Codec Networks
Coding Threats. Decoding Solutions.



INDUSTRY BROCHURE · ITES, BPO, KPO & GCCS

Protect Every Customer. Trust Every Seat.

Customer data protection, access reviews, DLP assessments, SOC, privacy and insider threat investigations for contact centres, shared service centres, GCCs and outsourced processing businesses.

Customer Data Protection | Access Reviews | DLP Assessments | 24/7 SOC | Privacy & DPDPA | Insider Investigations

THE CHALLENGE

Your people see client data all day. Attackers know it.

ITeS, BPO, KPO and GCC teams handle customer records, payments and privileged systems for clients and parent companies worldwide. Clients pass their regulators' and auditors' requirements straight to the delivery floor.



What keeps leadership teams awake

- Agents bribed or recruited to leak customer data
- Help desks tricked into resetting passwords and MFA
- Fraudulent payment and account changes
- Work-from-home devices holding customer data
- Client audits, PCI DSS and parent-company standards
- CERT-In, DPDP and overseas privacy laws

6 hours
To report cyber incidents to CERT-In

Mar 2025
PCI DSS v4.0 future-dated requirements mandatory

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 and audit guidelines (2022, 2025)	6-hour incident reporting, 180-day logs; risk-based independent cyber audits
DPDP Act & Rules	Processing client customers' data with reasonable security safeguards; breach intimation from May 2027
Client and card-industry requirements	RBI, SEBI and IRDAI outsourcing controls; PCI DSS v4.0 for card data; client audit rights
Overseas privacy and telemarketing rules	GDPR, HIPAA and other client-country laws; TRAI rules for outbound telemarketing

OUR SERVICE OFFERINGS

One partner across every seat and process

Built around our primary proposition for the sector: **customer data protection, access reviews, DLP assessments, SOC, privacy and insider threat investigations.**

Customer Data Protection

- Screen masking and data minimisation
- Clean-desk and secure-floor controls
- VDI and secure workstation reviews
- PCI DSS scoping for card data

Access Reviews

- Client system and CRM access recertification
- Shared and orphaned account clean-up
- Privileged access to parent systems
- Help-desk reset controls

DLP Assessments

- Endpoint, email and web DLP testing
- USB, print and screen-capture controls
- Work-from-home leakage reviews
- Policy tuning and exception review

24/7 SOC

- Managed SOC with SIEM and EDR/XDR
- UEBA for unusual look-ups and exports
- Help-desk and identity attack detection
- 6-hour CERT-In reporting support

Privacy & DPDPA

- Processor privacy programmes
- GDPR and HIPAA control mapping
- Retention and deletion controls
- Breach response workflow

Insider Threat Investigations

- Forensic investigation of data theft
- Evidence handling for HR and legal
- Bribery and collusion analysis
- Root-cause and control fixes

Who we serve: contact centres · BPO back-office operations · KPO and analytics firms · shared service centres · global capability centres · outsourced processing businesses.

BUNDLED SERVICE MODELS

Packaged for how service centres buy

Eleven Codec Networks bundles apply directly to ITeS, BPO, KPO and GCC organisations:

- **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 BPOs and KPOs

- Access review and account clean-up
- DLP quick assessment
- ISO 27001 gap assessment
- Security awareness for agents

Assurance

Mid-sized BPOs and shared service centres

- Client audit and PCI DSS readiness
- DLP and WFH assessment
- Help-desk reset controls review
- 24x7 managed SOC

Continuous Resilience

Large BPOs and GCCs

- Red teaming and insider simulations
- Zero-trust access for agents
- SOC with UEBA and insider signals
- Client, parent 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
Processing client customers' personal data with safeguards (DPDP)	Processor privacy programme and DLP	B6
Client regulator outsourcing controls (RBI, SEBI, IRDAI)	Client audit readiness and evidence	B4, B5
PCI DSS v4.0 for card data in contact centres	PCI DSS scoping and readiness	B4, B5
Access control and least privilege	Access reviews and recertification	B3
Overseas client privacy laws (GDPR, HIPAA)	Control mapping and audit support	B6
Insider threat and misuse	UEBA monitoring and investigations	B7, B8

THE CODEC NETWORKS VALUE ADD

Why service centres choose Codec Networks

CERT-In empanelled

Independent audits and testing that clients and parent companies recognise.

Certified and accountable

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

People-centric depth

Access, DLP, help-desk and insider controls tested on the delivery floor.

Client-ready evidence

Reports and closure evidence that answer client audits.

Investigations capability

Forensic insider investigations with evidence fit for HR and legal action.

Certified experts

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

How we engage

Discover & scope

Client sectors, processes, data handled, delivery model including WFH, and your client 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 client audit, floor walk and incident a non-event.

Tell us 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, 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, MeitY, PCI Security Standards Council. Confirm obligations against the official instruments.