Codec Networks
Coding Threats. Decoding Solutions.

CLOUD, DATA CENTRES & HOSTING CYBERSECURITY

Resilient platforms. Assured customers.

Cloud configuration reviews, virtualisation security, SOC, resilience and customer assurance for cloud, data centre and hosting providers.

Three questions every infrastructure leader should be able to answer

Could one exploit encrypt every customer?
Hypervisors and management planes must be isolated, patched and monitored, with backups outside their reach.

Are we meeting CERT-In's provider duties?
Data centres, cloud and VPS providers must keep subscriber records for five years, sync clocks and keep 180-day logs.

Could we report an incident within six hours?
CERT-In requires reporting within six hours of noticing an incident; customers expect prompt notice too.

6 hours
Incident reporting to CERT-In

5 years
Subscriber record retention

180 days
ICT log retention in India

May 2027
Most DPDP obligations take effect

Built for every infrastructure provider

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.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions (Apr 2022)	6-hour reporting, 180-day logs, clock sync, 5-year subscriber records
Customer regulator cloud rules	MeitY empanelment with STQC audit; SEBI, RBI and IRDAI cloud requirements
DPDP · standards	Customer data safeguards; ISO 27001/27017/27018, SOC 2

WHAT WE DO

Cloud configuration, virtualisation, SOC, resilience and assurance

Cloud Configuration Reviews
Control plane, IAM, consoles, APIs and secure defaults.

Virtualisation Security
Hypervisors, management planes, BMC, firmware and isolation.

24/7 SOC
Platform, abuse, DDoS and facility OT monitoring with 6-hour reporting support.

Resilience
Ransomware and outage simulations, DR and backup validation.

Customer Assurance
ISO 27001/27017/27018, SOC 2, empanelment and audit evidence.

Facility OT Security
BMS, power and cooling segmentation, vendor access, physical security.

Choose your starting point

Foundation
Control-plane VAPT, hypervisor and BMC hardening, CERT-In record-keeping check, ISO 27001 gap. For smaller hosting and VPS providers.

Assurance
Virtualisation and isolation testing, facility OT review, ISO 27017/27018 and SOC 2, managed SOC. For mid-sized clouds and colocation.

Continuous Resilience
Continuous testing and red teaming, empanelment and audit support, SOC with platform signals, customer reporting. For large clouds.

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, MeitY, customer regulator and DPDP requirements.

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

Book a scoping session

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