Digital Bharat Cumulative Cyber Governance Index: Integrating Telemetry, Governance, and Adversarial Assessment Metrics

Nazmeen Ansari
Management
Matrix3D Infocom Private Ltd
Mumbai, India
nazmeen.ansari@matrix3d.com

Parvez Diwan
Management
Matrix3D Infocom Private Ltd
Mumbai, India
parvez.diwan@matrix3d.com

Abstract: *Unified cyber risk reporting remains elusive within large enterprises. Existing practices separate technical security metrics from governance and compliance indicators. The Digital Bharat Cumulative Cyber Governance Index (DB-CCGI) is introduced as a composite corporate security posture index integrating technical telemetry metrics and compliance/governance metrics, reinforced with adversarial validation. Unlike frameworks that address technical controls or compliance independently, DB-CCGI provides a single numerical index on a 1-10 scale that ensures neither strong technical defences nor robust compliance alone can mask weaknesses in the other. The methodology defines five dimensions: Technical Exposure & Control Effectiveness (TECE), Governance, Compliance & Cyber Response Readiness (GCCR), Data Protection & DPDP Assurance (DPDA), Detection, Resilience & Control Validation (DRCV), and AI & Emerging Tech Governance (AETG) with representative metrics drawn from SIEM, IAM, GRC systems, and red-team testing results. Each metric is normalised and aggregated via a geometric mean model with floor constraints to derive the composite score, preserving balance between technical and governance pillars. A hypothetical case study demonstrates DB-CCGI scoring for two contrasting organisational profiles, highlighting how balanced improvement yields a higher index than siloed strength. DB-CCGI is evaluated against NIST CSF 2.0, MITRE ATT&CK, cyber maturity models, and commercial cyber risk indices, illustrating its novelty as an India-specific operational synthesis. The paper discusses future-proofing the framework for evolving AI governance and regulatory changes, and outlines limitations and next steps toward empirical validation.*

Keywords-*cybersecurity metrics, compliance index, security governance, composite index, risk posture, red-team validation, CERT-In, DPDP Act.*

I. Introduction

Modern enterprises struggle to obtain a unified view of cybersecurity posture across technical defences and governance practices. The NIST Cybersecurity Framework (CSF) 2.0, released on 26 February 2024, emphasises integrating governance into cyber risk management by introducing a new *Govern* function that highlights the importance of governance and supply chains [1] but does not prescribe a single quantitative index. Adversary-centric tools like MITRE ATT&CK provide rich coverage of threats and techniques, yet focus purely on technical detection coverage rather than compliance or governance [2]. Cyber maturity models (e.g., CMMC for defence contractors [4]) assign qualitative levels to processes and controls but lack a dynamic score integrating real-time telemetry. Security Operations Centre (SOC) and Governance, Risk & Compliance (GRC) teams continue to report on separate dashboards, making it difficult for executives or boards to reconcile these streams into one risk narrative.

This gap is especially acute in India, where regulatory mandates amplify the need for integrated metrics. The Indian Computer Emergency Response Team (CERT-In), under Directive No. 20(3)/2022-CERT-In dated 28 April 2022, requires covered entities such as service providers, intermediaries, data centres, body corporates, and government organisations to mandatorily report cyber incidents within 6 hours of noticing them. The same Directions require synchronisation of ICT system clocks with designated reference time sources and maintenance of ICT system logs for a rolling period of 180 days [5], pushing enterprises to bolster both technical detection and compliance infrastructure. The Digital Personal Data Protection (DPDP) Act, 2023 (Act No. 22 of 2023, gazetted 11 August 2023) [6] imposes strict consent and data-handling obligations, bringing legal compliance failures directly into the realm of cybersecurity risk. These developments demand a unified approach that treats technical controls and governance controls as two sides of the same coin.

In this paper, we propose the Digital Bharat Cumulative Cyber Governance Index (DB-CCGI) as a composite cyber governance and security posture index tailored to these needs. The core idea is a cumulative posture model in which technical and compliance contributions are aggregated into a single score that penalises imbalances: strong technical posture cannot fully compensate for governance weaknesses, and vice versa. DB-CCGI is designed with five dimensions to comprehensively span Indian corporate requirements in 2026:

(1) Technical Exposure & Control Effectiveness (TECE),
(2) Governance, Compliance & Cyber Response Readiness (GCCR),
(3) Data Protection & DPDP Assurance (DPDA),
(4) Detection, Resilience & Control Validation (DRCV)
(5) AI & Emerging Tech Governance (AETG).

Each dimension is quantified by specific metrics drawn from operational data (SIEM, EDR/XDR, IAM/PAM, NDR, cloud logs, GRC systems) and red-team reports. The index unifies these metrics via a geometric mean-based scoring formula with floor constraints that ensure a low score in any critical dimension drags down the composite index.

The rest of this paper is structured as follows: Section II reviews related frameworks and indices to position DB-CCGI's novelty. Section III details the methodology, including metric selection, normalisation, and the composite score computation with adversarial assessment integration. Section IV presents an evaluation through a hypothetical case

study. Section V discusses practical implications, future-proofing, and comparisons. Section VI outlines limitations and future work. Section VII concludes the paper.

II. Related Work

A. Cybersecurity Frameworks

The NIST CSF, first released in 2014 and updated to version 2.0 (CSWP 29) on 26 February 2024 [1], provides a widely adopted taxonomy of high-level cybersecurity outcomes. CSF 2.0 is designed to help organisations of all sizes and sectors manage and reduce cybersecurity risks and organises outcomes into Functions, Categories, and Subcategories that can be understood by executives, managers, and practitioners regardless of their cybersecurity expertise. Version 2.0 notably highlights the importance of governance and supply chains by adding the Govern function. However, the CSF does not prescribe how outcomes should be achieved, and it produces qualitative implementation tiers and organisational profiles rather than a unified numeric score.

MITRE ATT&CK is a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) based on real-world observations of cybersecurity threats [2]. ATT&CK was initiated in 2013 to document and categorise post-compromise adversary TTPs against Microsoft Windows systems and has since expanded to cover the Enterprise, Mobile, and ICS domains. According to a 2020 survey conducted by McAfee and the University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC) among security leaders across 325 large- and medium-sized enterprises in the UK, US, and Australia, more than 80% of enterprises use MITRE ATT&CK for threat protection, 57% use it to identify gaps in deployed security solutions, 55% recommend it for security policy implementation, and 54% use it for threat modelling [3]. ATT&CK is purely technical; it maps defensive coverage to known threats and does not incorporate compliance or maturity dimensions.

B. Cyber Maturity Models

Cyber maturity models such as the Cybersecurity Maturity Model Certification (CMMC) (Model Overview v2.0, December 2021) focus on organisational processes and control maturity for US Department of Defense (DoD) contractors and subcontractors. These models yield categorical maturity levels rather than a granular numeric index, and they emphasise audit certification rather than continuous posture tracking.

C. Composite Cyber Risk and Governance Indices

At the national level, the ITU Global Cybersecurity Index (GCI) is a composite indicator combining legal, technical, capacity-building, and cooperation measures to rank countries' cybersecurity commitments [7]. However, GCI operates at a macro scale and is not directly applicable to individual enterprise operations.

In academia, Bolpagni (2021) proposed a socio-technical Cyber Risk Index combining threat prevalence and readiness at a country scale [8]. The aim of that paper is to propose a composite index for assessing cyber risk and to investigate which socio-economic factors influence the index itself. Bolpagni used the Mazziotta-Pareto Index (MPI), which employs a non-linear function obtained from an arithmetic mean with penalty to give a synthetic measurement of a set of normalised indicators assumed to be not fully substitutable. This non-substitutability principle resonates with DB-CCGI's philosophy: governance cannot be completely substituted by technical controls, necessitating a careful aggregation formula.

Georgiadou, Mouzakitis, and Askounis (2021) presented a cyber-security culture framework with ten dimensions spanning organisational factors (Assets, Continuity, Access and Trust, Operations, Boundary Defense, Security Governance) and individual factors (Attitude, Awareness, Behaviour, Competency) [3], and mapped these to MITRE ATT&CK mitigations. Their work demonstrated the value of bridging cultural/human factors with technical threat assessment, a multi-dimensional approach that informs DB-CCGI's design, though DB-CCGI focuses on operational metrics rather than cultural assessment.

D. Commercial Risk Scoring Solutions

Trend Micro's Cyber Risk Index (CRI) provides a continuous, dynamic, real-time measurement of organisational cyber risk [9]. Powered by Trend Vision One™, the platform integrates telemetry from vulnerabilities, exposures, misconfigurations, and threat intelligence to calculate asset-level risk scores and an overall organisational index. These scores are derived from a weighted analysis of over 2,300 risk events, structured across three key categories: attack activity, exposure conditions, and security configuration. Each risk score reflects the geometric mean of likelihood and impact, with impact determined by the CIA triad (Confidentiality, Integrity, Availability) and asset criticality. The report positions the CRI as a cybersecurity KPI enabling operational prioritisation, proactive governance, benchmarking against industry peers, and support for zero-trust initiatives. DB-CCGI draws inspiration from this approach but differentiates itself by explicitly balancing technical telemetry with regulatory compliance evidence and by including red-team adversarial testing as a gating factor for score improvement.

E. Comparison of Frameworks

Table I summarises how DB-CCGI relates to these established frameworks and indices.

TABLE I. COMPARISON OF DB-CCGI WITH EXISTING FRAMEWORKS

Framework	Scope	Combines Technical & Governance?	Adversarial Testing Integration?	Output
DB-CCGI (proposed)	Corporate security & compliance posture, India-specific (DPDP Act, CERT-In mandates)	Yes: technical pillar + governance pillar across five dimensions on a 1–10 scale	Yes: adversarial assessment as validation overlay with defined metrics (AADR, ACGR, AGFR)	Single composite numeric index (1-10) plus dimension radar
NIST CSF 2.0 (Feb 2024) [1]	Cyber risk management across six Functions including Govern; targets all organisations regardless of size, sector, or maturity	Partially: Govern function addresses governance; CSF does not prescribe outcomes but links to resources	No explicit threat scoring	Qualitative tiers and organisational profiles; no single numeric score
MITRE ATT&CK [2]	Knowledge base of adversary tactics and techniques; used by >80% of large enterprises for threat protection	No: exclusively technical/operational (attacker behaviours, detection coverage)	Yes: entirely adversary-centric; 57% of surveyed enterprises use it to identify gaps	Coverage metrics (% techniques detected); no unified risk score
CMMC v2.0 (Dec 2021) [4]	Cybersecurity posture of US DoD contractors and subcontractors	Partially: covers process and control maturity including some governance	Indirectly: advanced levels may require testing	Categorical maturity levels; not a composite numeric score
Trend Micro CRI [9]	Corporate cyber risk scoring via XDR telemetry and threat intelligence	Partially: includes security configuration (governance-adjacent) but not regulatory compliance specifically	Yes: incorporates attack activity and threat detection data	Continuous numeric score derived from geometric mean of likelihood and impact across 2,300+ risk events
ITU GCI [7]	Country-level composite index measuring national cybersecurity commitment	Yes (country level): legal, technical, organisational, capacity, and cooperation measures	No direct adversarial testing	Composite country-level score; not designed for individual enterprises

In summary, to the best of our knowledge, no existing framework combines these elements into a single quantitative index that equally incorporates technical security telemetry, governance and compliance adherence, and adversarial resilience at the corporate level within an India-specific regulatory context. DB-CCGI's novelty lies in synthesising these elements into a unified metric.

III. Methodology: DB-CCGI Index Design

A. Overview and Design Principles

DB-CCGI is conceptualised as a composite security governance posture index, not a probabilistic risk model, that merges technical and governance performance into a single quantitative measure. The design follows three guiding principles:

In DB-CCGI, metrics are first grouped into five dimensions, each representing a distinct area of cyber posture. These dimensions are then grouped into two broader pillars: a technical pillar, comprising TECE and DRCV, and a governance pillar, comprising GCCR, DPDA, and AETG. The dimensions provide diagnostic granularity, while the pillars provide the higher-level structure used to compute the final composite score.

1) **Comprehensive Dimensions:** DB-CCGI spans five dimensions that span the full spectrum of cyber risk relevant in an Indian enterprise. Each dimension is measured by specific metrics derived from operational data sources.
2) **Balanced Pillars:** Technical security, and governance and compliance are equally critical for any organisation. Improvements in one pillar cannot fully offset deficiencies in the other.
3) **Empirical Scoring and Normalisation:** All metrics are quantitatively defined and normalised to a common 1-10 scale, ensuring comparable outputs across diverse inputs.

B. Architecture Description

The DB-CCGI architecture operates in a data pipeline with the following stages:

Input Layer: Data is collected from three streams (i) Telemetry data from security tools (SIEM, EDR/XDR, IAM/PAM, NDR, cloud logs), (ii) Governance data from GRC platforms, audit records, consent management systems, and regulatory compliance databases covering CERT-In readiness, incident reporting timelines, log retention practices, and the DPDP Act, and (iii) Adversarial assessment data from red-team reports, penetration testing, and Breach and Attack Simulation (BAS) outputs.

Normalisation Layer: Raw metric values from each input stream are converted to 1-10 scores using defined scoring functions (linear, piecewise linear, or threshold-based, depending on the metric).

Dimension Scoring Layer: Normalised metric scores are averaged within each of the five dimensions (TECE, GCCR, DPDA, DRCV, AETG) to produce dimension-level scores.

Adversarial Adjustment Layer: Red-team and BAS results are applied as validation overlays to the relevant dimension scores where controls fail under realistic attack conditions.

Pillar Aggregation Layer: The adversarially adjusted dimension scores are combined into a technical pillar (C) and a governance pillar (G).

Composite Index Layer: The final DB-CCGI score is computed via a constrained geometric mean of C and G, after which any governance floor cap is applied.

C. Dimensions and Metrics Identification

Table II describes the five DB-CCGI dimensions and provides representative metrics for each, including definitions, data sources, scoring approaches, and rationale. These dimensions and metrics were identified through analysis of industry standards (NIST CSF [1], CERT-In Directive of 28 April 2022 [5], DPDP Act 2023 [6] and common security KPIs in Indian enterprises.

Normalisation: Each metric's raw value is mapped to a score from 1 (worst) to 10 (best). For "higher is better" metrics (e.g., percentage of incidents detected within threshold), a linear or piecewise linear scaling assigns 10 to the defined target. For "lower is better" metrics (e.g., average incident response time), scores are inverted against benchmarks. To ensure consistency, each metric's scaling function is defined in a clear manner to ensure reproducibility.

Aggregation to Dimension Score: A dimension level score is generated by averaging of multiple metrics inside each dimension. Equal weights are used in the initial specification; explicit weighting might be applied where actual data suggests differences.

TABLE II. DB-CCGI DIMENSIONS AND REPRESENTATIVE METRICS

Dimension	Representative Metric	Data Source	Scoring Approach (1-10)	Rationale
1. TECE (Technical) S1	Privileged Access Governance score measures unpredictability and minimisation of highly privileged account use patterns over time.	PAM/IAM logs; UEBA analytics	If privileged access is limited to approved accounts, time-bound where applicable, and anomalous or excessive use remains below predefined thresholds, the score is 10; lower scores apply where privileged access is broad, persistent, or weakly monitored.	Indicates tight control over privileged accounts; Controlled, least-privilege, and well-monitored privileged access reduces misuse and escalation risk.
	API Shadow IT Exposure counts unmanaged or unreported APIs accessible externally.	App inventory; network scans	Score 10 if no unknown/unapproved APIs; decreases as count rises (scoring tiers based on risk criticality).	Unmanaged APIs increase attack surface; measuring and minimising them improves security posture.
2. GCCR (Governance) S2	Cyber Incident Governance Readiness: degree to which the organisation can execute documented incident classification, escalation, decision-making, regulatory reporting, stakeholder notification, and evidence preservation workflows within mandated or policy-defined timelines.	Incident management system; tabletop and drill records; escalation matrices; regulatory reporting workflows; evidence retention records	Score 10 if incident governance workflows are documented, assigned, tested, and consistently executed within required timelines across drills or real incidents; lower scores apply where escalation paths are unclear, reporting readiness is partial, or evidence preservation is inconsistent.	Measures whether the organisation can govern a material cyber incident in practice, not merely document compliance obligations
	Remediation and Governance Follow-Through Rate: percentage of incident findings, drill observations, audit issues, and adversarial assessment outputs that are converted into assigned, tracked, and timely closed remediation actions with auditable evidence	GRC platform; risk register; remediation trackers; internal audit records; post-incident review record	If the large majority of governance, incident, and adversarial findings are assigned, tracked, and closed within approved timelines with evidence of closure then you may score 10; lower scores apply where actions are overdue, weakly owned, or poorly evidenced.	Ensures that governance is evidenced through closure discipline and accountability, rather than limited to policy statements or reporting intent.
3. DPDA (Governance) S3	Consent Artefact Verifiability: proportion of user consent records verifiable and audit ready.	Consent management system; immutable database logs	If 100% of consents stored with immutable ledger enabling audit helps achieve a score of 10; partial deployment yields lower scores.	Verifiable consent records are a DPDP Act complaint, demonstrating lawful processing of personal data.
	Data Principal Request Latency: average time to fulfil user data access/correction/erasure requests.	Privacy request ticketing system; workflow records	A score of 10 can be awarded if the average latency is within DPDP-stipulated timeframe; 5 if moderately delayed; 1 if largely non-compliant.	Indicates organisation's agility in upholding data subject rights.
4. DRCV (Technical) S4	Detection Coverage Rate: proportion of critical attack paths, assets, identities, workloads, and control points for which reliable detection logic and telemetry coverage are in place.	SIEM/XDR detection catalogues; telemetry coverage reports; detection engineering records	Detection coverage should be implemented and validated across nearly all defined critical attack paths and asset classes to get a score of 10; lower scores apply where major gaps in telemetry or detection logic remain.	Measures whether the organisation has meaningful technical visibility across the attack surface rather than isolated monitoring depth.
	Continuous Control Validation Coverage: extent to which	BAS reports; security validation	Score 10 if more than 90% of critical controls are continuously	Ensures that technical controls are not assumed to work merely

Dimension	Representative Metric	Data Source	Scoring Approach (1-10)	Rationale
	critical preventive, detective, and hardening controls are continuously validated through BAS, attack simulation, configuration assurance, or equivalent technical testing.	platforms; configuration assurance logs; security testing records.	or regularly validated through automated or repeatable testing; lower scores apply where validation is partial, infrequent, or manual.	because they are deployed, but are repeatedly validated under changing conditions
5. AETG (Governance & Technical) S5	Algorithmic Bias Audit Coverage: proportion of deployed AI/ML models with completed bias and fairness audits.	AI governance logs; audit reports	Score 10 if all production AI models audited at policy-defined frequency; lower if infrequent or ad hoc.	As AI usage grows, algorithmic accountability becomes vital; frequent audits mitigate socio-technical risk.
	AI-to-GRC Automation Rate: percentage of AI-detected security events that automatically create GRC artefacts (risk register entries, control test results).	GRC platform integration logs	Score 10 if ≥90% of AI-detected events flow to GRC automatically; lower for manual handoffs.	Addresses the growing need for AI-driven insights to directly inform governance processes.

Additional metrics can be incorporated within each dimension as needed; DB-CCGI's architecture is modular, allowing metrics to evolve with technology and regulatory changes without altering the overall framework.

Within GCCR, regulatory requirements such as CERT-In's 6-hour reporting expectation, clock synchronisation, log retention, and incident evidence preservation are treated as components of broader cyber incident governance readiness rather than standalone compliance-only indicators.

D. Aggregation and Scoring Model

Composite Score Formulation: The original conceptual draft proposed an additive formula

$$R = \Sigma(C_{telemetry} + G_{governance}).$$

However, an additive model implies full substitutability between pillars, meaning extremely high performance in one area could offset near-zero performance in another. This contradicts the stated design intent that strong technical scores should not mask weak governance. We therefore adopt a geometric mean-based approach, which inherently penalises imbalances, a principle validated in composite index literature where the Mazziotta-Pareto Index uses non-linear functions to ensure non-substitutability among components [8].

Let C represent the aggregated technical posture score and Grepresent the aggregated governance posture score, each on a 1–10 scale. The technical pillar is defined as the average of TECE and DRCV because both dimensions primarily measure operational security capability: TECE captures exposure and control effectiveness, while DRCV captures detection strength, technical resilience, and continuous validation of security controls. The governance pillar is defined as the average of GCCR, DPDA, and AETG because these dimensions collectively measure governance execution, regulatory and legal compliance, data protection assurance, and oversight of emerging technologies.

Formally,

$$DB\text{-}CCGI = \sqrt{C \times G}$$

where

$$C = \frac{S_1 + S_4}{2}$$

and

$$G = \frac{S_2 + S_3 + S_5}{3}$$

where S_1= TECE, S_2= GCCR, S_3= DPDA, S_4= DRCV, and S_5= AETG. This assignment intentionally separates regulatory compliance readiness from incident operations: GCCR captures governance execution capacity, including incident escalation readiness, reporting accountability, evidence preservation, remediation discipline, and regulatory compliance obligations such as CERT-In reporting and log retention, whereas DRCV captures detection strength and the continuous technical validation of security control. Both $C$and $G$are bounded at 10, so the maximum DB-CCGI value is 10.

Advantages of Geometric Mean: If either pillar is extremely low, the geometric mean is low regardless of the other. For example, C = 9.0 and G = 3.0 will lead to DB-CCGI = $\sqrt{(9.0 \times 3.0)} = \sqrt{27.0} \approx 5.2$. Compare this to a simple average of (9.0 + 3.0)/2 = 6.0. The geometric mean produces a 14% lower score for the same inputs, penalising the imbalance. This is consistent with the principle that components should be treated as not fully substitutable [8].

Floor Constraint: DB-CCGI enforces a minimal governance baseline: if any governance-linked dimension (S_2, S_3, or S_5) falls below a critical threshold of 3 out of 10, the composite score is capped at a maximum of 5.0 regardless of other contributions. This reflects the real-world reality that certain compliance failures (such as a major DPDP violation or persistent failure to meet CERT-In's 6-hour reporting mandate) can outweigh technical successes.

Limitations of the Chosen Formulation: The geometric mean assumes values are reasonably scaled (which the 1-10 normalisation ensures). It can underweight moderate improvements when one pillar remains low-an intended feature for governance posture signalling, but one requires careful communication to stakeholders. An equal-weight assignment between dimensions is a simplifying assumption; empirical calibration with organisational data may suggest differential weighting. The floor constraint threshold (set at 3)

is a policy parameter that should be agreed with stakeholders and may vary by industry sector.

E. Integration of Adversarial Assessment Metrics

A distinctive feature of DB-CCGI is the integration of adversarial testing outcomes into the scoring process. Rather than treating adversarial assessment as a separate sixth pillar, we implement it as a validation overlay that modifies technical and governance dimension scores. Dimension scores are first adjusted by adversarial evidence. Then they are aggregated into the technical and governance pillars, after which the composite geometric mean is computed. Once done governance floor cap is applied if applicable.

The original framework defines three specific adversarial metrics:

1) **Adversarial Assessment Detection Rate (AADR):** The percentage of red-team test scenarios detected by the organisation's telemetry. A low AADR directly reduces the TECE and DRCV dimension scores.
2) **Adversarial Control Gap Rate (ACGR):** The percentage of scenarios in which expected controls fail to perform as designed. A high ACGR triggers point deductions in the relevant dimension. e.g., if preventive controls or exposure management controls fail, TECE is penalised; if detection logic, telemetry coverage, or technical validation mechanisms fail, DRCV is penalised.
3) **Adversarial Governance Follow-Through Rate (AGFR):** The percentage of adversarial findings that result in risk register entries or control changes within a defined remediation window. A low AGFR penalises the GCCR dimension by evidencing weak governance follow-through, poor ownership of findings, or ineffective conversion of adversarial observations into accountable remediation actions.
   Where adversarial exercises expose failures in escalation discipline, evidence retention, or governance-side response execution, the penalty applies to GCCR rather than to the technical dimensions.
4) **MITRE ATT&CK Coverage** is also incorporated: the adversarial assessment should map tested scenarios to specific ATT&CK tactics and techniques [2]. The proportion of relevant techniques for which the organisation demonstrates effective detection or mitigation provides a reproducible Adversarial Coverage Score that caps the maximum achievable TECE and DRCV scores. For instance, if only 60% of tested ATT&CK techniques were successfully detected, TECE and DRCV scores are capped at 60% of their self-assessed values before pillar aggregation.

Through this integration, DB-CCGI only improves when controls and governance hold up under realistic attack simulations. This injects a ground-truth check absent from purely self-reported maturity scores.

F. Implementation Workflow

1) **Data Collection:** Collect raw metrics from the operational and governance and adversarial systems for a defined reporting period (e.g., quarterly).
2) **Normalisation:** Convert each metric to a 1-10 score using its defined scoring function.
3) **Dimension Aggregation:** Compute each dimension's score as the arithmetic mean of its metric scores.
4) **Adversarial Adjustment:** Apply AADR, ACGR, and AGFR adjustments, plus ATT&CK-based coverage caps, to the relevant dimension scores; governance-side failures in escalation, reporting, evidence preservation, or remediation follow-through are applied to GCCR.
5) **Pillar Aggregation:** Compute $C = (S_1 + S_4)/2$ and $G = (S_2 + S_3 + S_5)/3$.
6) **Composite Index Calculation:** Compute DB-CCGI = $\sqrt{(C \times G)}$, subject to any applicable cap.
7) **Floor Constraint Check:** If any governance dimension is < 3, cap the final score at 5.0.
8) **Output:** Present the final DB-CCGI score with dimension breakdowns and a radar diagram identifying key weaknesses.

IV. Evaluation: Hypothetical Case Study

We evaluate the DB-CCGI model using a hypothetical case study contrasting two stylised organisations to illustrate how the index reflects different posture profiles.

- **Org A:** Strong technical controls, weak governance. Heavy investment in security tooling has achieved high exposure management and control scores, but compliance, data protection, and AI governance practices lag significantly.
- **Org B:** Balanced technical and governance posture. Moderately good security controls paired with equally solid compliance and governance, without extreme deficiencies in any area.

TABLE III. HYPOTHETICAL DIMENSION SCORES FOR ORG A VS ORG B

Dimension	Org A Score	Org B Score
1. TECE (Technical Exposure & Control Effectiveness)	9.0 (High)	7.5 (Good)
2. GCCR (Governance, Compliance & Cyber Response Readiness)	3.0 (Low)	6.8 (Good)
3. DPDA (Data Protection & DPDP Assurance)	2.0 (Very Low)	7.2 (Good)
4. DRCV (Detection, Resilience & Control Validation)	8.0 (High)	6.9 (Good)
5. AETG (AI & Emerging Tech Governance)	4.0 (Low)	7.1 (Good)

Step-by-step computation for Org A:

- Technical Pillar: $C\_A = (S_1 + S_4) / 2 = (9.0 + 8.0) / 2 = 8.5$
- Governance Pillar: $G\_A = (S_2 + S_3 + S_5) / 3 = (3.0 + 2.0 + 4.0) / 3 = 3.0$
- Pre-constraint DB-CCGI_A = $\sqrt{(8.5 \times 3.0)} = \sqrt{25.5} \approx 5.05$
- Floor constraint check: S_3 (DPDA) = 2.0 < 3.0 → cap applies; DB-CCGI_A = min(5.05, 5.0) = 5.0

Step-by-step computation for Org B:

- Technical Pillar: $C\_B = (7.5 + 6.9) / 2 = 7.2$
- Governance Pillar: $G\_B = (6.8 + 7.2 + 7.1) / 3 = 7.05$
- DB-CCGI_B = $\sqrt{(7.2 \times 7.05)} = \sqrt{50.76} = 7.125$
- Floor constraint check: all governance dimensions ≥ 3 → no cap.

Interpretation: Org A's high technical strength does not translate into a high composite score because weak governance pulled the index to a moderate 5.0. A simple arithmetic average would have yielded (8.5 + 3.0)/2 = 5.75,

masking the severity of the governance shortfall, including weak cyber response readiness and data protection assurance . By contrast, the 12% lower result of the geometric mean (5.05 vs. 5.75) provides a stronger signal, and the floor constraint further caps the score at 5.0, reflecting the material risk of a DPDP violation when the DPDA dimension is at 2.0. Org B's balanced performance yields a DB-CCGI of 7.125, a 40% higher score than Org A despite Org A's superior technical metrics.

Adversarial Assessment Overlay (hypothetical extension): To demonstrate the effect of independent validation, assume both organisations undergo a red-team exercise and Org A's detection rate (AADR) is only 50% while Org B achieves 85%:

- Org A's TECE and DRCV scores are capped at 50% of their self-assessed values: TECE drops from 9.0 to 4.5, DRCV drops from 8.0 to 4.0.
- Revised C_A = (4.5 + 4.0)/2 = 4.25; G_A remains 3.0.
- Revised DB-CCGI_A = $\sqrt{(4.25 \times 3.0)} = \sqrt{12.75} \approx 3.6$ (capped at 5.0 is not binding here since 3.6 < 5.0).
- If AADR = 85% and the same cap logic applies, TECE and DRCV reduce to 6.375 and 5.865 respectively, resulting in C_B=(6.375+5.865)/2=6.12; with G_B=7.05, the revised DB-CCGI becomes $\sqrt{6.12 \times 7.05} \approx 6.57$. This illustrates how adversarial validation can expose inflated self-assessments and produce a score that more accurately reflects real-world resilience.

V. Discussion

A. Novelty and Differentiation

DB-CCGI's novelty lies in its integrated, operational focus specific to the Indian regulatory context. It integrates elements from technical risk indices and governance maturity assessments into one metric. Unlike NIST CSF which guides practice but does not assign a score [1], or ATT&CK which maps adversary techniques without regard for governance [2], DB-CCGI explicitly quantifies and unifies both aspects. Compared to commercial risk indices like Trend Micro's CRI [9], DB-CCGI has an open methodology and it's a better fit for Indian regulations (CERT-In, DPDP Act). Compared to Bolpagni's country-level composite index [8], DB-CCGI functions at the corporate level with operational metrics directly tied to enterprise security tooling and compliance processes.

DB-CCGI is not a replacement for probabilistic risk models or in-depth control assessments. It is a management-level posture index that complements these by providing an accessible summary anchored in measurable data. The emphasis on adversarial validation through defined metrics (AADR, ACGR, AGFR) differentiates DB-CCGI from static compliance checklists.

B. Future-Proofing and Modularity

The framework is designed to be modular and extensible. New metrics can be introduced or existing ones modified within the five dimensions without recalibrating the overall model:

- **AI governance evolution:** As AI regulations mature, dimension 5 (AETG) can integrate new metrics (such as compliance with AI-specific rules or model explainability requirements) alongside the current algorithmic bias audit metric.
- **Regulatory updates:** If DPDP Act rules are amended or sector-specific requirements emerge from RBI, IRDAI, or SEBI, dimension 3 (DPDA) and dimension 2 (GCCR) can absorb new legal, sectoral, and cyber-response readiness metrics without structural change.
- **Technology shifts:** The telemetry inputs are described as technology-neutral, drawing from SIEM, EDR/XDR, IAM/PAM, NDR, and cloud logs. If new technology categories emerge (e.g., quantum-safe cryptography monitoring), they slot into the existing dimension framework. Specific metric names (e.g., "API Shadow IT Exposure") are illustrative instances within each dimension; the five-dimensional structure is intended to persist even as individual metrics rotate.

C. Implementability for Corporate India

Operationalisation: DB-CCGI is directly actionable by CISOs and GRC heads. Many medium-to-large Indian enterprises already maintain the data sources required. DB-CCGI provides a blueprint to consolidate existing SOC logs, compliance reports, and red-team outputs into a continuous scoring pipeline, implementable with modest tooling or via integration into existing GRC dashboards.

Board-level reporting: The single-score nature of DB-CCGI may make it suitable as a board-level cyber posture indicator, subject to validation and consistent metric governance. Boards and executive committees increasingly view cybersecurity as a governance issue, and a unified index can be reported quarterly to track improvement against risk appetite thresholds.

Regulator-facing usage: While not a mandated metric, DB-CCGI can help corporates demonstrate comprehensive risk management to auditors and regulators by bridging technical and legal controls in a single, evidence-based scorecard. The index should not be seen as a substitute for meeting specific regulatory requirements but as an internal governance indicator.

Trade-off between academic rigour and practitioner guidance: Excessive implementation detail in a conference paper risk diluting the research contribution. The recommendation is to confine the implementability discussion, as done here, to the Discussion section, clearly separated from the core model design and evaluation.

D. Sensitivity Analysis

- **Weighting sensitivity:** If technical and governance pillars were weighted differently (e.g., 60/40 split), composite scores would shift but the comparative ranking of organisations with differing balance profiles would remain stable as long as both pillars are required. For example, with a 60% weight on C and 40% on G for Org A: weighted geometric mean ≈ C^0.6 × G^0.4 = 8.5^0.6 × 3.0^0.4 ≈ 3.623 × 1.552 ≈ 5.62, which is notably higher than the equal-weight 5.05, demonstrating that weight choices materially affect absolute scores and should be calibrated with empirical data.
- **Floor constraint effects:** The constraint clusters low-performing organisations at a similar low index value, which serves as a signalling mechanism that one severe governance weakness overshadows technical

achievements. Adjusting the threshold (e.g., from 3 to 4) or penalty cap (e.g., from 5.0 to 4.0) calibrates punitiveness.

- **Adversarial input frequency:** If red-team exercises are conducted annually rather than quarterly, their impact is episodic. Smoothing functions (e.g., rolling averages of adversarial findings) can prevent abrupt index swings from a single test.

VI. Limitations and Future Work

Data availability and quality: DB-CCGI's accuracy depends on underlying data. Smaller organisations or those early in security maturity may lack advanced telemetry (e.g., UEBA for Privileged Access Entropy). This can be mitigated by substituting proxy metrics or computing partial indices with reduced metric sets.

Subjectivity of scoring thresholds: Normalising metrics to 1-10 inevitably introduces expert judgement in threshold selection. Where possible, thresholds should align with regulatory targets (e.g., the 6-hour CERT-In deadline [5] directly defines the scale for incident reporting time). Over time, collecting industry averages can enable empirical recalibration.

Absence of empirical validation: DB-CCGI is currently a conceptual model. Future work includes a pilot study with volunteer organisations to compute actual DB-CCGI scores, assess correlation with independent risk indicators (incident frequency, audit findings, cyber insurance premiums), and gather practitioner feedback on the index's face validity.

Benchmarking and comparability: The index is designed for internal improvement tracking. External benchmarking requires standardised metric definitions and possibly an industry baseline repository-an area for future collaboration via industry associations or CERT-In empanelled auditor networks.

Expanding adversarial integration: The current model applies AADR, ACGR, and AGFR adjustments somewhat discretely. More nuanced integration, such as progressively adjusting scores based on the fraction of MITRE ATT&CK techniques detected, or feeding continuous BAS output into live metric streams would enhance the adversarial dimension.

Human and cultural factors: The current framework focuses on operational metrics. Research such as Georgiadou, Mouzakitis, and Askounis's cyber-security culture framework, which spans ten dimensions including Attitude, Awareness, Behaviour, and Competency [3], suggests that human factors significantly influence cyber risk. If DB-CCGI intentionally excludes cultural assessment, this scoping choice should be documented; alternatively, a future sixth dimension could incorporate cultural metrics.

Generalisation beyond India: While tailored to Indian regulations (DPDP Act, CERT-In directives), the concept is adaptable to other jurisdictions by substituting regulatory metrics. Future work could test generalisability in different regulatory environments.

VII. Conclusion

Cybersecurity risk management in enterprises demands bridging the traditional gap between technical security operations and governance/compliance oversight. Digital Bharat Cumulative Cyber Governance Index (DB-CCGI) addresses this gap: a unified, quantitative index that captures an organisation's security posture. The technical pillar combines TECE and DRCV, while the governance pillar combines GCCR, DPDA, and AETG. Within this structure, GCCR captures governance execution under operational pressure, including escalation, reporting, accountability, and remediation readiness.

By design, DB-CCGI ensures that a strong showing in one domain cannot obscure weakness in another, enforced by geometric mean aggregation, floor constraints, and adversarial validation through defined metrics (AADR, ACGR, AGFR).

The index's five-dimension structure addresses the salient aspects of 2026-era cybersecurity from AI ethics to the 6-hour CERT-In incident reporting mandate in a modular framework suited to India's regulatory climate yet extendable beyond. Through a hypothetical case evaluation, we demonstrated how DB-CCGI differentiates a balanced security programme (scoring 7.0) from a technically strong but governance-weak one (scoring 5.0), providing actionable insight into where investment should be directed.

There is significant opportunity to refine and validate DB-CCGI with real-world deployments. We believe it provides a promising foundation for holistic cyber posture quantification that resonates with both technical teams and governance bodies-a common language for CISOs, risk officers, and regulators to identify where to invest next, with the ultimate aim of raising the organisation's overall cyber resilience.

References

[1] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, Feb. 26, 2024. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29

[2] MITRE, *MITRE ATT&CK®*. [Online]. Available: https://attack.mitre.org/

[3] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," *Sensors*, vol. 21, no. 9, p. 3267, May 2021, doi: 10.3390/s21093267.

[4] U.S. Dept. of Defense (Office of the Under Secretary of Defense for Acquisition & Sustainment), *Cybersecurity Maturity Model Certification (CMMC) Model Overview*, Version 2.0, Dec. 2021. ModelOverview.pdf

[5] Indian Computer Emergency Response Team (CERT-In), "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000," No. 20(3)/2022-CERT-In, New Delhi, India, 28 Apr. 2022. [Online]. Available: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

[6] Ministry of Law and Justice, Govt. of India, *The Digital Personal Data Protection Act, 2023* (Act No. 22 of 2023), Gazette of India, 11 Aug. 2023. [Online]. Available: https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf

[7] International Telecommunication Union, *Global Cybersecurity Index (GCI)*, ITU-D, Geneva, 2018.

[Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[8] M. Bolpagni, "Cyber risk index: a socio-technical composite index for assessing risk of cyber attacks with negative outcome," *Quality & Quantity*, vol. 56, pp. 1125–1147, 2022, doi: 10.1007/s11135-021-01199-3.

[9] Trend Micro, "More Than a Number: Your Cyber Risk Index Explained," Trend Micro Cyber Risk Exposure Management White Paper, 2025.