

Codec Networks

Coding Threats. Decoding Solutions.

GOVERNMENT, PSUS & PUBLIC DIGITAL
SERVICES

Protect the Service. Protect the Citizen.

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

Coding Threats. Decoding Solutions. · www.codecnetworks.com



What we will cover



The sector and its risks

Scale, players and the threats that matter most



What regulators now expect

CERT-In guidelines and Directions, NCIIPC, GIGW 3.0 and DPDP



How Codec Networks helps

Services, bundles and packages built for the sector



Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Government and PSUs are a high-impact target

Official figures and statements show what is at stake

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

What this means: government departments, PSUs and public digital services must keep citizen services available, audit their systems on a fixed cycle with CERT-In empanelled auditors, protect citizen and employee data under DPDP, secure protected systems and plant networks, hold vendors to account, and report incidents within six hours.

Sources: PIB (CERT-In 2025 figures), Rajya Sabha replies on AIIMS New Delhi (December 2022), CERT-In.

Who we serve across government and the public sector



Central ministries and departments

Policy, schemes, e-Office, portals



State governments

Citizen services, treasuries, police



Central PSUs

Energy, engineering, telecom, finance



State PSUs and utilities

Power, water, transport, corporations



State data centres and clouds

Hosting, SWAN, government clouds



GovTech providers

Integrators, developers, AMC



Citizen digital platforms

Identity, documents, payments, apps



Health and municipal services

Hospitals, municipal bodies, police

The threats that cost the public sector the most

Six priorities from our 18-threat government and PSU assessment



Ransomware

Hospital and e-governance servers



Citizen data exposure

Portals, APIs and scraped records



State-linked espionage

Spear-phishing of officials



Defacement and DDoS

Hacktivists during sensitive events



Vendor and SI compromise

Developers, AMC and hosting partners



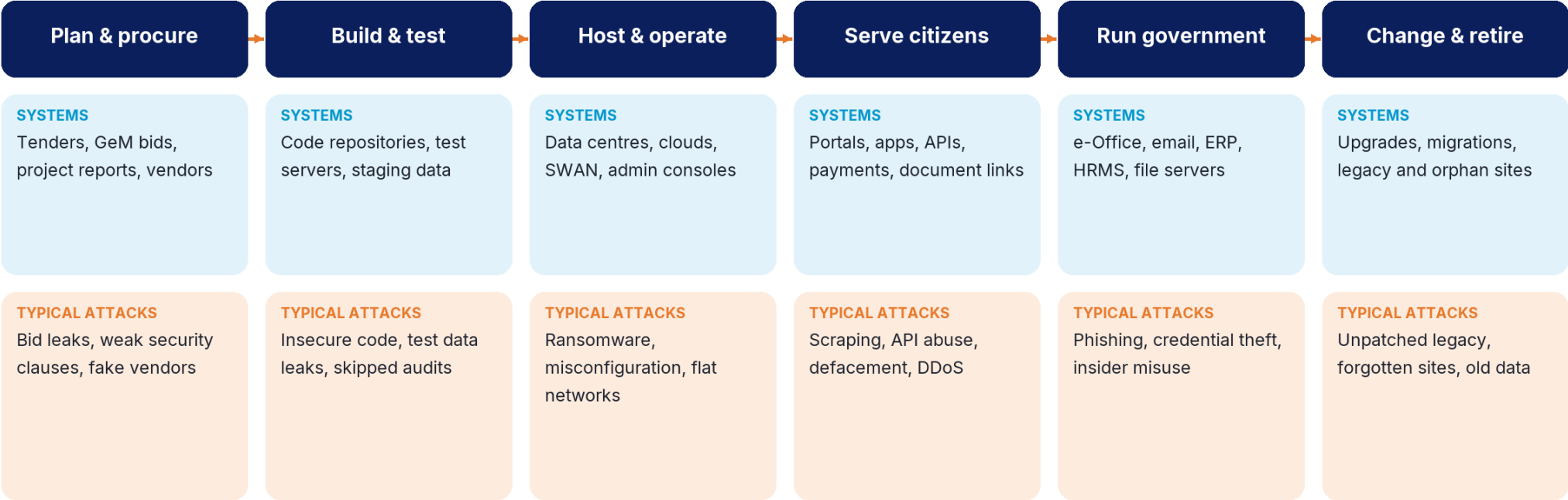
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage from tender to citizen service

Where Cyber Risk Sits Across the Public Digital Service Lifecycle

Every stage from tender to retirement carries its own attack surface



In government, availability and trust are the service: a stalled hospital system, a defaced portal or a leaked beneficiary list becomes a public event within hours.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In guidelines and Directions, NCIIPC, GIGW 3.0 and DPDP

The rules shaping government and PSU cybersecurity

Requirement	Frequency / deadline	Source
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
ICT log retention	180 days, in India	CERT-In Directions, 2022
CISO and security team	Nominated CISO, separate security team	CERT-In government guidelines, 2023
Security audits	Internal six-monthly, third-party yearly	CERT-In government guidelines, 2023
Independent cyber audits	Risk-based, incl. OT/ICS	CERT-In audit guidelines, 2025
Protected systems	NCIIPC controls for notified CII	IT Act, Sections 70 and 70A
Government websites and apps	Quality, accessibility, cybersecurity	GIGW 3.0, 2023
Citizen and employee data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Government cloud hosting	Empanelled providers, STQC audit	MeitY cloud empanelment

Key dates on the regulatory timeline

Policy and Regulatory Timeline Shaping Government and PSU Cybersecurity

Cyber, audit, platform and privacy instruments that reach ministries, states, PSUs and their vendors

● In force

● Upcoming (from Oct 2026)

2000	● Information Technology Act, 2000; Sections 70A (NCIIPC) and 70B (CERT-In) added in 2008
Jul 2013	● National Cyber Security Policy 2013 calls for a 24x7 NCIIPC and security audits
Jan 2014	● NCIIPC notified under Section 70A as nodal agency for critical information infrastructure
Jan 2018	● MeitY launches Cyber Surakshit Bharat to train government CISOs and IT officials
Apr 2022	● CERT-In Directions: 6-hour reporting and 180-day logs, incl. government organisations
Nov 2022	● Ransomware at AIIMS New Delhi encrypts five servers hosting the e-Hospital application
2023	● GIGW 3.0 for government websites and apps, with a cybersecurity chapter by CERT-In
Jun 2023	● CERT-In Guidelines on Information Security Practices for Government Entities issued
Aug 2023	● DPDP Act, 2023 enacted, with provisions on processing by the State in Sections 7 and 17
Jul 2025	● CERT-In Comprehensive Cyber Security Audit Policy Guidelines, incl. OT/ICS
Nov 2025	● DPDP Rules notified, incl. standards for processing by the State and its instrumentalities
May 2027	● Most DPDP Rules obligations, incl. security safeguards and breach intimation, apply

Sources: MeitY, CERT-In, NCIIPC, NeGD, Rajya Sabha replies, Gazette of India. Confirm against the official instruments.

Codec Networks

How Codec Networks helps

Security audits · Citizen platform VAPT · Cloud & data centres · Privacy · Managed SOC · Incident readiness

One partner from tender to citizen service



Security Audits

CERT-In guideline audits



Citizen Platform VAPT

Portals, apps, APIs



Cloud & Data Centres

Clouds, SDCs, segmentation



Privacy & DPDP

Citizen and employee data



24/7 Managed SOC

Detection and reporting



Incident Readiness

Plans, drills, forensics

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services



Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Departments, autonomous bodies and smaller PSUs

- Website and application audits (B2)
- Infrastructure VAPT and hardening (B1)
- CERT-In guideline gap review (B4)
- Phishing awareness for officials (B10)

Assurance

State governments, large departments and PSUs

- Six-monthly and annual audits (B4, B1)
- Citizen portal and API testing (B2)
- DPDP programme (B6)
- 24x7 managed SOC (B7)

Continuous Resilience

Data centres, citizen platforms and strategic PSUs

- Continuous testing and red teaming (B1, B10)
- NCIIPC-aligned and OT reviews (B4, B3)
- SOC with threat hunting (B7)
- Crisis exercises and IR retainer (B10, B8)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

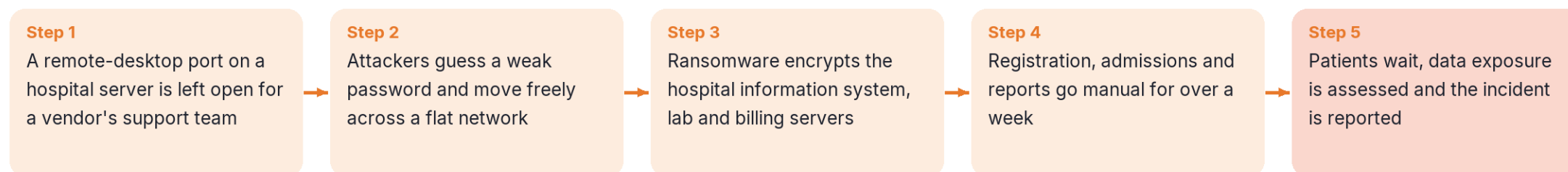
Illustrative composite scenarios written for 2026—not client engagements

1	The Hospital That Went Back to Paper	An open vendor remote-access port lets ransomware cross a flat network; segmentation and SOC stop it	B3 · B7 · B8
2	The Certificate Portal That Said Too Much	A sequential-ID API flaw exposes lakhs of citizen records; authorisation testing closes it	B2 · B1 · B6
3	The Circular That Was Not From the Ministry	A spoofed circular plants a backdoor at a central PSU; email controls and threat hunting catch it	B7 · B10 · B8
4	One Vendor Account, Twelve Portals	One integrator's weak password compromises twelve department portals; vendor controls stop it	B9 · B2 · B7
5	The Night Forty Websites Were Defaced	Hacktivists exploit old CMS sites in a state data centre; inventory, patching and monitoring contain it	B1 · B7 · B10

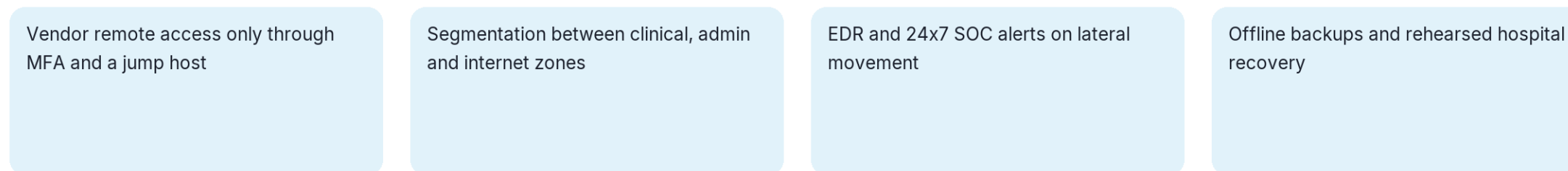
Example: breaking a hospital ransomware chain

Case 1: The Hospital That Went Back to Paper

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: whether vendor remote access is forced through MFA and a jump host, whether clinical, administrative and internet zones are segmented, whether the SOC sees lateral movement and mass encryption early, whether backups are offline and restorable within hours, and how hospital leadership handles manual operations, patient communication and CERT-In reporting in a tabletop exercise.

Why government and PSUs choose Codec Networks



CERT-In empanelled

For information security auditing services; NICS empanelled for application audits



Certified

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



Regulation-mapped

Mapped to CERT-In guidelines and Directions, NCIIPC controls, GIGW 3.0, DPDP and ISO/IEC 27001



Tests the whole chain

Technical, process and monitoring tests together



Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected



Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST



How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement



Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTDD and MTTR metrics

Let's start with a scoping session

1 Scoping session

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 audit and reporting obligations

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

 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

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

 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.