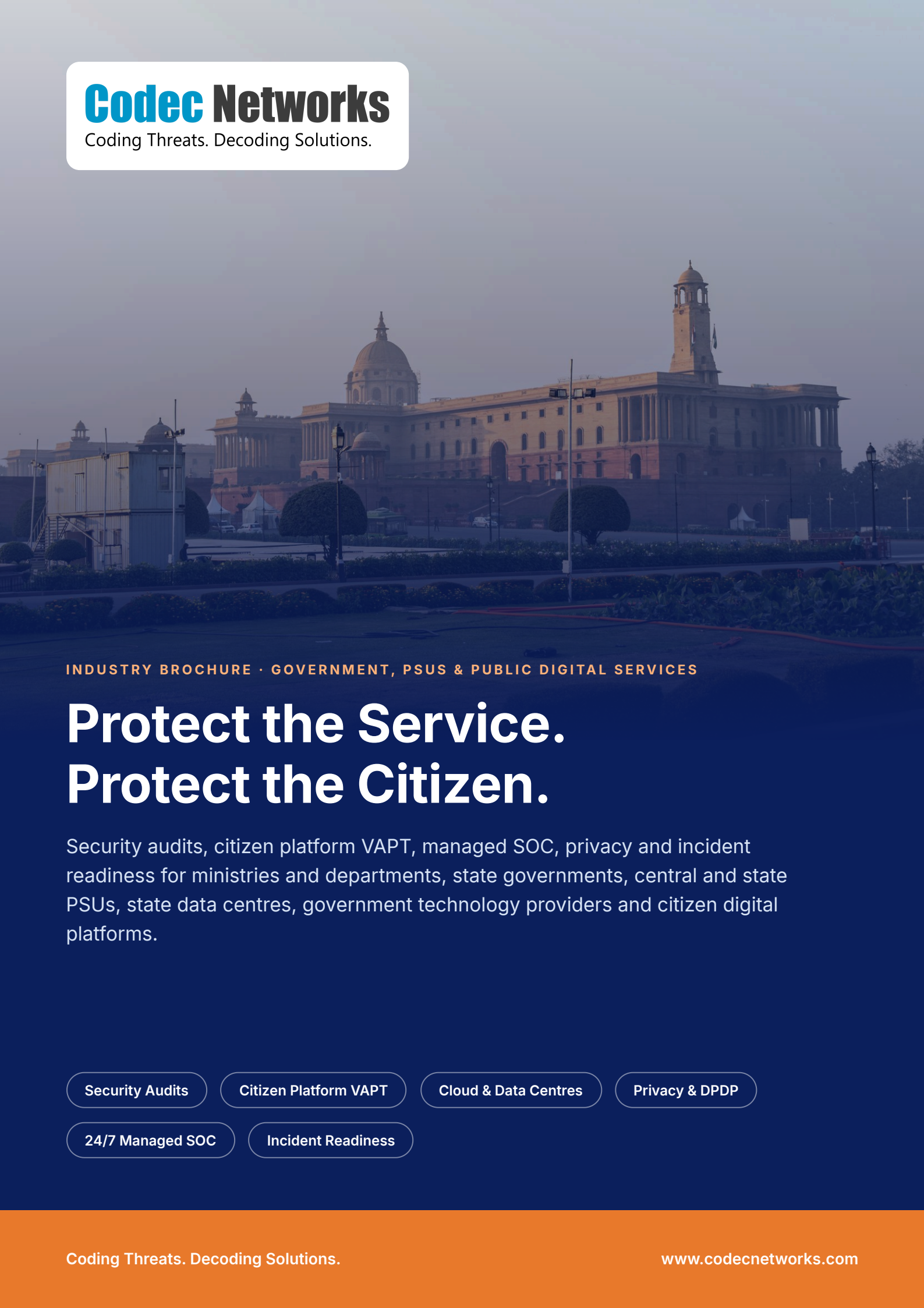




Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · GOVERNMENT, PSUS & PUBLIC DIGITAL SERVICES

Protect the Service. Protect the Citizen.

Security audits, citizen platform VAPT, managed SOC, privacy and incident readiness for ministries and departments, state governments, central and state PSUs, state data centres, government technology providers and citizen digital platforms.

Security Audits

Citizen Platform VAPT

Cloud & Data Centres

Privacy & DPDP

24/7 Managed SOC

Incident Readiness

Coding Threats. Decoding Solutions.

www.codecnetworks.com

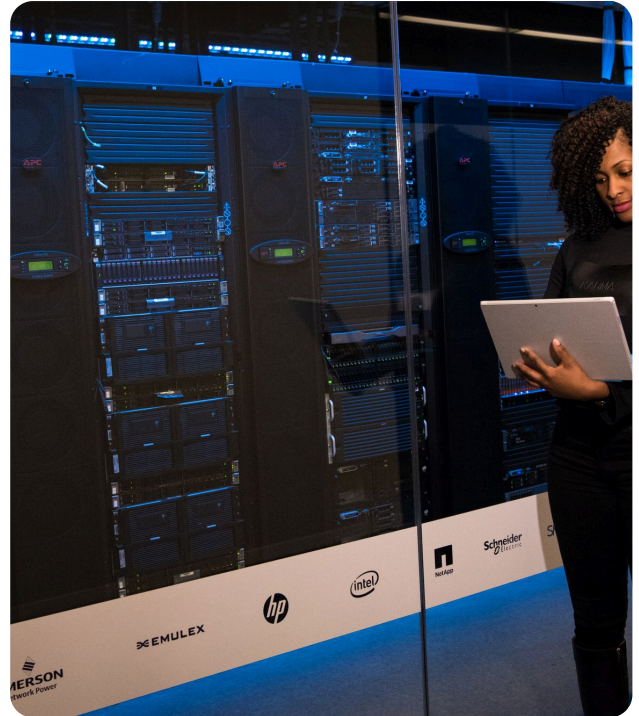
THE CHALLENGE

In government, a cyber incident is a public-service outage.

CERT-In handled over 29.44 lakh cyber incidents in 2025. Ransomware at AIIMS New Delhi in 2022 pushed a national hospital onto manual processes, and a 2023 attack corrupted a state portal serving 413 towns. Ministries and PSUs now need audits, monitoring and rehearsed response.

What keeps leadership teams awake

- Ransomware stopping citizen services
- Citizen data exposed through portals and APIs
- Defacement and DDoS during sensitive events
- Phishing of officials and email takeover
- Vendor and system integrator weaknesses
- Audit, CERT-In and DPDP obligations



29.44 lakh

Cyber incidents handled by CERT-In in 2025

1.3 TB

Data encrypted in the AIIMS New Delhi attack (2022)

231

Audit organisations empanelled by CERT-In (2025)

6 hours

To report cyber incidents to CERT-In

The rulebook has changed

Instrument	What it means for you
CERT-In guidelines for government entities (2023)	Nominated CISO and security team; internal audits every six months, third-party audits at least yearly
CERT-In Directions and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs in India; risk-based independent audits incl. OT/ICS
IT Act Sections 70 and 70A, NCIIPC	Notified protected systems in government, strategic and public enterprises; NCIIPC controls
DPDP Act and Rules (2023, 2025)	Standards for processing by the State; security safeguards; most obligations apply from May 2027

One partner from tender to citizen service

Built around our primary proposition for the sector: **security audits, citizen platform VAPT, managed SOC, privacy and incident readiness.**

Security Audits

- CERT-In guideline compliance audits
- Comprehensive infrastructure audits
- NCIIPC and protected system reviews
- Six-monthly and annual audit cycles

Citizen Platform VAPT

- Portal, app and API security audits
- Security clearance before hosting
- Aadhaar, payment and document flows
- Retests and closure certificates

Cloud & Data Centres

- MeitY-empanelled cloud reviews
- State data centre assessments
- Segmentation and privileged access
- Backup and recovery assurance

Privacy & DPDP

- DPDP gap assessment for departments
- Citizen and beneficiary data mapping
- Vendor and processor contracts
- Breach-intimation workflows

24/7 Managed SOC

- Portal, server and email monitoring
- Defacement and DDoS detection
- Threat hunting for APT activity
- 6-hour CERT-In reporting support

Incident Readiness

- Cyber crisis plans and playbooks
- Tabletop exercises for officials
- Ransomware response and forensics
- Phishing simulation and awareness

Who we serve: ministries and departments · state governments · central and state PSUs · state data centres · government technology providers and system integrators · citizen digital platforms.

Packaged for how government buys

Eleven Codec Networks bundles apply directly to government departments, PSUs and public digital service providers:

B1

Cyber Assessment & VAPT Assurance

B2

Application, API & DevSecOps Security

B3

Cloud, Infrastructure & Zero Trust

B4

Regulatory Cyber Audit & Compliance

B5

GRC, ISO, SOC 2 & PCI DSS Maturity

B6

Data Privacy & DPDPA Program

B7

Managed SOC, MDR & Threat Monitoring

B8

Forensics, Incident Response & Malware RCA

B9

Third-Party & Supply-Chain Risk

B10

Cyber Simulation, Awareness & Tabletop

B11

Emerging Tech, AI & Web3 Security

Foundation

Departments, autonomous bodies and smaller PSUs

- Website and application security audits
- Infrastructure VAPT and hardening
- CERT-In guideline gap review
- Phishing awareness for officials

Assurance

State governments, large departments and PSUs

- Six-monthly and annual audit programme
- Citizen portal, app and API testing
- DPDP programme for citizen data
- 24x7 managed SOC

Continuous Resilience

Data centres, citizen platforms and strategic PSUs

- Continuous testing and red teaming
- NCIIPC-aligned and OT reviews
- SOC with threat hunting
- Crisis exercises and IR retainer

Mapped to your obligations

Requirement	How we help	Bundle
Incidents to CERT-In in six hours; 180-day logs (CERT-In Directions)	SOC, IR retainer, reporting support	B7, B8
Six-monthly internal, yearly third-party audits (CERT-In, 2023)	Audit programme, closure tracking	B4, B1
Risk-based independent audits (CERT-In audit guidelines, 2025)	Comprehensive and OT audits	B4, B1
Controls for notified protected systems (IT Act s.70, NCIIPC)	Control reviews, segmentation, SOC	B4, B3
Secure government websites and apps (GIGW 3.0)	Pre-hosting audits and retests	B2, B1
Citizen and employee data safeguards (DPDP Act and Rules)	DPDPA programme for departments	B6
Security duties for vendors and integrators (contracts, CERT-In)	Vendor audits, contract clauses	B9, B4

Why government departments and PSUs choose Codec Networks

CERT-In empanelled

Information security audits recognised in government and PSU tenders.

NICSI empanelled

Empanelled for application audit and compliance services (start-up category).

Public-sector experience

Serving central ministries, state governments and public-sector undertakings.

Certified and accountable

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018 certified.

Full stack, one partner

Audit, testing, privacy, SOC and forensics connected from finding to closure.

Certified experts

CISA, ISO 27001 LA/LI, CEH, OSCP and CHFI professionals.

How we engage

Discover & scope

Citizen portals, apps and APIs, data centres and clouds, e-Office and email, ERP and finance systems, plant and OT networks, vendors and system integrators, and the audit and reporting obligations that apply to you.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next portal launch, national event and audit a non-event.

Tell us your departments, platforms, data centres and obligations. We will propose a practical, CERT-In-aligned audit, monitoring and readiness plan.

New Delhi

507, 5th Floor, New Delhi House, Barakhamba
Road, Connaught Place, New Delhi – 110001

Gurugram

707, 7th Floor, Silverton Tower, Golf Course
Extension Road, Sector 50, Gurugram – 122018,
Haryana

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003
31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: PIB (CERT-In 2025 figures, January 2026), Rajya Sabha replies on AIIMS New Delhi (December 2022), CERT-In. Confirm obligations against the official instruments.