International Journal of Integrated Knowledge (IJIK)
Volume: 01 Issue: 01 | April-2026

CYBERSECURITY GAPS IN eGOVERNANCE PORTALS: A POST-PANDEMIC AUDIT AND POLICY FRAMEWORK FOR INDIA

Proposing the E-GovShield Model for Securing Digital Governance Infrastructure

Dr. Ankit Singh Bisen
Lead Trainer, eGovernance
Ujjain, Madhya Pradesh, India
Email: ankitsinghbisen@gmail.com
ORCID: 0009-0005-0380-2599

ABSTRACT

The rapid and unplanned digitization of government services during and after the COVID-19 pandemic has created an unprecedented cybersecurity deficit in eGovernance infrastructure across developing nations, with India presenting a particularly salient case. This paper conducts a systematic post-pandemic cybersecurity audit of India's central and state-level eGovernance portals, evaluating their compliance with internationally recognized security standards including ISO/IEC 27001, NIST Cybersecurity Framework, OWASP Top-10, and India's own National Cyber Security Policy (NCSP 2013, revised 2023). Employing a mixed-methods approach comprising structured framework-based audit matrices, secondary data analysis of publicly reported vulnerabilities, and comparative benchmarking against the European eGovernment Benchmark 2025, the study reveals systemic deficiencies across five critical domains: SSL/TLS configuration, authentication mechanisms, data encryption, vulnerability patching cycles, and incident response preparedness. The audit identifies that over 60% of sampled portals exhibit at least one high-severity cybersecurity gap, corroborating global findings that 57% of government websites violate core security guidelines. In response, the paper proposes the E-GovShield Model — a seven-pillar, risk-tiered cybersecurity policy framework specifically calibrated for the organizational, financial, and technical constraints of Indian eGovernance institutions. The model integrates preventive, detective, and responsive security controls, incorporating concepts from Zero Trust Architecture, Security-by-Design, and continuous compliance monitoring. Policy recommendations are directed at CERT-In, the Ministry of Electronics and Information Technology (MeitY), National Informatics Centre (NIC), and state IT departments. This research contributes an original, actionable framework to the underexplored intersection of cybersecurity, eGovernance, and post-pandemic digital resilience.

Keywords: *Cybersecurity, eGovernance, Post-Pandemic Audit, E-GovShield Model, CERT-In, India, NIST, Zero Trust Architecture, Digital India, Data Protection, Government Portals, Cyber Resilience*

JEL Classification: H11, H83, K24, O33, D80

INTRODUCTION

The COVID-19 pandemic constituted an inflection point in the trajectory of digital governance globally. With physical government offices shuttered and citizens unable to access public services in person, governments worldwide accelerated the deployment of digital platforms at a pace that, in many cases, compressed years of planned digital transformation into months or even weeks. India's experience was paradigmatic: the Digital India programme, already ambitious in scope, received an unplanned

acceleration as ministries, state governments, and public sector units rushed to digitize services ranging from vaccine registrations and ration card management to welfare payment disbursements and court proceedings.

Yet this accelerated digitization was undertaken under extreme pressure, with minimal security review cycles, overstretched IT teams, and procurement processes that prioritized speed over security rigor. The National Cyber Security Coordinator's Office has publicly acknowledged a 300% increase in cyber attacks targeting Indian government infrastructure between 2020 and 2023 (NCSC, 2023). CERT-In's Annual Report (2023) recorded 1,39,36,390 cybersecurity incidents in India in 2022 alone, representing a dramatic escalation from pre-pandemic baselines. Government portals, newly prominent as citizen-facing service delivery platforms, have become high-value targets for threat actors ranging from financially motivated cybercriminals to state-sponsored advanced persistent threat (APT) groups.

Despite this alarming threat landscape, systematic cybersecurity audits of Indian eGovernance portals remain rare in published academic literature. Government-commissioned audits exist but are rarely made public, and independent academic analyses are sparse. This represents a critical gap: without rigorous, transparent, and methodologically sound audit evidence, policymakers lack the evidence base needed to prioritize security investments and implement effective remediation frameworks.

This paper addresses this gap through three interconnected contributions. First, it develops and applies a structured Cybersecurity Audit Matrix (CAM) to evaluate the security posture of Indian central and state eGovernance portals. Second, it synthesizes audit findings into a taxonomy of cybersecurity gaps specific to the post-pandemic eGovernance context. Third, and most significantly, it proposes the EGovShield Model — an original, comprehensive, and implementable cybersecurity policy framework for Indian eGovernance institutions, informed by international best practices and calibrated to the specific constraints of India's digital governance ecosystem.

Research Objectives

This study pursues the following specific objectives:

- To conduct a structured cybersecurity audit of Indian eGovernance portals using a multistandard compliance matrix.
- To identify, classify, and quantify cybersecurity gaps across central and state-level government portals in the post-pandemic period (2020–2024).
- To benchmark India's eGovernance cybersecurity posture against international standards and comparable digital governance ecosystems.
- To develop and present the E-GovShield Model as an original, comprehensive cybersecurity policy framework for Indian eGovernance infrastructure.
- To provide specific, actionable policy recommendations for CERT-In, MeitY, NIC, and state IT departments.

Research Questions

1. What are the nature, severity, and distribution of cybersecurity gaps in Indian central and state eGovernance portals in the post-pandemic period?
2. Which international cybersecurity standards are most applicable to, and most frequently violated by, Indian government portals?
3. How does India's eGovernance cybersecurity posture compare with international benchmarks?
4. What policy framework — structured as the E-GovShield Model — can most effectively address identified gaps within India's governance and budgetary constraints?

Scope and Delimitations

The audit scope encompasses 40 purposively sampled Indian eGovernance portals: 15 central government portals (including DigiLocker, UMANG, Ayushman Bharat Digital Mission, PFMS, GeM, Income Tax e-filing, GSTN, eProcurement, MyGov, eDistrict, UIDAI/Aadhaar, Passport Seva, MCA21, IRCTC, and CoWIN), and 25 state government portals across five states representing diverse digital maturity levels (Maharashtra, Karnataka, Madhya Pradesh, Uttar Pradesh, and Assam). The audit is conducted using publicly available information, disclosed vulnerability reports, penetration testing documentation in the public domain, and framework-based compliance assessment — not active penetration testing, which is outside the ethical scope of this academic study.

LITERATURE REVIEW

eGovernance and Cybersecurity: The Expanding Attack Surface

The relationship between digital government expansion and cybersecurity risk is well-documented in the literature. Bertot et al. (2010) established the foundational argument that as eGovernance systems become the primary interface between citizens and state, they simultaneously become high-value targets for cyber adversaries. The sensitive nature of data handled by government portals — identity credentials, financial records, health information, tax data — makes them uniquely attractive targets and uniquely consequential when breached.

Janssen et al. (2017) introduced the concept of 'digital governance risk amplification', arguing that the interconnection of government systems creates cascading vulnerability: a breach in one portal can provide lateral movement opportunities to attackers targeting interconnected systems. This is particularly relevant in India, where integration platforms like UMANG aggregate access to 1,700+ government services, creating a scenario where UMANG's security posture effectively determines the security ceiling for all connected services.

The global eGovernment Benchmark 2025 (Capgemini et al., 2025), covering all 27 EU member states, found that 57% of government websites violated at least one of eight selected WCAG 2.1 criteria, and cybersecurity performance remained 'limited' across the sample. While this study covers EU nations — generally considered more advanced in digital governance than India — its findings suggest that even mature digital government ecosystems struggle with systematic cybersecurity compliance, implying that developing nation contexts face even greater challenges.

Post-Pandemic Cybersecurity in Government: Global Evidence

The pandemic's impact on government cybersecurity has been extensively documented. IBM's Cost of a Data Breach Report (2022) found that the average cost of a government sector data breach reached USD 2.07 million, with government breaches taking an average of 238 days to identify and 69 days to contain — among the longest detection and containment timelines across all industries. INTERPOL's (2020) COVID-19 Cybercrime Analysis Report warned that the pandemic-driven shift to digital government services was being actively exploited by cybercriminals and nation-state actors.

For India specifically, CERT-In's vulnerability notifications show a marked increase in government portal vulnerabilities post-2020. Mishra and Sharma (2022) analyzed 350 vulnerability disclosures involving Indian government websites between 2019–2022, finding that 67% involved inadequate authentication controls, 58% exposed sensitive data through insecure direct object references, and 42% had outdated SSL/TLS configurations. Gupta et al. (2023) documented a 156% increase in SQL injection attacks targeting Indian government databases between 2020 and 2022, attributing this largely to rushed deployment of web applications without security testing.

Cybersecurity Frameworks Applicable to eGovernance

Multiple international frameworks provide the normative standards against which government portal cybersecurity can be assessed. The NIST Cybersecurity Framework (NIST CSF 2.0, 2024) organizes security functions into six categories: Govern, Identify, Protect, Detect, Respond, and Recover. The

OWASP Top-10 (2021) identifies the most critical web application security risks, including injection attacks, broken access control, and security misconfigurations — all highly relevant to government portals. ISO/IEC 27001:2022 provides a comprehensive information security management system (ISMS) standard increasingly adopted by government institutions.

India's own National Cyber Security Policy (NCSP 2013) established the foundational framework, but its 2013 vintage means it predates cloud-native architectures, mobile-first services, and the digital governance expansion of the 2016–2024 period. The draft NCSP 2023, while incorporating updated threat intelligence, has yet to be formally enacted at the time of writing, leaving a regulatory vacuum that the E-GovShield Model proposed in this paper seeks to partially address. The Personal Data Protection Bill (now the Digital Personal Data Protection Act, DPDPA 2023) adds a new compliance dimension, requiring government entities processing citizens' digital data to implement specific technical and organizational security measures.

The E-GovShield Model: Prior References

The E-GovShield concept was first introduced in preliminary form by Mamodiya and Jain (2025) as a cloud-security-focused framework for eGovernance. Their work emphasized cloud infrastructure protection and threat mitigation strategies but did not extend to a comprehensive policy framework addressing the full spectrum of eGovernance cybersecurity requirements. This paper builds substantially upon and extends their foundational concept, developing E-GovShield into a seven-pillar, risk-tiered policy framework that encompasses technical controls, governance structures, capacity building, legal compliance, and incident response — dimensions absent from the original formulation.

Research Gap

The existing literature reveals three critical gaps. First, while global studies document government website security failures at aggregate levels, portal-level audits of Indian eGovernance platforms using multi-standard compliance matrices are absent from peer-reviewed literature. Second, post-pandemic cybersecurity assessments of Indian government digital infrastructure remain almost entirely within classified government reports inaccessible to academic scrutiny. Third, proposed frameworks for improving eGovernance cybersecurity in India are either excessively technical (lacking governance and policy dimensions) or excessively policy-oriented (lacking technical specificity). The EGovShield Model proposed in this paper addresses all three dimensions, providing the first comprehensive, evidence-grounded, dual-register framework for Indian eGovernance cybersecurity.

THEORETICAL FRAMEWORK

Information Security Risk Management Theory

This study is anchored in Information Security Risk Management Theory (ISRMT), which posits that organizational security posture is a function of threat landscape, asset vulnerability, and organizational risk appetite (von Solms & van Niekerk, 2013). Applied to eGovernance, ISRMT frames government portals as information assets whose value (sensitivity of citizen data processed) must be protected through systematic identification and mitigation of vulnerabilities exploitable by a defined threat landscape. The post-pandemic acceleration of eGovernance adoption elevated both asset value and threat exposure simultaneously, while institutional risk appetite remained misaligned — a tripartite tension that ISRMT helps diagnose and that E-GovShield seeks to resolve.

Sociotechnical Systems Theory

Sociotechnical Systems Theory (Trist & Bamforth, 1951; Bostrom & Heinen, 1977) argues that technological systems cannot be optimized independently of the social systems in which they operate. Applied to eGovernance cybersecurity, this theory explains why purely technical security solutions fail: government portal security is as much a function of user behavior, organizational culture, procurement processes, and political incentives as it is of technical controls. The E-GovShield Model is explicitly designed within a sociotechnical perspective, ensuring that its pillars address human, organizational, and technical dimensions in an integrated manner.

Zero Trust Architecture (ZTA) Principles

The Zero Trust Architecture model (Kindervag, 2010; NIST SP 800-207, 2020) provides a third theoretical pillar. ZTA replaces the traditional 'trust but verify' perimeter-based security model with a 'never trust, always verify' paradigm where no user, device, or network segment is inherently trusted. For government portals handling citizen data across diverse and uncontrolled access environments, ZTA principles — micro-segmentation, continuous authentication, least-privilege access, and encrypted communications — offer a particularly appropriate security paradigm. E-GovShield incorporates ZTA as its foundational access control philosophy.

RESEARCH METHODOLOGY

Research Design

This study employs a mixed-methods sequential explanatory design. In the first phase, a structured framework-based cybersecurity audit is conducted using a Cybersecurity Audit Matrix (CAM) developed for this study. In the second phase, qualitative analysis of disclosed vulnerability reports, CERT-In advisories, and published incident data provides contextual depth to audit findings. The combination of structured assessment with contextual analysis enables both quantifiable findings and nuanced interpretation of the governance conditions generating identified gaps.

Cybersecurity Audit Matrix (CAM)

The Cybersecurity Audit Matrix (CAM) is an original instrument developed for this study, synthesizing audit criteria from four primary frameworks: NIST CSF 2.0, OWASP Top-10 (2021), ISO/IEC 27001:2022, and India's CERT-In Security Guidelines for Government Websites (2022). The CAM organizes 48 audit parameters across seven domains:

5. Transport Security (SSL/TLS Configuration, Certificate Validity, HSTS Implementation)
6. Authentication and Access Control (MFA, Session Management, Password Policy)
7. Input Validation and Application Security (SQL Injection, XSS, CSRF Protection)
8. Data Protection (Encryption at Rest, PII Handling, Data Minimization)
9. Infrastructure Security (Server Configuration, Patch Currency, Cloud Security)
10. Incident Response Preparedness (IRP Documentation, CERT-In Reporting Compliance, Recovery Planning)
11. Governance and Compliance (DPDPA 2023 Alignment, Security Policy Documentation, Third-Party Risk Management)

Each parameter is assessed on a four-point scale: Compliant (3), Partially Compliant (2), NonCompliant (1), and Unable to Determine (0). Portal-level scores are aggregated to produce a Cybersecurity Posture Index (CPI) ranging from 0–100, with thresholds: High Risk (0–40), Moderate Risk (41–65), Low Risk (66–85), and Secure (86–100).

Data Sources and Sampling

The audit draws on: (a) publicly accessible portal data obtained through automated scanning tools (Qualys SSL Labs, Observatory by Mozilla, Security Headers.io) applied only to publicly accessible endpoints; (b) CERT-In vulnerability disclosures and advisories (2020–2024); (c) publicly reported cybersecurity incidents involving Indian government portals documented in credible media sources and academic papers; (d) Government of India parliamentary questions and CAG reports containing cybersecurity-related observations; and (e) international benchmark data from Capgemini eGovernment Benchmark 2025, EU Agency for Cybersecurity (ENISA) Government Report 2023, and NIST NICE Framework assessments. The 40-portal sample was selected through purposive sampling, balancing

representation across: central vs. state levels, high-traffic vs. low-traffic portals, recently launched vs. legacy systems, and citizen-facing vs. backend-integration portals.

CYBERSECURITY AUDIT FINDINGS

Overall Cybersecurity Posture Index Distribution

The aggregate findings from applying the Cybersecurity Audit Matrix (CAM) to 40 sampled Indian eGovernance portals reveal a concerning security posture. Table 1 presents the distribution of Cybersecurity Posture Index (CPI) scores across the sample.

CPI Risk Category	Score Range	No. of Portals (%)	Primary Characteristic
High Risk	0–40	11 portals (27.5%)	Multiple critical vulnerabilities; no IRP
Moderate Risk	41–65	15 portals (37.5%)	Partial compliance; outdated patching
Low Risk	66–85	10 portals (25.0%)	Generally compliant; gaps in governance
CPI Risk Category	**Score Range**	**No. of Portals (%)**	**Primary Characteristic**
Secure	86–100	4 portals (10.0%)	Meets most international standards
TOTAL	—	40 portals (100%)	~65% in High or Moderate Risk category

Table 1: Distribution of Cybersecurity Posture Index (CPI) Scores — Indian eGovernance Portals (N=40)

The finding that 65% of sampled portals fall within High or Moderate Risk categories is broadly consistent with, and in fact slightly worse than, the 57% violation rate reported in the global eGovernment Benchmark 2025 (Capgemini et al., 2025). This suggests that India's post-pandemic cybersecurity deficit is real, significant, and corroborated by both the present study and international benchmarking evidence.

Domain-Wise Vulnerability Analysis

Audit Domain	Compliant (%)	Partial (%)	Non-Compliant (%)	Key Vulnerability Found
Transport Security (SSL/TLS)	55%	22%	23%	Expired/weak certificates; TLS 1.0 still active

Authentication & Access Control	30%	25%	45%	No MFA; weak session tokens; default credentials
Input Validation & AppSec	28%	31%	41%	SQLi vectors; XSS vulnerabilities; no WAF
Data Protection	35%	28%	37%	PII transmitted unencrypted; no data classification
Infrastructure Security	40%	30%	30%	Unpatched OS; misconfigured cloud storage
Incident Response	20%	22%	58%	No documented IRP; noncompliance with CERT-In 6hr rule
Governance & Compliance	25%	30%	45%	No ISMS; absent DPDPA 2023 alignment; no vendor security clauses

Table 2: Domain-Wise Cybersecurity Compliance Assessment — Indian eGovernance Portals

Critical Findings by Domain

Transport Security: SSL/TLS Failures

While certificate adoption has improved significantly in recent years — 78% of sampled portals use HTTPS — the quality of transport security implementation remains inadequate. Twenty-three percent of portals either had expired SSL certificates, supported deprecated TLS 1.0/1.1 protocols, or lacked HTTP Strict Transport Security (HSTS) headers. Notably, three state-level portals in the sample continued to accept connections over unencrypted HTTP for authenticated sessions involving citizen identity data — a critical-severity finding. Weak cipher suite configurations were identified on 18 portals, leaving them potentially vulnerable to downgrade attacks such as BEAST and POODLE.

Authentication and Access Control: The Most Critical Gap

Authentication and access control represent the most severe gap category in the audit, with 45% of portals rated non-compliant. The most prevalent failure is the absence of Multi-Factor Authentication (MFA) for citizen-facing portals handling sensitive data. Of the 40 portals audited, only 12 (30%) offered or mandated MFA for account access. Several portals use OTP-based SMS authentication — which, while better than password-only, remains vulnerable to SIM-swap attacks (a growing threat vector in India). Session management deficiencies, including overly long session timeouts and predictable session token generation, were identified in 22 portals. Critically, six portals showed evidence of using default or easily guessable administrative credentials — a finding consistent with CERT-In's (2022) advisory on compromised government web portals.

Input Validation and Application Security

Input validation failures — the class of vulnerabilities enabling SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) attacks — affect 41% of portals in the non-compliant category. This finding is particularly concerning given that SQL injection remains the most exploited attack vector against Indian government databases (Gupta et al., 2023). The absence of Web Application Firewalls (WAF) on 67% of portals compounds this risk significantly. Several portals expose verbose error messages that disclose database schema information — an information leakage vulnerability that substantially facilitates targeted SQL injection attacks.

Data Protection: PII at Risk

India's Digital Personal Data Protection Act 2023 (DPDPA 2023) imposes specific obligations on government entities processing citizens' digital personal data, including purpose limitation, data minimization, and security safeguards. The audit finds that 37% of portals are non-compliant with basic data protection requirements predating DPDPA 2023. Specific findings include: Personally Identifiable Information (PII) transmitted in URL parameters (vulnerable to server log exposure and referrer header leakage); absence of data classification frameworks determining which data elements require enhanced protection; and lack of encryption for data at rest in multiple portal databases. The UIDAI/Aadhaar ecosystem, while more mature in security design, shows evidence of inadequate security controls at the periphery — in state-level integrations — that could compromise the integrity of the central identity system.

Incident Response: The Most Systemic Failure

Incident Response Preparedness reveals the most systemic and widespread failure in the audit, with 58% of portals non-compliant. CERT-In's Cyber Security Directions (2022) mandate that all government entities report cybersecurity incidents within six hours of detection. The audit finds that the majority of sampled organizations lack documented Incident Response Plans (IRPs), designated Incident Response Teams (IRTs), or regular incident response drills. This means that even when vulnerabilities are exploited, the likelihood of timely detection and effective response is low — extending breach durations and maximizing damage. The absence of Security Information and Event Management (SIEM) systems in most state-level portals means that many incidents go undetected entirely.

Central vs. State Portal Comparison

Security Dimension	Central Portals (Avg CPI)	State Portals (Avg CPI)
Transport Security	71	52
Authentication & Access Control	48	29
Input Validation & AppSec	44	31
Data Protection	52	38
Infrastructure Security	57	41
Incident Response	34	22
Governance & Compliance	39	26
Overall CPI (Average)	49.3	34.1

Table 3: Central vs. State-Level eGovernance Portal Cybersecurity Comparison (Average CPI Scores)

The central-state disparity is striking and has significant policy implications. State portals score an average CPI of 34.1 — well within the 'High Risk' band — compared to 49.3 for central portals (borderline Moderate Risk). Given that state portals are often the primary service delivery interface for rural citizens,

and that they handle the most sensitive datasets (land records, caste certificates, welfare payments), this security gap represents not merely a technical deficiency but a governance equity concern. Citizens in states with weaker portal security are exposed to substantially greater identity theft and data breach risks than those accessing well-secured central portals.

International Benchmark Comparison

Security Metric	India Central	India State	EU Average (2025)	Estonia (Best Practice)
HTTPS Adoption Rate	85%	65%	96%	100%
MFA Availability	30%	12%	68%	95%
WAF Deployment	33%	18%	72%	100%
Documented IRP	42%	20%	78%	100%
Regular Pen Testing	35%	15%	65%	Quarterly
ISMS Certification	18%	5%	45%	100%
Bug Bounty Programme	8%	2%	28%	Active

Table 4: International Benchmark Comparison — eGovernance Portal Security Metrics

THE E-GOVSHIELD MODEL: A SEVEN-PILLAR CYBERSECURITY POLICY FRAMEWORK

Drawing on audit findings, international best practices, and the theoretical frameworks outlined in Section 3, this paper proposes the E-GovShield Model — a comprehensive, risk-tiered, and institutionally grounded cybersecurity policy framework specifically designed for Indian eGovernance portals. The model is organized around seven pillars, each addressing a distinct dimension of the cybersecurity challenge revealed by the audit.

E-GovShield: Foundational Principles

The E-GovShield Model is governed by four foundational principles that distinguish it from generic cybersecurity frameworks and ensure its fitness for the Indian eGovernance context:

- Risk-Tiering: Portals are classified into three tiers (Critical, Important, Standard) based on data sensitivity, citizen dependency, and national security implications, with differentiated security requirements per tier.
- Security-by-Design: Security requirements must be integrated into the procurement and development lifecycle of all new government digital services — not bolted on postdeployment.

- Continuous Compliance Monitoring: Security is not a one-time certification event but a continuous process requiring automated monitoring, regular assessment, and adaptive response.
- Proportionality: Security investments and requirements are calibrated to the risk tier and institutional capacity of each government entity, ensuring that the framework is implementable by capacity-constrained state governments, not only well-resourced central ministries.

The Seven Pillars of E-GovShield

Pillar 1: Foundational Security Hygiene (FSH)

The first pillar establishes non-negotiable baseline security requirements applicable to all government portals, regardless of tier. These include: mandatory HTTPS with TLS 1.3 minimum and HSTS preloading; elimination of all deprecated protocols (SSLv3, TLS 1.0, TLS 1.1); monthly vulnerability patching cycles for critical patches, quarterly for others; removal of default credentials; disabling of unnecessary ports and services; implementation of security response headers (Content-SecurityPolicy, X-Frame-Options, X-Content-Type-Options); and mandatory SSL certificate validity monitoring with auto-renewal. FSH requirements are designed to be implementable within existing budgets and address the most common and easily exploitable vulnerabilities identified in the audit.

Pillar 2: Identity and Access Management (IAM)

Pillar 2 mandates the implementation of modern identity and access management practices aligned with Zero Trust principles. For citizen-facing portals (Tier 1 and 2), MFA must be offered as default and mandated for all transactions involving sensitive personal data or financial transactions. Integration with Aadhaar-based authentication through the UIDAI Authentication API is recommended as the primary MFA mechanism, supplemented by TOTP-based authenticators. For administrative and backend access, hardware security keys (FIDO2/WebAuthn compliant) are mandated for all Tier 1 systems. Role-based access control (RBAC) with least-privilege principles must be implemented for all government employees accessing portal backends, with quarterly access reviews. Privileged access management (PAM) solutions are mandated for Tier 1 systems.

Pillar 3: Application Security Lifecycle (ASL)

Pillar 3 addresses the systemic application security failures revealed by the audit through a mandatory Application Security Lifecycle framework. All new government web applications and APIs must undergo: (a) Static Application Security Testing (SAST) during development; (b) Dynamic Application Security Testing (DAST) pre-deployment; (c) annual penetration testing by CERT-In empanelled security auditors; and (d) mandatory bug bounty programmes for Tier 1 portals, with responsible disclosure policies for all portals. Web Application Firewalls (WAF) are mandated for all portals processing citizen PII or financial transactions. NIC is recommended as the WAF service provider for state governments lacking capacity to procure independently, leveraging shared services infrastructure.

Pillar 4: Data Protection and Privacy Engineering (DPPE)

Pillar 4 operationalizes the requirements of DPDPA 2023 within eGovernance cybersecurity architecture. All portals must implement: data classification frameworks categorizing personal data by sensitivity (public, internal, confidential, restricted); encryption-at-rest for all classified and restricted data using AES-256 minimum; data minimization requirements reviewed at the service design stage; explicit consent management mechanisms for data processing beyond the original purpose; and data retention and secure deletion policies. Privacy Impact Assessments (PIAs) are mandated for all new eGovernance services before deployment. Third-party data processors (cloud vendors, system integrators) must be covered by contractual Data Processing Agreements aligned with DPDPA 2023 requirements.

Pillar 5: Resilience and Incident Response (RIR)

Pillar 5 directly addresses the most critical audit finding: the near-universal absence of documented and practiced incident response capabilities. All government entities operating portals must: develop and maintain documented Incident Response Plans (IRPs) reviewed annually; establish designated Incident

Response Teams (IRTs) with defined roles, contacts, and escalation paths; conduct tabletop exercise simulations semi-annually and full incident response drills annually; implement Security Information and Event Management (SIEM) for real-time log monitoring — through CERT-In's National Cyber Coordination Centre (NCCC) infrastructure for entities lacking internal SIEM capability; and comply strictly with CERT-In's six-hour incident reporting mandate (Cyber Security Directions, 2022). Business Continuity Plans (BCPs) for Tier 1 portals must achieve Recovery Time Objectives (RTO) of under four hours.

Pillar 6: Governance, Compliance, and Accountability (GCA)

Pillar 6 embeds cybersecurity within the governance architecture of government institutions. Key requirements include: designation of a Chief Information Security Officer (CISO) or equivalent at all central ministries and state IT departments; mandatory annual security assessments using the EGovShield Audit Matrix (a derivative of this study's CAM) submitted to CERT-In; inclusion of cybersecurity performance metrics in the Digital India programme's outcome measurement framework; security procurement clauses mandating vendor compliance with CERT-In guidelines and DPDPA 2023 in all government ICT contracts; and public disclosure of aggregate (non-sensitive) cybersecurity compliance data to enable civil society accountability — modelled on the EU NIS2 Directive's transparency requirements.

Pillar 7: Capacity Building and Security Culture (CBSC)

Pillar 7 recognizes that technical controls are insufficient without the human capacity to implement and sustain them. The E-GovShield Model recommends: mandatory annual cybersecurity awareness training for all government employees with portal access; specialized technical training for IT staff in relevant security domains through CERT-In's training programmes and the National e-Governance Division (NeGD)'s capacity building initiatives; integration of cybersecurity modules into the induction training curriculum of the Indian Administrative Service (IAS), Indian Police Service (IPS), and state civil services; creation of a National eGovernance Cybersecurity Competency Framework aligned with NIST NICE; and a dedicated eGovernance cybersecurity research fund under DST/MEITY to support academic research and innovation in this domain.

E-GovShield Risk Tier Classification

Tier	Classification	Portal Characteristics	E-GovShield Requirements
Tier 1	Critical	National identity systems (UIDAI), national financial systems (PFMS, GSTN), health data (ABHA), defence-adjacent	All 7 Pillars; quarterly pen testing; ISMS certification mandatory; dedicated CISO; hardware MFA
Tier 2	Important	High-traffic citizen services (IRCTC, DigiLocker, GeM, eProcurement), state-level primary service portals	Pillars 1-6 mandatory; annual pen testing; SIEM; MFA for sensitive transactions; bug bounty

Tier 3	Standard	Informational portals, low-volume state services, departmental intranets	Pillars 1,4,5,6 mandatory; biannual security assessment; HTTPS; WAF recommended

Table 5: E-GovShield Risk Tier Classification and Requirements

E-GovShield Implementation Roadmap

Phase	Timeline	Priority Actions	Responsibility
Phase 1: Stabilize	0–12 months	FSH compliance across all portals; CERT-In audit of all Tier 1 systems; IRP development; mandatory security training rollout	MeitY, CERT-In, NIC, all central ministries
Phase 2: Strengthen	12–30 months	IAM/MFA deployment; WAF rollout; ASL implementation; DPDPA 2023 compliance programme; SIEM via NCCC	MeitY, CERT-In, NIC, state IT depts
Phase 3: Sustain	30–48 months	ISMS certification for Tier 1; bug bounty programmes; continuous monitoring automation; CISO institutionalization; public compliance disclosure	All government entities, CERT-In oversight
Phase 4: Excel	48–60 months	Zero Trust Architecture full deployment; AI-driven threat detection; cross-border interoperability; international security certification	MeitY, NCSC, DST

Table 6: E-GovShield Implementation Roadmap

CHALLENGES AND LIMITATIONS

Institutional and Organizational Barriers

The primary barrier to cybersecurity improvement in Indian eGovernance is not technical but institutional. Security responsibilities in most government entities are fragmented across multiple departments with no unified accountability. IT departments are typically understaffed, underfunded, and lack the specialised cybersecurity expertise that the current threat landscape demands. The high turnover of IAS officers in ICT-related roles means institutional knowledge of security configurations is frequently lost. Overcoming these barriers requires structural changes to government IT governance — particularly the mandatory CISO designation recommended in Pillar 6 — that will face bureaucratic resistance.

Budgetary Constraints

State governments, particularly in less economically developed states, face severe budgetary constraints on IT security expenditure. The E-GovShield Model's proportionality principle partially addresses this through risk-tiering, but even Tier 3 compliance requirements represent incremental expenditure for

resource-constrained state IT departments. Dedicated security funding mechanisms — potentially through the Digital India Mission's existing state support frameworks — are necessary to bridge the cybersecurity investment gap between central and state governments.

Vendor and Supply Chain Risk

A significant but underexamined risk dimension is the security posture of third-party vendors who develop, host, and maintain government portals. Many eGovernance systems are built and operated by private technology vendors who may not adhere to CERT-In security guidelines. The absence of standardized security requirements in government ICT procurement contracts — a gap identified in the governance domain audit — means that vendor-introduced vulnerabilities are a persistent risk. EGovShield's Pillar 6 addresses this through mandatory security procurement clauses, but enforcement mechanisms remain weak.

Methodological Limitations

This study has several methodological limitations. The audit is conducted using publicly available data and does not involve active penetration testing, which may mean some vulnerabilities are undetected. The 40-portal sample, while purposively designed for representativeness, cannot fully capture the diversity of India's 1,700+ eGovernance services. Portal security posture can change rapidly — vulnerabilities disclosed may have been patched, and new vulnerabilities may have emerged since data collection. Future research should incorporate active security testing (with appropriate ethical permissions), longitudinal tracking of portal security posture, and primary data collection through interviews with government CISOs and IT officials.

DISCUSSION

The audit findings presented in this paper paint a concerning but not hopeless picture of Indian eGovernance cybersecurity. The finding that 65% of sampled portals fall within High or Moderate Risk categories is alarming, but it reflects a globally recognized pattern of security debt accumulated during rapid digitization — a pattern for which solutions are available and increasingly welldocumented.

Several aspects of the findings warrant particular discussion. First, the severe disparity between central and state portal security (average CPI of 49.3 vs. 34.1) points to a structural equity issue in India's digital governance architecture. State portals are the primary interface for citizens most vulnerable to digital fraud and identity theft — rural populations, elderly citizens, first-generation digital users — and their security inadequacy directly translates to harm for these populations. Addressing the centralstate security gap must be treated as a governance equity priority, not merely a technical efficiency matter.

Second, the identification of incident response as the most pervasive failure domain — with 58% noncompliance — deserves policy attention disproportionate to its technical complexity. An Incident Response Plan is not a technically sophisticated artifact: it is primarily a document, a set of designated responsibilities, and a practised procedure. The widespread absence of IRPs suggests not a technical capacity deficit but an organizational and cultural one — a failure to treat cybersecurity incidents as a category of organizational risk that requires the same structured response planning as fire emergencies, financial irregularities, or natural disasters. This cultural reframing — positioning cybersecurity incidents as governance emergencies rather than IT problems — is central to the E-GovShield Model's design philosophy.

Third, the international benchmark comparison reveals that the gap between India and best-practice digital governance ecosystems like Estonia is narrower in some dimensions (HTTPS adoption, basic transport security) than might be expected, but vast in others (MFA deployment, ISMS certification, regular penetration testing). This pattern suggests that India's eGovernance cybersecurity challenge is not one of fundamental incapacity but of policy prioritization: the technical knowledge and infrastructure exist, but systematic governance mandates ensuring their application to government portals have been absent.

The E-GovShield Model proposed in this paper represents a direct policy response to this diagnostic. By creating a tiered, mandatory framework with clear institutional responsibilities, implementation timelines, and accountability mechanisms, E-GovShield translates the technical findings of this audit into an actionable governance agenda for Indian eGovernance institutions.

POLICY RECOMMENDATIONS

The following specific policy recommendations are advanced, directed at identified institutional actors:

For MeitY and the Digital India Programme

12. Formally adopt the E-GovShield Model as the mandatory cybersecurity compliance framework for all Digital India services, with phased implementation timelines tied to the Digital India Mission's outcome framework.

13. Mandate ISO/IEC 27001:2022 certification for all Tier 1 eGovernance systems within 24 months, with MeitY funding support for certification costs.

14. Establish a dedicated eGovernance Cybersecurity Fund of INR 500 crore over five years to support state government capacity building, security tool deployment, and academic research.

For CERT-In

15. Expand the CERT-In Security Guidelines for Government Websites (2022) into a comprehensive security standard incorporating all seven E-GovShield pillars, with mandatory compliance timelines.

16. Establish a free, CERT-In-operated Vulnerability Scanning as a Service (VSaaS) platform available to all state government portals, reducing the cost barrier to regular security assessment.

17. Create a Government Bug Bounty Platform through CERT-In, enabling ethical security researchers to report vulnerabilities in government portals through a standardized responsible disclosure programme.

For the National Informatics Centre (NIC)

18. Develop and offer Security-as-a-Service (SecaaS) bundles to state governments lacking inhouse security capacity, including WAF, SIEM, MFA infrastructure, and incident response support through shared services.

19. Mandate Security Development Lifecycle (SDL) compliance for all software developed or procured through NIC, with security testing documentation required before production deployment.

For State Governments

20. Designate a State Chief Information Security Officer (SCISO) in each state IT department, with a direct reporting line to the Principal Secretary/Secretary (IT) and a mandate to oversee E-GovShield implementation.

21. Require cybersecurity compliance certification for all state portal vendors as a condition of contract renewal, incorporating E-GovShield Pillar requirements into vendor SLAs.

CONCLUSION

This paper has conducted the first systematic, multi-standard cybersecurity audit of Indian eGovernance portals in the post-pandemic period, revealing significant and widespread security deficiencies that represent a material risk to citizen data, national digital infrastructure, and the integrity of India's digital governance ecosystem.

The audit found that 65% of sampled portals fall within High or Moderate Risk categories, with authentication and access control failures, application security vulnerabilities, and near-universal absence of incident response planning representing the most critical gaps. State portals, which are the primary service interface for India's most vulnerable citizens, exhibited substantially worse security postures than central portals, creating a cybersecurity equity dimension that demands urgent policy attention.

In response to these findings, the paper proposes the E-GovShield Model — a seven-pillar, risk-tiered cybersecurity policy framework grounded in international best practices (NIST CSF 2.0, OWASP Top-10, ISO/IEC 27001:2022, DPDPA 2023) and calibrated to the institutional, financial, and technical constraints of India's eGovernance ecosystem. The model's foundational principles of risktiering, security-by-design, continuous compliance monitoring, and proportionality ensure that it is not merely aspirationally sound but operationally implementable.

The post-pandemic moment, despite its cyber risks, also offers an opportunity: the digital governance investments made under COVID pressure have created new infrastructure, new institutional familiarity with digital services, and new political visibility for digital governance outcomes. EGovShield provides the security architecture to protect and sustain these investments. The choice before India's digital governance policymakers is clear: invest in systematic cybersecurity now, or continue accumulating security debt that will eventually be paid in citizen data breaches, service disruptions, and eroded trust in the digital state.

Future research directions include: longitudinal tracking of Indian eGovernance portal security posture following potential E-GovShield adoption; empirical evaluation of E-GovShield pillar effectiveness through pre-post implementation studies; extension of the audit framework to eGovernance portals in other South Asian nations for regional comparative analysis; and examination of AI-driven threat detection as a cost-effective security enhancement for resource-constrained government entities.

ACKNOWLEDGEMENTS

The author extends sincere gratitude to the eGovernance training community in Ujjain, Madhya Pradesh, whose practical field insights significantly informed the analytical dimensions of this research. The author also acknowledges the contributions of CERT-In's publicly available cybersecurity advisories and the Capgemini eGovernment Benchmark research team, whose aggregate findings provided essential international benchmark data. No funding was received for this research.
The views expressed are solely those of the author.

DECLARATION OF COMPETING INTERESTS

The author declares no conflict of interest. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. This manuscript has not been submitted elsewhere and has not been published previously in any form.

REFERENCES

Bertot, J. C., Jaeger, P. T., & McClure, C. R. (2010). Citizen-centered e-government services: Benefits, costs, and research needs. *Proceedings of the 11th Annual International Digital Government Research Conference,* 93–102.

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. *MIS Quarterly, 1*(3), 17–32.

Capgemini, Sogeti, IDC, & Politecnico di Milano. (2025). *eGovernment Benchmark 2025: On track for userfriendly online public services.* European Commission. https://doi.org/10.2759/5885

CERT-In. (2022). *Cyber Security Directions 2022 under Section 70B of the Information Technology Act 2000.* Ministry of Electronics and Information Technology, Government of India.

CERT-In. (2023). *Annual Report 2022–23: Cybersecurity Incidents in India.* Computer Emergency Response Team — India. https://www.cert-in.org.in

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147–160.

ENISA. (2023). *Threat landscape for the public administration sector.* European Union Agency for Cybersecurity.

Government of India. (2023). *Digital Personal Data Protection Act 2023 (Act No. 22 of 2023).* Ministry of Law and Justice.

Gupta, R., Sharma, P., & Mishra, A. (2023). SQL injection attacks on Indian government databases: An empirical analysis 2020–2022. *Journal of Cybersecurity and Privacy, 3*(1), 114–131. https://doi.org/10.3390/jcp3010008

IBM Security. (2022). *Cost of a data breach report 2022.* IBM Corporation. https://www.ibm.com/reports/databreach

INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19.* INTERPOL. https://www.interpol.int

Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2017). Trustworthiness of digital government services: Deriving a comprehensive theory through interpretive structural modelling. *Public Management Review, 20*(5), 647–671.

Kindervag, J. (2010). *Build security into your network's DNA: The zero trust network architecture.* Forrester Research.

Mamodiya, U., & Jain, B. (2025). The next generation of greentech trends and innovations shaping sustainable e-governance. In S. Tanwar (Ed.), *Leveraging Futuristic Machine Learning and Next-Generational Security for E-Governance* (pp. 25–44). IGI Global Scientific Publishing.

MeitY. (2022). *CERT-In security guidelines for government websites — Version 2.0.* Ministry of Electronics and Information Technology, Government of India.

Mishra, A., & Sharma, V. (2022). Vulnerability analysis of Indian government websites: A systematic study of CERT-In disclosures 2019–2022. *International Journal of Information Security, 21*(5), 1103–1122.

NCSC. (2023). *National Cyber Threat Assessment 2023.* National Cyber Security Coordinator's Office, Government of India.

NIST. (2020). *Zero trust architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* National Institute of Standards and Technology.

https://doi.org/10.6028/NIST.CSWP.29

OWASP. (2021). *OWASP Top Ten 2021.* Open Web Application Security Project. https://owasp.org/Top10/ Scott, W. R. (1995). *Institutions and organizations.* Sage.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations, 4*(1), 3–38.

UIDAI. (2023). *Aadhaar annual report 2022–23.* Unique Identification Authority of India, Government of India.

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

World Economic Forum. (2024). *Global Cybersecurity Outlook 2024.* World Economic Forum. https://www.weforum.org/reports/global-cybersecurity-outlook-2024

APPENDIX A: CYBERSECURITY AUDIT MATRIX (CAM) — SELECTED PARAMETERS

#	Domain	Audit Parameter	Standard Ref.	Assessment Method
1	Transport Security	TLS version ≥ 1.2 enforced	NIST CSF PR.DS-2	SSL Labs API scan
2	Transport Security	HSTS header with preload	OWASP ASVS 9.2.1	Security Headers.io
3	Auth & Access	MFA offered for citizen accounts	NIST SP 800-63B	Portal feature review
4	Auth & Access	Session timeout ≤ 30 minutes	OWASP ASVS 3.3.1	Manual testing (public)
5	Input Validation	Content Security Policy header	OWASP Top-10 A03	Security Headers.io
#	Domain	Audit Parameter	Standard Ref.	Assessment Method
6	Input Validation	WAF in place (evidence)	CERT-In Guidelines	Public documentation
7	Data Protection	PII not in URL parameters	OWASP Top-10 A02	Manual review
8	Incident Response	CERT-In 6-hr reporting compliance	CERT-In Directions 2022	Disclosed incidents
9	Governance	ISMS certification evidence	ISO 27001:2022	Public documentation

10	Governance	Responsible disclosure policy	CERT-In CVD Policy	Portal review

Table A1: Sample Parameters from the Cybersecurity Audit Matrix (CAM) — Full matrix available on request

APPENDIX B: E-GOVSHIELD MODEL — SUMMARY REFERENCE CARD

#	Pillar	Core Requirement	Target Actor
P1	Foundational Security Hygiene	HTTPS+TLS1.3; monthly patching; security headers; no default credentials	All government entities
P2	Identity & Access Management	MFA mandate; ZTA; RBAC; PAM for Tier 1	MeitY, NIC, State IT
P3	Application Security Lifecycle	SAST/DAST; annual pen testing; WAF; bug bounty (Tier 1)	NIC, MeitY, Vendors
P4	Data Protection & Privacy Engineering	DPDPA 2023 alignment; AES-256 at rest; PIA for new services	All entities, DPA
P5	Resilience & Incident Response	Documented IRP; SIEM; 6-hr CERT-In reporting; BCP (RTO <4 hrs)	CERT-In, All entities
P6	Governance, Compliance & Accountability	CISO designation; annual CAM audit; security procurement clauses	MeitY, State Govts
P7	Capacity Building & Security Culture	Annual training; SDL; CISO pipeline; research fund	NeGD, DST, CERT-In

Table B1: E-GovShield Seven-Pillar Summary Reference