



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · CLOUD, DATA CENTRES & HOSTING

Run the Cloud Others Trust. Prove It Every Day.

Cloud configuration reviews, virtualisation security, SOC, resilience and customer assurance for cloud providers, colocation operators, managed hosting and VPS and infrastructure providers.

Cloud Configuration Reviews

Virtualisation Security

24/7 SOC

Resilience Testing

Customer Assurance

Facility OT Security

Coding Threats. Decoding Solutions.

www.codecnetworks.com

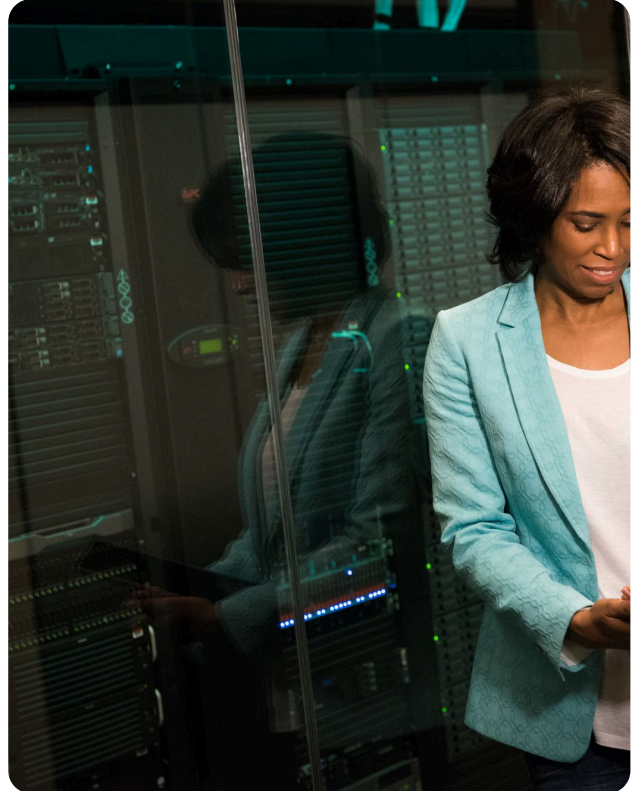
THE CHALLENGE

Thousands of customers run on you. Attackers target the platform.

Cloud, data centre and hosting providers run the hypervisors, control planes and facilities that regulated and government customers depend on. CERT-In's Directions set specific duties for cloud, VPS and data centre providers, and customers' regulators require assured, empanelled cloud services.

What keeps leadership teams awake

- Hypervisor ransomware taking down many customers at once
- Control-plane and console takeover
- Exposed out-of-band management interfaces
- Platform abuse for phishing and attacks
- Facility BMS and OT compromise
- Customer audits, empanelment and CERT-In record-keeping



6 hours

To report cyber incidents to CERT-In

5 years

Subscriber records kept by cloud and VPS providers (CERT-In)

180 days

ICT logs to be kept in India

May 2027

Most DPDP obligations take effect

The rulebook has changed

Instrument	What it means for you
CERT-In Directions (28 Apr 2022)	6-hour incident reporting, 180-day logs, clock synchronisation, and 5-year subscriber records for data centres, cloud and VPS providers
Customer regulator cloud rules	MeitY empanelment with STQC audit; SEBI cloud framework (2023); RBI and IRDAI cloud and outsourcing requirements
DPDP Act & Rules	Safeguards for customer personal data; breach intimation from May 2027
Standards and contracts	ISO/IEC 27001, 27017, 27018, SOC 2, PCI DSS where card data is hosted; SLAs and audit rights

One partner from facility to control plane

Built around our primary proposition for the sector: **cloud configuration reviews, virtualisation security, SOC, resilience and customer assurance.**

Cloud Configuration Reviews

- Control-plane and IAM reviews
- Customer-facing console and API testing
- Secure defaults and sharing settings
- Tenant isolation assessments

Virtualisation Security

- Hypervisor and management-plane hardening
- BMC, IPMI and firmware security
- VM isolation and escape testing
- Backup architecture reviews

24/7 SOC

- Platform and management-plane monitoring
- Abuse and DDoS detection
- Facility OT and BMS monitoring
- 6-hour CERT-In reporting support

Resilience

- Ransomware and outage simulations
- DR and failover testing
- Immutable backup validation
- Crisis and customer communication drills

Customer Assurance

- ISO 27001, 27017 and 27018 readiness
- SOC 2 readiness
- MeitY empanelment and STQC audit support
- Customer audit evidence packs

Facility OT Security

- BMS, power and cooling segmentation
- Vendor remote-access reviews
- Physical security assessments
- OT incident playbooks

Who we serve: cloud service providers · colocation and data centre operators · managed hosting providers · VPS, bare-metal and infrastructure providers · edge and GPU cloud providers · sovereign and government cloud operators.

Packaged for how providers buy

Eleven Codec Networks bundles apply directly to cloud, data centre and hosting 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

Smaller hosting and VPS providers

- Control-plane and console VAPT
- Hypervisor and BMC hardening review
- CERT-In record-keeping gap check
- ISO 27001 gap assessment

Assurance

Mid-sized clouds and colocation

- Virtualisation and tenant isolation testing
- Facility OT and BMS review
- ISO 27017/27018 and SOC 2 readiness
- 24x7 managed SOC

Continuous Resilience

Large and sovereign cloud providers

- Continuous testing and red teaming
- Empanelment and regulator audit support
- SOC with platform and abuse signals
- Customer and Board reporting

Mapped to your obligations

Requirement	How we help	Bundle
Cyber incidents to CERT-In within six hours; 180-day logs (CERT-In Directions)	SOC monitoring, IR retainer and reporting support	B7, B8
Subscriber records for 5 years; clock synchronisation (CERT-In Directions)	Record-keeping and logging gap assessment	B4
MeitY cloud empanelment with STQC audit	Empanelment readiness and audit support	B4, B5
SEBI, RBI and IRDAI cloud requirements for customers	Customer assurance evidence and audits	B4, B5
Secure virtualisation and tenant isolation	Virtualisation and isolation testing	B1, B3
DPDP safeguards for customer personal data	DPDPA programme and data handling review	B6
Resilience and recovery commitments (SLAs)	DR, failover and ransomware simulations	B10

Why infrastructure providers choose Codec Networks

CERT-In empanelled

Independent audits and testing recognised by customers and regulators.

Certified and accountable

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

Platform depth

Hypervisors, control planes, BMC and facility OT tested end to end.

Customer-ready evidence

Reports and certifications that answer regulated customers' audits.

Full stack, one partner

Testing, SOC, forensics, resilience and privacy connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Service model, facilities, virtualisation stack, customer sectors and your empanelment and audit calendar.

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 audit, empanelment and incident a non-event.

Tell us your platform, facilities and customers. We will propose a practical, regulation-mapped assessment and assurance 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: CERT-In Directions (28 April 2022), MeitY. Confirm obligations against the official instruments.