Codec Networks

Coding Threats. Decoding Solutions.

ITES, BPO, KPO & GCCS CYBERSECURITY

Every customer protected. Every seat trusted.

Customer data protection, access reviews, DLP assessments, SOC, privacy and insider threat investigations for ITeS, BPO and GCCs.

Three questions every service-centre leader should be able to answer

What can each agent see and copy?

Masking, least privilege and DLP decide whether one bribed agent becomes a mass breach.

Could our help desk be talked into a reset?

Password and MFA resets need strong identity checks and out-of-band approval.

Could we report an incident within six hours?

CERT-In requires reporting within six hours of noticing an incident; clients expect prompt notice too.

6 hours
Incident reporting to CERT-In

Mar 2025
PCI DSS v4.0 fully mandatory

180 days
ICT log retention in India

May 2027
Most DPDP obligations take effect

Built for every service centre

Contact centres · BPO back-office operations · KPO and analytics firms · shared service centres · global capability centres · outsourced processing businesses.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent cyber audits
DPDP · client requirements	Processor safeguards; RBI, SEBI, IRDAI outsourcing controls; PCI DSS v4.0
Overseas and telemarketing rules	GDPR, HIPAA and client-country laws; TRAI telemarketing rules

WHAT WE DO

Customer data, access, DLP, SOC, privacy and insider investigations

Customer Data Protection
Screen masking, secure floors, VDI and PCI DSS scoping.

Access Reviews
Client system recertification, shared accounts, help-desk reset controls.

DLP Assessments
Endpoint, email, USB, print, screen-capture and WFH leakage testing.

24/7 SOC
Managed SOC with UEBA, identity attack detection and 6-hour reporting support.

Privacy & DPDPA
Processor privacy programmes, GDPR and HIPAA mapping, breach workflows.

Insider Investigations
Forensic investigation of data theft, bribery and collusion.

Choose your starting point

Foundation
Access review and clean-up, DLP quick assessment, ISO 27001 gap assessment, agent awareness. For smaller BPOs and KPOs.

Assurance
Client audit and PCI DSS readiness, DLP and WFH assessment, help-desk controls, managed SOC. For mid-sized BPOs and SSCs.

Continuous Resilience
Red teaming and insider simulations, zero-trust access, SOC with UEBA, client and parent reporting. For large BPOs and GCCs.

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, DPDP, client, PCI DSS and overseas requirements.

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

Book a scoping session

Share your clients, processes and delivery model. We will propose a practical 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, MeitY, PCI Security Standards Council. Confirm obligations against the official instruments.