

Codec Networks

Coding Threats. Decoding Solutions.

ITES, BPO, KPO & GCCS

Protect Every Customer. Trust Every Seat.

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

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, DPDP, client flow-down, PCI DSS and overseas laws



How Codec Networks helps

Services, bundles and packages built for the sector



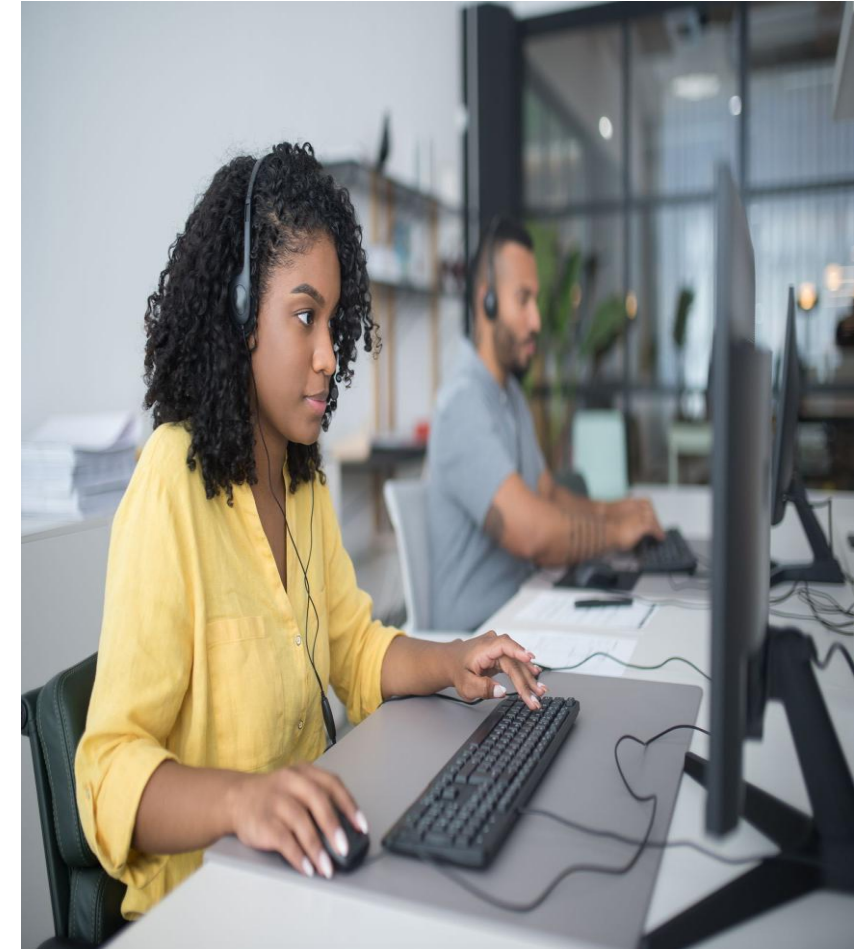
Proof in scenarios

Five new case studies and the controls that break the chain



Why Codec Networks and next steps

Our value add and how to start



Clients bring their rules to your delivery floor

CERT-In, DPDP, PCI DSS and client regulators shape what centres must prove

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

What this means: service centres must limit what each person can see and copy, harden help desks, monitor for insider misuse and report incidents within six hours—while proving controls to clients and parent companies.

Sources: CERT-In, MeitY, PCI Security Standards Council.

Who we serve across ITeS, BPO, KPO and GCCs



Contact centres

Voice, chat and email support



BPO back-office

Claims, payments, records



KPO and analytics

Research and knowledge services



Shared service centres

Finance, HR, procurement



Global capability centres

Captive hubs of global firms



Collections and telemarketing

Outbound operations



Healthcare and insurance BPO

Medical billing and claims



Work-from-home teams

Distributed delivery

The threats that cost service centres the most

Six priorities from our 18-threat ITeS and GCC assessment



Insider data theft

Bribed or recruited agents



Help-desk social engineering

Resets for the wrong person



Payment fraud

Vendor and account changes



Customer data leakage

Screens, files and devices



Ransomware

Client and parent systems



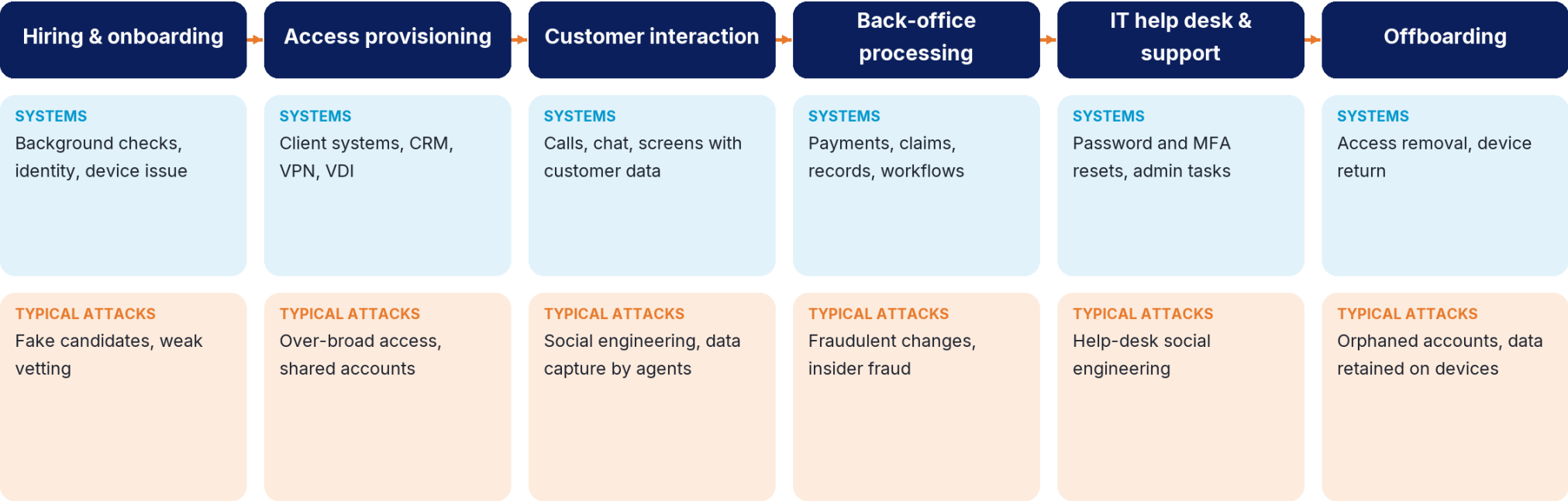
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage of service delivery

Where Cyber Risk Sits in Service Delivery

Every stage of an outsourced process carries its own attack surface



In people-intensive operations, the biggest control is what each person can see, copy and change.

Source: Codec Networks analysis

Codec Networks

What regulators now expect

CERT-In, DPDP, client flow-down, PCI DSS and overseas laws

The rules that reach the delivery floor

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
Independent cyber audits	Risk-based	CERT-In audit guidelines, 2025
Processing client customers' data	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Outsourcing controls for regulated clients	Per contract	RBI, SEBI, IRDAI rules
Card data in contact centres	v4.0 fully mandatory since Mar 2025	PCI DSS
Overseas customer data	Per client country	GDPR, HIPAA and others
Outbound telemarketing	Registration and consent rules	TRAI regulations

Key dates on the regulatory timeline

Regulatory Timeline Shaping ITeS, BPO and GCC Security

Indian, international and client-driven instruments

● In force ● Upcoming (from Oct 2026)

2018	●	TRAI telecom commercial communications regulations for telemarketing
Nov 2020	●	DoT liberalised Other Service Provider (OSP) guidelines
Apr 2022	●	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Aug 2023	●	Digital Personal Data Protection Act, 2023 enacted
Mar 2025	●	PCI DSS v4.0 future-dated requirements become mandatory
Nov 2025	●	DPDP Rules, 2025 notified with phased commencement
May 2027	●	Most DPDP Rules obligations, incl. breach intimation, take effect

Sources: CERT-In, MeitY, DoT, TRAI, PCI SSC. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

Customer data · Access reviews · DLP · SOC · Privacy · Insider investigations

One partner across every seat and process



Customer Data Protection

Masking, secure floors, VDI, PCI DSS



Access Reviews

Recertification, shared accounts, resets



DLP Assessments

Endpoint, email, USB, screen capture, WFH



24/7 SOC

UEBA, identity attacks, 6-hour reporting



Privacy & DPDPA

Processor programmes, GDPR, HIPAA



Insider Investigations

Forensics, bribery and collusion

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

Smaller BPOs and KPOs

- Access review (B3)
- DLP quick assessment (B6)
- ISO 27001 gap assessment (B5)
- Agent awareness (B10)

Assurance

Mid-sized BPOs and shared service centres

- Client audit and PCI DSS (B4, B5)
- DLP and WFH assessment (B6)
- Help-desk controls review (B3)
- 24x7 managed SOC (B7)

Continuous Resilience

Large BPOs and GCCs

- Red teaming and insider simulations (B1, B10)
- Zero-trust access (B3)
- SOC with UEBA (B7)
- Client, parent and Board reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1

The Agent Who Sold Screenshots

Recruited agents photograph customer records; masking and UEBA stop it

B6 · B7 · B8

2

The Help Desk That Reset the Wrong MFA

A caller talks the help desk into a reset; strong verification stops it

B3 · B10 · B7

3

The Vendor Master Change in Shared Services

A fake bank letter diverts a payment run; call-backs and maker-checker stop it

B10 · B4 · B7

4

The Home Laptop That Kept Customer Files

A stolen WFH laptop exposes data; VDI, encryption and DLP prevent it

B3 · B6 · B8

5

The GCC Account That Reached Headquarters

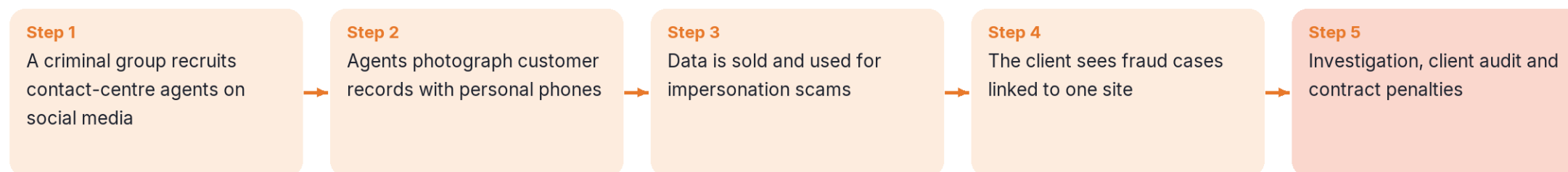
A GCC admin account opens the parent's network; tiered admin stops it

B3 · B7 · B8

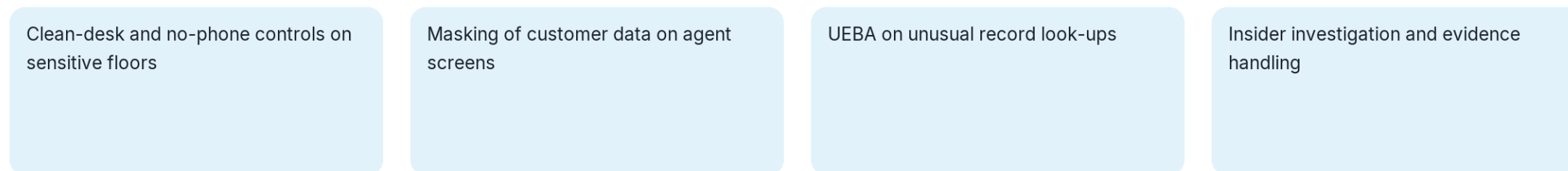
Example: breaking an insider data-theft chain

Case 1: The Agent Who Sold Screenshots

ILLUSTRATIVE ATTACK PATH



WHERE CONTROLS BREAK THE CHAIN



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

Codec Networks

What we test: clean-desk and no-phone controls, screen masking and least privilege in CRM, UEBA on unusual look-ups, DLP coverage, and the investigation and CERT-In reporting steps.

Why service centres choose Codec Networks



CERT-In empanelled

For information security auditing services; NISCI empanelled for application audits



Certified

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



Regulation-mapped

Mapped to CERT-In, DPDP, client, PCI DSS and overseas requirements



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

Clients, processes, data handled, delivery model and audit calendar

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.