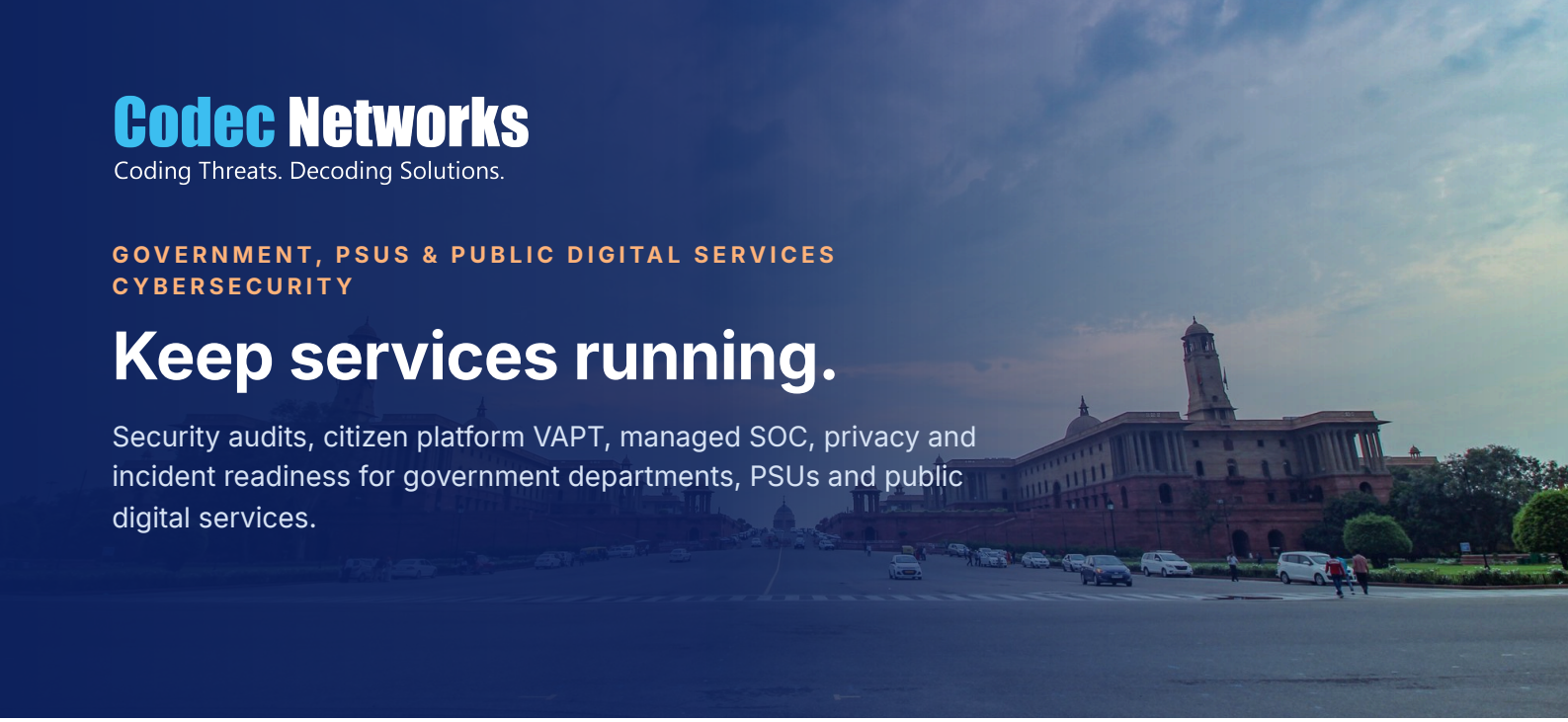
Codec Networks
Coding Threats. Decoding Solutions.

GOVERNMENT, PSUS & PUBLIC DIGITAL SERVICES CYBERSECURITY

Keep services running.

Security audits, citizen platform VAPT, managed SOC, privacy and incident readiness for government departments, PSUs and public digital services.



Three questions every department head should be able to answer

Could ransomware stop our citizen services tomorrow?
Segmentation, offline backups and rehearsed recovery decide whether an attack is an outage of hours or of weeks.

Can one citizen see another's records on our portal?
Authorisation testing of every portal, app and API decides whether a scraper becomes a data breach.

Would we report an incident to CERT-In within six hours?
24x7 monitoring, a named CISO and tested playbooks decide whether the clock is met or missed.

29.44 lakh
Incidents handled by CERT-In in 2025

1.3 TB
Encrypted in the AIIMS attack (2022)

231
CERT-In empanelled audit organisations

6 hours
Incident reporting to CERT-In

Built for every level of government

Ministries and departments · state governments · central and state PSUs · state data centres · government technology providers and system integrators · citizen digital platforms.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In guidelines · Directions · audit policy (2022–2025)	Named CISO; six-monthly and yearly audits; 6-hour reporting
IT Act s.70 · NCIIPC · GIGW 3.0	Protected systems; secure government websites and apps
DPDP Act and Rules (2023, 2025)	Standards for State processing; safeguards; breach intimation

WHAT WE DO

Audits, VAPT, cloud, privacy, SOC and readiness

Security Audits
CERT-In guideline, comprehensive, NCIIPC-aligned and OT audits.

Citizen Platform VAPT
Portal, app and API testing, pre-hosting audits, retests and closure.

Cloud & Data Centres
MeitY cloud, state data centre, segmentation and backup reviews.

Privacy & DPDP
Citizen and beneficiary data, vendor contracts, breach workflows.

24/7 Managed SOC
Portal, server and email monitoring, defacement alerts, 6-hour reporting.

Incident Readiness
Crisis plans, tabletop exercises, ransomware response and forensics.

Choose your starting point

Foundation
Website and application audits, infrastructure VAPT, CERT-In guideline gap review, phishing awareness. For departments, autonomous bodies and smaller PSUs.

Assurance
Six-monthly and annual audit programme, citizen portal and API testing, DPDP programme, managed SOC. For state governments, large departments and PSUs.

Continuous Resilience
Continuous testing and red teaming, NCIIPC-aligned and OT reviews, SOC with hunting, crisis exercises and IR retainer. For data centres, citizen platforms and strategic PSUs.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

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

Regulation-mapped
Every finding mapped to CERT-In guidelines and Directions, NCIIPC controls, GIGW 3.0, DPDP, ISO/IEC 27001 and your tender and audit obligations.

One connected partner
Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share 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 – 110001
Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018
Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220
Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. 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.