TEN FOUNDATIONAL DIMENSIONS AND THE 10×7 MATRIX

The ten foundational dimensions constitute the analytical engine of BNRI. They derive from a two-stage methodology: Stage One applies ten deductive frameworks drawn from tested global CIP practices; Stage Two reinterprets them through seven India-specific governance perspectives, producing a **10×7 analytical matrix** with 70 intersections. Each represents a distinct assessment question (Dash, 2025).

8.A The Ten Dimensions; Global Best Practice Origins

No.	Dimension	Objective	Weight
1	Threat, Risk & Vulnerability Assessment (TRVA)	Identify, evaluate, and mitigate multi-domain threats. Dynamic threat modelling, real-time risk dashboards, red-teaming, predictive analytics.	12%
2	Zero-Tolerance Compliance	Mandatory adherence to statutory, technical, and operational standards. Inspection compliance, MTTR/MFA deadlines, legal accountability.	10%
3	Resilience-Centric Systems Engineering	Design-level embedding of resilience; modularity, redundancy, rapid recovery. Digital twins, MTTR compliance, adaptive modular design.	10%
4	All-Hazards Consequence Focus	Preparedness for any disruption class based on consequence severity. All-hazards plans, compound crisis simulations, multi-agency coordination.	10%
5	Defence-in-Depth Layered Security	Depth, redundancy, and integration of protection layers. Tiered access, red-teaming, AI anomaly detection, insider threat management.	10%
6	Public–Private Governance Integration	Collaboration between government, operators, and industry. PPP frameworks, joint drills, data exchange, CIPA-aligned corporate governance.	8%
7	Adaptive Risk Governance & Foresight	Anticipatory policy, data-driven foresight, institutional agility. AI/ML foresight, early warning, horizon scanning, cross-ministerial fusion.	10%
8	Integrated Supply Chain Security	Integrity, traceability, and continuity of logistics and manufacturing. Blockchain verification, supplier audits, contingency routing.	10%

No.	Dimension	Objective	Weight
9	Human Factors & Organisational Culture	Preparedness, skill, and resilience culture. Training frequency, crisis leadership, insider threat awareness, after-action reviews.	10%
10	Legal & Regulatory Harmonisation	Coherence among sectoral laws, state policies, and CIPA. Legal audit coverage, inter-ministerial harmonisation, NIST/ISO/UNDRR alignment.	10%

Composite Formula: BNRI_Score = Σ(Wi × Si) for i = 1 to 10. Derivation and weight justification in Appendix A.

8.B The Seven India-Specific Perspectives (10×7 Matrix)

The ten dimensions are reinterpreted through seven India-specific perspectives; interpretive filters that translate global logics into nationally relevant policy signals:

Perspective	Governance Dimension	India-Specific Application
1. Technological Priorities	Innovation-led modernisation	Predictive maintenance, AI-based monitoring, IoT integration
2. Cyber-Driven World Order	Digital infrastructure as sovereignty	CERT-defence integration; joint cyber crisis simulations
3. Economic & Business Technicalities	Fiscal incentives and resilience-linked growth	PPP-based scoring; catastrophe bonds; tax-linked incentives
4. Disaster Management	Multi-hazard preparedness	Hazard-neutral planning; decentralised crisis command
5. Legal & Statutory Provisions	Enforceability through statute	Mandatory operator resilience plans; centralised compliance audits
6. Socio-Political Governance	Coordination, legitimacy, institutional trust	Federal-state mechanisms; statutory CIP authority
7. National Security	Sovereignty and civil-military security	Joint exercises; foresight within defence doctrine

The 10×7 matrix yields 70 analytical intersections; structured exhaustiveness that prevents ad hoc assessment and eliminates blind spots in systematic review.

8.C BNRI Five Scoring Domains

Within the ten-dimension framework, the scoring methodology operates across five measurement domains; each weighted according to sector-cluster risk profiles (Ganin et al., 2016, Jan. 19; Popovski, 2023, Jul. 20):

Scoring Domain	What It Measures	Illustrative Indicators
1. Technical Redundancy	Hardware and systems resilience	Failover ratios, redundant node density, digital-twin coverage
2. Detection & Response Velocity	Speed of threat identification and containment	MTTD and MTTR against sector-specific baselines
3. Institutional Coordination	Multi-agency interoperability and governance coherence	Joint-exercise participation, inter-agency data-sharing compliance, escalation response times
4. Social Resilience Readiness	Community-level awareness, trust, continuity behaviours	Public risk-communication reach, community drill participation, trust indices
5. Adaptive Learning	Institutional capacity to learn from disruption	Post-incident audit completion rates, policy-revision cycles,

Scoring Domain	What It Measures	Illustrative Indicators
		simulation-to-implementation conversion ratios

Annual BNRI scores, disaggregated by sector cluster and by state, feed directly into Union Budget allocation decisions, linking fiscal resource flows to demonstrated resilience performance rather than expenditure volume (Dash, 2025, Jan. 30). The five scoring domains combine quantitative indices with qualitative assessments from simulation debriefs and post-incident audits, addressing the risk of reductionism (Moteff, 2012, Aug. 23; Theocharidou & Giannopoulos, 2015).

IX. SECTORAL INTEGRATION FRAMEWORK; TWELVE BAP-I CLUSTER SPECIFICS

The BAP-I twelve-cluster securitisation model organises India's infrastructure environment into operationally distinct domains that capture the country's evolving character, economic priorities, and multi-vector threat environment; moving well past the seven-sector NCIIPC designation (Dash, 2025; B.A.P-I, n.d.). Each cluster is assessed through all ten foundational dimensions and classified against the BNRI Scale (Class I–V).

Cluster	Name	Description
1	Critical Sectors	Energy, water, transport, health, finance, communication; immediate service lifelines
2	Logistics & Supply Chain	Ports, airports, freight corridors, cold chains; physical movement of commodities and materiel
3	Blue-Water Infrastructure	Maritime systems, undersea cables, naval logistics; trade access and strategic mobility
4	Research to Resilience	Universities, R&D hubs, labs; foresight and intellectual capital
5	Indigenisation & Tech Sovereignty	Defence, semiconductor, MEMS, quantum; fabrication sovereignty
6	Business Innovation	Start-ups, MSMEs, industrial corridors; distributed resilience and surge capacity
7	Corporate Governance & Social Security	ESG, pensions, welfare; stability within the social contract
8	Global Partnership	International logistics, overseas enterprises; transnational resilience buffers
9	Digital Revolution & Critical Automation	Data centres, SCADA, AI command; cyber-physical integrity
10	Disaster Dynamics & Eco-Protection	NDMA-linked systems; climate, seismic, ecological risk
11	Internal Security Management	Homeland, hybrid-threat domains; counter-terrorism, border security
12	Commercial-Industrial Complex (CCIIC)	Defence-industrial base fused with civilian manufacturing

X. CORE COMMERCIAL–INDUSTRIAL INFRASTRUCTURE COMPLEX (CCIIC)

The CCIIC is the integrated continuum of industrial, commercial, and manufacturing networks sustaining India's defence production, economic continuity, and employment security. It fuses the defence-industrial base with civilian manufacturing under one statutory resilience architecture.

Composition: Strategic manufacturing corridors; heavy and core industries; MSME and export networks; energy, mining, logistics, SEZs; business-critical utilities and financial systems. **Tier Classification:** Tier-A; national/transnational industrial systems; Tier-B; regional corridors and SEZs; Tier-C; local clusters supporting cumulative supply-chain resilience. **Regulatory Integration:** NCIA audit mandate; BNRI-AAC certification (Class I–V); BNRI Grid Industrial Resilience Node for telemetry; ratings tied to fiscal incentives, export credit, and FDI eligibility.

XI. IMPLEMENTATION AND GOVERNANCE DOCTRINE

11.1 National Dashboard

Real-time aggregated resilience scorecards visible to NCIA and state authorities. Pattern detection for emerging risks. Non-sensitive data displayed to citizens and industry via a BNRI Transparency Portal. Decision support directs funding, capacity-building, and emergency planning toward quantified resilience gaps.

11.2 Predictive Governance

Resilience forecasting using data from inspections, incidents, and simulations. The NRDG generates early-warning signals for systemic stress; automatic threshold alerts prompt corrective protocols. Continuous model recalibration keeps governance ahead of emerging risks.

11.3 Public Disclosure and Transparency

BNRI publishes resilience grades (A–E) for key operators through the Transparency Portal; creating reputational regulation that rewards preparedness and exposes neglect without new legislation. RAS's annual National Resilience Report Card, published for parliamentary scrutiny and public accountability, makes BNRI scores across all twelve BAP-I clusters a matter of public record (Dash, 2025, Jan. 30).

11.4 Parliamentary Oversight

Annual National Resilience Report tabled in Parliament; sector-wise rankings, trend analysis, and policy recommendations based on verified audit data. Resilience becomes an instrument of governance accountability.

11.5 International Standardisation

BNRI equivalence recognised by UNDRR, ISO 22301/31000, NATO infrastructure resilience principles, and QUAD-aligned frameworks. Cross-certification and mutual recognition enable India to participate in multilateral resilience diplomacy.

11.6 Implementation Checklist

Deliverable	Description	Owner
Legal text	BNRI statutory authority, inspection powers, penalties, incentives	NCIA / MHA
Data-sharing instruments	Standard BNRI Data-Sharing Agreement (central–state–operator)	NCIA
Accreditation schema	BNRI-AAC by-laws; RAB qualification and renewal criteria	BNRI-AAC
Measurement handbook	Indicator catalogue, evidence requirements, sampling rules, scoring rubrics	BNRI-AAC / RAS
Security posture	Data classification, anonymisation, redaction for national security	NCIA
Operational cadence	Annual certification, post-incident re-score, quarterly dashboards, Parliament report	NCIA / RAS

XII. THREE-TIER INTERLOCK ARCHITECTURE

BNRI's doctrinal and measurement power derives from the structured interaction of three interlocking matrices at three distinct levels.

12.1 Level 1; Macro: The 6×4 Operational Domain Matrix

Six operational domains define what BNRI covers; four cross-cutting parameters define how each domain is measured. This produces 24 macro-level measurement cells; the scope architecture of national resilience.

12.2 Level 2; Analytical: The 10×7 Framework Matrix

Ten foundational dimensions provide the deductive assessment methodology; seven India-specific perspectives provide interpretive contextualisation. This produces 70 analytical intersections; the assessment engine that generates scores.

12.3 Level 3; Sectoral: The 12 BAP-I Cluster Specifics

Twelve BAP-I clusters provide the granular sectoral classification. Each cluster sits within one of the six operational domains and is assessed through all ten dimensions.

12.4 Interaction Logic

- **Top-down:** The 6×4 matrix sets scope → the 10×7 matrix provides the analytical framework → the 12 clusters provide sectoral granularity.
- **Bottom-up:** Cluster-level audits → aggregate through 10 dimensions into domain-level scores → feed the 6×4 matrix to produce the national resilience dashboard.
- **Cross-cutting:** The four measurement parameters cut across all three levels; foresight, data fusion, and adaptive capacity are embedded at every granularity.

From BNRI as the doctrinal and measurement instrument, individual operational instruments derive their authority: sectoral-cluster resilience audits, individual sector compliance assessments, internal security and safety audits, operational continuity drills, and BNRI-linked procurement and fiscal eligibility; each drawing measurement

logic, scoring rubrics, and enforcement authority from this unified three-tier architecture.

Level	Matrix	Function	Output
1. Macro	6 Domains × 4 Parameters	Defines WHAT and HOW	24 measurement cells; national scope
2. Analytical	10 Dimensions × 7 Perspectives	Assessment engine	70 intersections; scored indicators
3. Sectoral	12 BAP-I Clusters	Granular classification	Cluster-level BNRI scores; sector audits

XIII. STRATEGIC VISION

Resilience has become the operative grammar of national power. Energy shocks, digital outages, and supply-chain fractures now influence geopolitical calculus as profoundly as conventional warfare. India's scale, economic momentum, and digital expansion make resilience not an adjunct but a precondition of sovereignty.

A National Resilience Index is therefore not an administrative innovation; it is a strategic necessity. It unites systems engineering with governance, compliance with foresight, and law with accountability. Through BNRI, India transitions from asset protection to functionality assurance, from crisis management to continuity mastery.

The BNRE's institutional triad; BIPCARD for governance, RAS for measurement, Prahari for operational force; transforms resilience into a quantifiable, auditable, and incentivised national capability. Every sector, from defence manufacturing to cold-chain logistics, operates under the same measurable covenant of resilience.

This framework positions India as the first developing nation to codify resilience as a legal and quantifiable state function; where compliance, safety, and continuity are auditable national capabilities, not policy artefacts. BNRI establishes India's indigenous capacity for resilience quantification, positioning the country as a standard-maker in resilience governance for the Global South (Dash, 2025, May 31; Dash, 2025, Jan. 30).

APPENDIX A: FORMULA DERIVATIONS, INDEX JUSTIFICATIONS, AND MEASUREMENT RATIONALE

A.1 The Resilience Function: Rc = f(P, M, Ra, Rr)

The resilience function derives from the Resilience Measurement Index framework developed by Argonne National Laboratory (Fisher et al., 2010; Argonne National Laboratory, 2013). It decomposes resilience into four operationally distinct phases; preparedness, mitigation, response, and recovery; each independently measurable yet jointly determinative of systemic continuity. This decomposition aligns with CISA's Infrastructure Resilience Planning Framework (CISA, 2022, Aug.), which structures resilience governance around the same four-phase cycle, and with the OECD's systemic risk metrics, which treat each phase as a weighted contributor to aggregate infrastructure performance (OECD, 2025, Jun. 19). The function is not additive but composite: the four parameters interact through feedback loops; preparedness quality affects response speed; mitigation depth determines recovery duration. The weighted geometric mean, rather than arithmetic summation, is used to prevent any single parameter from masking deficits in others.

A.2 The BNRI Computation Model: BNRI_Score = [Σ(Wi × Si^norm)] × K_comp × (1 − C_cascade) × C_crit

Base score [Σ(Wi × Si^norm)]: The weighted sum of normalised indicator scores across the ten BNRI dimensions provides the raw resilience assessment. Min–max normalisation (0–100) converts heterogeneous metrics into a common scale. Weights (Wi) are derived from empirical resilience-impact studies and calibrated through the Annual BNRI Review Conference (Yang et al., 2024; Guo et al., 2021).

Compliance gate (K_comp ∈ [0,1]): Operates as a multiplicative penalty on the base score. An operator that scores well on technical indicators but fails statutory obligations; overdue audits, late disclosures, critical non-conformances; cannot attain a high BNRI rating. K_comp is calculated as a decay function of compliance delinquency, ensuring that scores are earned against verifiable evidence rather than self-reported performance. This design prevents the score-gaming that undermines purely indicator-based indices (OECD, 2024).

Cascade-exposure penalty (C_cascade ∈ [0,1]): Derived from interdependency stress tests and digital-twin simulations, this modifier penalises operators whose failure would propagate disproportionately across sectors. It operationalises the system-of-systems principle: an operator serving a tightly coupled node faces a higher scoring threshold than one in a loosely coupled position. The Dependency-Interdependency Matrix developed in the CIP research programme (Dash, 2025; Rinaldi, Peerenboom & Kelly, 2001) provides the analytical substrate.

Criticality uplift (C_crit ≥ 1): Applied to Tier-A national lifelines, this modifier tightens scoring thresholds and amplifies identified deficits. A Tier-A power grid substation, for instance, faces stricter MTTR and redundancy requirements than a Tier-C local distribution node. C_crit values are set by NCIA under CIPA Schedule-II and reviewed annually.

A.3 Tiered Model: BNRI_Tiered = α(Tier A) + β(Tier B) + γ(Tier C)

The tiered aggregation model produces a weighted national resilience score from tier-level performance. The coefficients α, β, and γ (where α > β > γ) reflect the principle of proportional governance: Tier-A assets carry greater systemic significance and therefore greater weight in the national aggregate. This prevents a scenario where high Tier-C performance masks critical Tier-A deficits. The coefficient values are calibrated through the BNRI Review Conference and published under CIPA Schedule-II. The inequality constraint (α > β > γ) is structurally enforced: reclassification of an entity from Tier-C to Tier-A automatically increases its weight in the national score; creating an institutional incentive for accurate self-classification. Entry criteria (GVA ≥ 1%, population ≥ 10 lakh, dependency index ≥ 0.6, recovery sensitivity ≤ 48 h) are drawn from empirical studies on infrastructure criticality thresholds (Guo et al., 2021; Ouyang, 2014).

A.4 Composite Pillar Weights: 30% / 25% / 25% / 20%

The pillar weighting structure prioritises Safety and Security Integrity (30%) as the foundational risk-containment layer; reflecting empirical evidence that detection latency and access-control failures are the dominant initiators of cascade events (Rehak et al., 2020, May 12; CISA, 2022, Aug.). Operational Continuity (25%) and Compliance (25%) are equally weighted, reflecting the OECD's position that recovery capacity and governance assurance are co-equal determinants of sustained resilience (OECD, 2025, Jun. 19). Systemic Interdependency (20%) carries the lowest weight not because it is least important, but because it represents an emergent property. Measurable only through inter-sectoral interaction and therefore dependent on the prior three pillars being functional (Guo et al., 2021). Weights are re-baselined every five years through the Annual BNRI Review Conference.

A.5 Compliance Velocity Gain (CVG)

CVG measures the reduction in average audit-closure cycles attributable to BNRI's automation, tiered obligations, and integrated dashboards. It is calculated as: CVG = (T_baseline – T_bnri) / T_baseline × 100%, where T_baseline is the pre-BNRI average audit-closure time and T_bnri is the post-implementation average. The projected range is derived from comparative analysis of jurisdictions that have implemented tiered compliance regimes; notably the Basel framework in financial regulation and NIST's cyber-maturity model (OECD, 2024).

A.6 Predictive Governance Index (PGI)

PGI quantifies foresight accuracy as a ratio of predicted systemic stress events (identified through NRDG analytics and digital-twin simulations) to actual events within a defined period: PGI = Predicted_events_confirmed / Total_actual_events × 100%. Improvement in PGI over successive BNRI cycles indicates growing institutional capacity for anticipatory governance. The metric draws on the predictive analytics framework articulated in the UNDRR's Global Methodology for Infrastructure Resilience Review (UNDRR & CDRI, 2025, Apr. 24).

A.7 Global Equivalence Ratio (GER)

GER measures the degree to which BNRI controls map onto international resilience frameworks: GER = Controls_mapped_and_accepted / Total_BNRI_controls × 100%.

Control-to-control mapping is conducted against ISO/IEC 27001:2022, UNDRR Sendai Framework, EU NIS2 Directive, and Australia SOCI Act 2018. GER values are published annually under CIPA Schedule-V and inform mutual recognition negotiations.

A.8 Equivalence Score

Equivalence Score = BNRI controls accepted under foreign regime / Total mapped BNRI controls × 100%. This metric underpins the International Reciprocity Clause (Section 3.6) and is calculated through bilateral control-mapping exercises conducted by NCIA under signed MoUs.

APPENDIX B: REGISTER OF PROPOSED BODIES, ACTS, AUTHORITIES, INDEXES, AND INSTRUMENTS

This appendix catalogues every institutional body, legislative instrument, measurement index, operational platform, and governance mechanism proposed or referenced within the BNRI doctrinal framework. Each entry records the instrument's designation, institutional locus, statutory anchor, and primary function within the Bharat National Resilience Ecosystem.

B.1 Proposed Legislative Instruments

Instrument	Full Designation	Function	Statutory Anchor
CIPA	Critical Infrastructure Protection Act	Overarching statute for India's CIP regime; BNRI constitutes Pillar-II	Proposed under Union legislative competence
BIP-CARE	Bharat Infrastructure Protection & Critical Assets Resilience Enactment	Unified legislative foundation codifying sectoral roles, BIPCARD authority, compliance obligations	Primary enactment under CIPA
CIPA Schedule-II	Metrics and Methods	Indicator catalogue, normalisation rules, model governance SOP, scoring rubrics	Subsidiary instrument under CIPA
CIPA Schedule-III	Sanctions and Incentives	Penalty bands, Resilience Credits, procurement/FDI preferences	Subsidiary instrument under CIPA
CIPA Schedule-IV	Recalibration	Annual and post-incident re-scoring protocols; model versioning	Subsidiary instrument under CIPA
CIPA Schedule-V	Reciprocity	Equivalence and mutual recognition with allied international standards	Subsidiary instrument under CIPA

B.2 Proposed Governance Bodies and Authorities

Body	Full Designation	Institutional Locus	Function
NCIA	National Critical Infrastructure Authority	Apex enforcement body (proposed)	Rule-making, inspections, sanctions/relief, national dashboard
BIPCARD	Bharat Infrastructures Protection & Critical Assets Resilience Directorate	Under the National Security Council	Apex governance over cross-sector resilience standards, enforcement, inter-agency coordination
BNRI-AAC	BNRI Assessment & Accreditation Council	Autonomous under NCIA	Accredits RABs, governs scoring models, administers appeals, publishes annual report
RAS	Resilience Assessment & Synchronisation	Structurally independent of BIPCARD	Administers BNRI scoring across twelve domains, conducts audits, issues tiered certifications
SOMA	Sectoral Operators, Managers, and Authorities	Mandatory multi-stakeholder platform	Permanent coordination forum: operators, state managers, regulators, academia, intelligence

Body	Full Designation	Institutional Locus	Function
Prahari	Dedicated Multi-Domain Operational Force	Operational tier under BNRE	Field-level protection, cyber-physical rapid response, simulation exercises, compliance verification
RABs	Resilience Audit Bodies	Licensed under BNRI-AAC	Independent audits, evidence packs, field-level assessment
BNRI-AAC Appeals Board	Appeals and Review Board	Under BNRI-AAC	Independent review of contested assessments; judicial review under CIPA

B.3 Proposed Sub-Structures under BIPCARD

Sub-Structure	Function
Inter-Ministerial CIP Committee	Cross-ministry policy alignment for infrastructure protection
State CIP Coordination Cells	Federal coherence; Centre-State interoperability in data and inspections
Intelligence Fusion Centre	Integrated threat feeds from RAW, IB, NTRO, CERT-In, DIA into infrastructure-specific assessment
Exclusive Zone Protection Directorates	Defence, nuclear, maritime, SEZ, space, and border infrastructure governance
Twelve BAP-I Sector Cluster Desks	Translating national BNRI standards into sector-specific compliance requirements

B.4 Proposed Indexes, Metrics, and Scoring Instruments

Index / Metric	Abbreviation	Function	Reference Section
Bharat National Resilience Index	BNRI	Composite national resilience score (0–100); Class I–V certification	Sections I, V, VIII
Safety Integrity Index	SII	Weighted score of safety and security indicators per operator	Section V.A
Compliance Assurance Score	CAS	Compliance gate multiplier (K_comp) in BNRI computation	Section V.C
Enforcement Index	EI	Composite of inspection coverage, penalty realisation, disclosure timeliness	Section II.1
Learning Velocity Index	LVI	Ratio of closed recommendations to new findings per quarter	Section II.3
Compliance Velocity Gain	CVG	Reduction in audit-closure cycles post-BNRI implementation	Section II.5; Appendix A.5
Predictive Governance Index	PGI	Ratio of predicted stress events confirmed to actual events	Section II.5; Appendix A.6
Global Equivalence Ratio	GER	BNRI controls mapped and accepted under international frameworks	Section II.5; Appendix A.7
Equivalence Score	ES	BNRI controls accepted under specific foreign regime / total mapped	Section 3.6; Appendix A.8
Data Completeness Index	DCI	Completeness of data ingested into BNRI computation	Section 3.7
Evidence Confidence Level	ECL	Statistical confidence in evidentiary validation of indicators	Section 3.7

Index / Metric	Abbreviation	Function	Reference Section
Data Quality Index	DQI	Quality of data within the NRDG; target ≥ 0.9	Section 3.4
Physical Intrusion Control Index	PICI	Ratio of successful penetration tests to attempts; target ≤ 0.05	Section V.A
Cyber Detection Latency	CDL	Mean time from intrusion to alert; target ≤ 15 min for Tier-A	Section V.A
Red-Team Audit Pass Rate	RAPR	Percentage of red-team tests passed per cycle; target ≥ 85%	Section V.A
Cross-Sector Stress-Test Index	CSSI	Number of joint cross-sector exercises per year	Section V.D
Adaptive Planning Rate	APR	Percentage of policies updated post-incident; target ≥ 80%	Section V.D
Interdependency Stress-Test Index	ISTI	Quantified cross-sector vulnerability from stress tests	Section V.D
Weight Stability Coefficient	WSC	Stability of indicator weights across recalibration cycles	Section 3.7
Reproducibility Checksum	RC	Verification hash for every published BNRI score	Section 3.7

B.5 Proposed Programmes, Frameworks, and Platforms

Programme / Platform	Abbreviation	Function
Bharat National Resilience Ecosystem	BNRE	Overarching doctrine; seven interdependent components under closed governance loop
Bharat Infrastructure Protection & Critical Assets Resilience Programme	BIP-CARP	Phased implementation framework for CIPA rollout
National Resilience Simulation Protocol	NRSP	Codified simulation and stress-testing doctrine managed by NCIA
National Resilience Data Grid	NRDG	Federated sovereign data backplane; ingestion, analytics, early warning
BNRI Grid	N/A	Real-time federated digital infrastructure: Central Fusion Node, Sectoral Nodes, State Cells
BNRI Data Lake	N/A	Sovereign repository of audit records, incident reports, simulation outputs
BNRI Transparency Portal	N/A	Public-facing portal for resilience grades and non-sensitive data
NCIA Secure Ingest Gateway	S-SIG	Validated data ingestion from operators and RABs
BNRI Indicator Vault	N/A	Feature store converting raw data into structured P, M, Ra, Rr indicators
Adaptive Resilience Model	ARM	AI/ML modelling core for anomaly detection and risk forecasting
Transparent Analytics Interface	TAI	Explainability layer for policy-review-grade model outputs
BNRI Decision Console	N/A	Policy output layer: dashboards, alerts, governance actions
Algorithm Registry	N/A	BNRI-AAC register of model versions, validation scores, bias tests

Programme / Platform	Abbreviation	Function
Domain Mapping Register	N/A	NCIA register resolving overlap where entities span multiple domains
National Interdependency Map	NIM	Upstream/downstream linkage map across all six operational domains
BAP-I Twelve-Cluster Securitisation Model	N/A	Classification architecture organising India's infrastructure into twelve sectoral clusters

B.6 Proposed Reports and Publications

Publication	Frequency	Authority	Purpose
National Resilience Report	Annual	NCIA / RAS	Tabled in Parliament; sector-wise rankings, trend analysis, policy recommendations
National Resilience Report Card	Annual	RAS	Public scorecard across twelve BAP-I clusters for parliamentary scrutiny
Post-Incident Re-Score Bulletins	Event-driven	NCIA / RAS	Published after severity/impact threshold breaches; updated BNRI scores
NCIA Directions	As required	NCIA	Statutory directions under CIPA to operators and regulators
Resilience Insight Notes	Annual	B.A.P-I / BNRI-AAC	Peer-reviewed analytical briefs translating compliance patterns into policy signals
BNRI Scoring Handbook	Versioned	BNRI-AAC	Indicator catalogue, evidence requirements, sampling rules, scoring rubrics
Model Governance SOP	Versioned	BNRI-AAC	Algorithm Registry protocols, version control, validation procedures

B.7 Proposed Certifications, Credits, and Fiscal Instruments

Instrument	Function	Statutory Basis
BNRI Class/Tier Certification (I/A+ through V/D)	Tiered resilience grading for all covered operators	CIPA Schedule-II
Resilience Credits	Fiscal credits for operators scoring ≥ 85; redeemable against licence fees and procurement preference	CIPA Schedule-III
Equivalence Certification	Cross-border mutual audit recognition through control-to-control mapping	CIPA Schedule-V
Trusted-Vendor Certification	Cyber-resilience certification for supply chain vendors in government/PSU contracts	CIPA Schedule-III
Resilience-Linked Insurance	Insurance premium adjustments tied to BNRI Class/Tier grading	Market instrument; CIPA-enabled

Instrument	Function	Statutory Basis
Resilience-Linked Credit Pricing	Lending rate adjustments tied to demonstrated resilience performance	Market instrument; CIPA-enabled
Procurement Eligibility	Government/PSU procurement restricted to operators above defined BNRI thresholds	CIPA Schedule-III

FIGURES AND DIAGRAMS

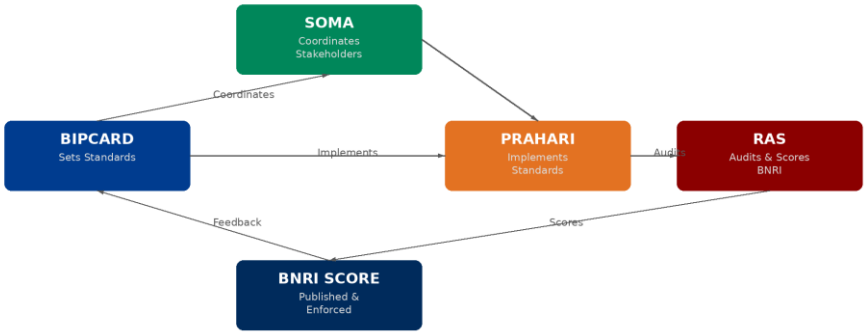

Figure 1. BNRE Closed Governance Loop

Figure 1. BNRE Closed Governance Loop: BIPCARD → Prahari → RAS → BNRI Score → BIPCARD (with SOMA coordinating all stakeholders)

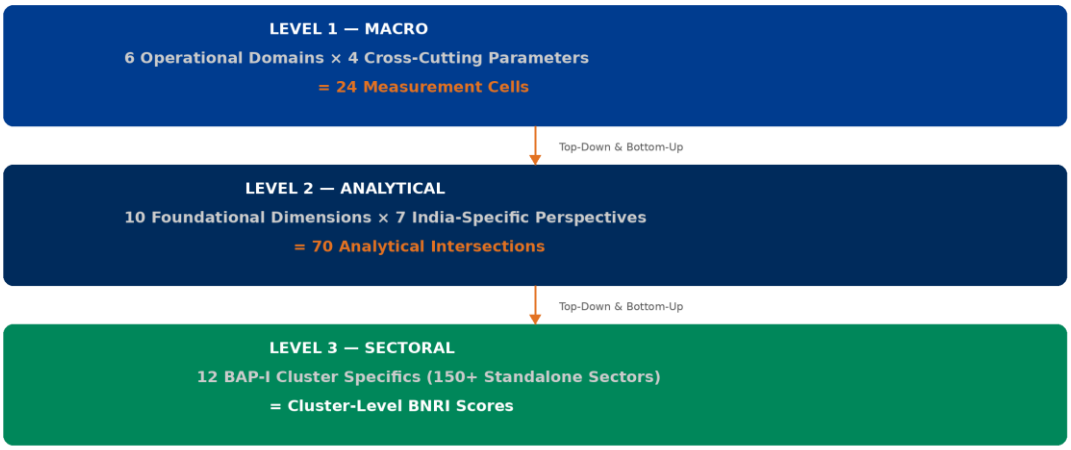

Figure 2. Three-Tier Interlock Architecture of the BNRI

Figure 2. Three-Tier Interlock Architecture: Macro (6×4) → Analytical (10×7) → Sectoral (12 Clusters)

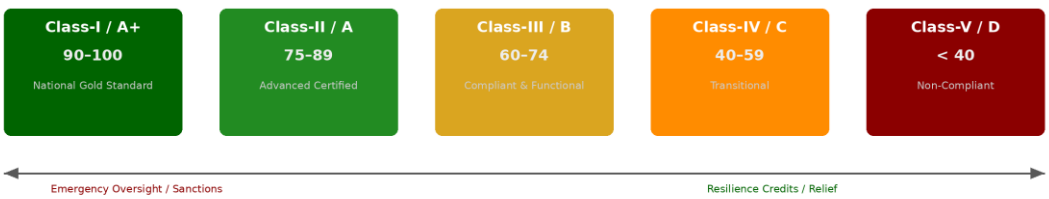

Figure 3. BNRI Scale — National Measurement Framework

Figure 3. BNRI Scale; National Measurement Framework (Class I/A+ through Class V/D)

REFERENCES

Argonne National Laboratory (2013). Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. US Department of Energy.

B.A.P-I (n.d.). BAP-I Twelve-Cluster Securitisation Model. Bharat Assets Protection Institute.

Bach, C., Bouchon, S., Fekete, A., Birkmann, J. & Serre, D. (2013). Adding Value to Critical Infrastructure Research and Disaster Risk Management. International Journal of Disaster Risk Science.

CERT-In (2025). Directives on Information Security Practices for Government, Critical Sector, and Protected System Organisations. Ministry of Electronics and Information Technology, Government of India.

Chester, M., Underwood, B.S., Allenby, B., Garcia, M., Samaras, C., Markolf, S., Sanders, K., Preston, B. & Miller, C.A. (2021, Feb. 23). Infrastructure Resilience to Navigate Turbulence and Uncertainty. Proceedings of the National Academy of Sciences.

Chowdhury, N. & Gkioulos, V. (2021, Mar. 11). Key Competencies for Critical Infrastructure Cyber-Security. Information and Computer Security.

CISA (2022, Aug.). Infrastructure Resilience Planning Framework (IRPF). Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security.

Dash, P. (2025, May 31). Proposing the Bharat National Resilience Index (BNRI): Building Secure and Continuity-Ready Infrastructure for India. Bharat Assets Protection Institute.

Dash, P. (2025, Jul. 1). Legislating Resilience: Why India Needs a Critical Infrastructure Protection Act for the Cyber-Physical Age. Bharat Assets Protection Institute.

Dash, P. (2025, Jan. 30). Bharat National Resilience Ecosystem: Legislative Orientation Paper. Bharat Assets Protection Institute.

Dash, P. (2025, Dec. 25). Prahari: A Dedicated Multi-Domain Force Framework for Critical Infrastructure Protection. Bharat Assets Protection Institute.

Dash, P. (2025). Exploring the Best Practices for Critical Infrastructure Protection Programme in India. Post-Doctoral Research Design Framework. Unpublished.

Fisher, R.E., Bassett, G.W., Buehring, W.A., Collins, M.J., Dickinson, D.C., Eaton, L.K., Haffenden, R.A., Hussar, N.E., Klett, M.S., Lawlor, M.A., Miller, D.J., Petit, F.D., Peyton, S.M., Wallace, K.E., Whitfield, R.G. & Peerenboom, J.P. (2010). Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program. Argonne National Laboratory, ANL/DIS-10-9.

Ganin, A.A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J.M., Kott, A., Mangoubi, R. & Linkov, I. (2016, Jan. 19). Operational Resilience: Concepts, Design and Analysis. Scientific Reports, 6, 19540.

Guo, Y., Fu, G., Wilkinson, S. & Meng, F. (2021). A Review of Resilience Assessment and Recovery Strategies for Interdependent Infrastructure Systems. International Journal of Critical Infrastructure Protection.

Moteff, J.D. (2012, Aug. 23). Critical Infrastructures: Background, Policy, and Implementation. Congressional Research Service, RL30153.

OECD (2024). Compendium of Good Practices on Quality Infrastructure. OECD Publishing.

OECD (2025, Jun. 19). Systemic Risk Governance in Critical Infrastructure. OECD Publishing.

Ouyang, M. (2014). Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. Reliability Engineering and System Safety, 121, 43–60.

Petit, F.D. & Verner, D. (2016, Oct. 2). Resilience Assessment and Measurement. In Critical Infrastructure Protection and Risk Management. J. Ross Publishing.

Popovski, V. (2023, Jul. 20). Operationalising Resilience in Critical Infrastructure. Journal of Infrastructure Policy.

Rehak, D., Senovsky, P., Hromada, M. & Lovecek, T. (2020, May 12). Failures of Critical Infrastructure Elements. Sustainability, 12(10), 4019.

Rinaldi, S.M., Peerenboom, J.P. & Kelly, T.J. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine, 21(6), 11–25.

Theocharidou, M. & Giannopoulos, G. (2015). Risk Assessment Methodologies for Critical Infrastructure Protection. European Commission Joint Research Centre.

UNDP India (2023). Building Resilient Governance: Institutional Continuity and National Preparedness. United Nations Development Programme.

UNDRR (2023, Mar. 30). Principles for Resilient Infrastructure. United Nations Office for Disaster Risk Reduction.

UNDRR & CDRI (2025, Apr. 24). Global Methodology for Infrastructure Resilience Review. United Nations Office for Disaster Risk Reduction.

Yang, Y., Xu, K., Langseth, H. & Weber, P. (2024). A Unified Framework for Evaluating Resilience of Critical Infrastructure. Reliability Engineering and System Safety.

AUTHOR'S NOTE AND INTELLECTUAL PROPERTY DISCLAIMER

The concept of the Bharat National Resilience Index (BNRI), including its structure, methodology, analytical framework, and the wider Bharat National Resilience Ecosystem (BNRE) comprising BIP-CARE, BIP-CARP, BIPCARD, SOMA, RAS, Prahari, and the BNRI measurement instrument, is an original intellectual formulation conceived and developed by the author, Dr. Padmalochan Dash. Any reproduction, adaptation, or citation; whether in part or whole; must provide proper academic and institutional attribution to the author. Unauthorised use, redistribution, or derivative work without explicit citation or consent constitutes a violation of intellectual property rights under applicable academic and copyright standards.

AI Disclosure Statement

Artificial intelligence tools were used in a strictly limited capacity during the preparation of this document; confined to the organisation of qualitative material, preliminary structuring, and formatting assistance. No AI tool performed analysis, interpretation, synthesis, or content generation. All substantive reasoning, critical argumentation, doctrinal formulation, and scholarly judgement underpinning this work are entirely the author's own.