Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · INSURANCE INTERMEDIARIES & INSURTECH

Every Policy You Sell. Secured End to End.

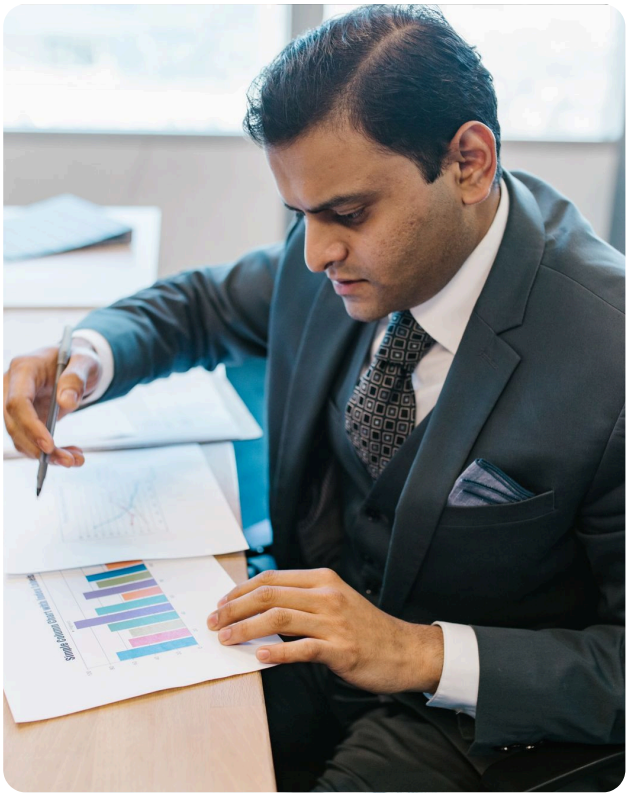
Cyber audits, IRDAI-aligned assessments, API security, claims platform testing and vendor risk for brokers, corporate agents, web aggregators, TPAs, repositories and digital insurance platforms.

- IRDAI Cyber Audits
- Platform Assessments
- API Security
- Claims Platform Testing
- Vendor Risk
- 24/7 SOC

THE CHALLENGE

You hold the customer. Attackers want the data.

Intermediaries handle identity, health and payment data and connect straight into insurers' systems. IRDAI's revised Information and Cyber Security Guidelines, issued on 6 April 2026, apply to brokers, corporate agents, web aggregators and TPAs.



What keeps leadership teams awake

- Leakage of customer, KYC and health data
- Broken APIs exposing quotes, policies and claims
- Phishing and fake sites using your brand
- Premium diversion and business email compromise
- Ransomware halting claims processing or servicing
- Audits, external PT and insurer due-diligence questionnaires

6 Apr 2026
IRDAI's revised guidelines issued, covering intermediaries

6 hours
To report cyber incidents to CERT-In

6-monthly
External penetration testing by CERT-In empanelled auditors

30 days
To submit compliance reports after audit completion (as reported)

The rulebook has changed

Instrument	What it means for you
IRDAI Information and Cyber Security Guidelines (6 Apr 2026)	Apply to brokers, corporate agents, web aggregators and TPAs from FY 2026-27; audits by CERT-In empanelled auditors; compliance reports within 30 days of audit completion (as reported)
Testing and reporting under the 2026 guidelines	External PT at least six-monthly, grey or white box; incidents to CERT-In within six hours
Cloud and vendor requirements	MeitY-empanelled cloud providers with STQC audit status; right-to-audit and sub-outsourcing controls in vendor contracts
CERT-In Directions · DPDP Act & Rules	180-day logs in India; safeguards for personal data; breach intimation from May 2027

OUR SERVICE OFFERINGS

One partner from lead to claim

Built around our primary proposition for the sector: **cyber audits, IRDAI-aligned platform assessments, API security, claims platform testing and vendor risk.**

IRDAI Cyber Audits

- Gap assessment against the 2026 guidelines
- Audit by a CERT-In empanelled auditor
- Compliance report and closure tracking
- Board and insurer-ready evidence

Platform Assessments

- Website, app and portal testing
- Distributor and POSP portal reviews
- e-KYC and onboarding flow testing
- Half-yearly external PT (grey/white box)

API Security

- Insurer quote, issuance and claims APIs
- Object-level authorisation testing
- Rate limiting and abuse detection
- Secure SDLC and code review

Claims Platform Testing

- TPA and claims portal testing
- Hospital interface reviews
- Document upload and forgery controls
- Health data protection

Vendor Risk

- Cloud, SaaS and KYC vendor assessments
- Contract and right-to-audit reviews
- Supervised privileged vendor access
- Partner security questionnaires

24/7 SOC & Response

- Managed SOC with SIEM and EDR/XDR
- API abuse and fraud signals
- Brand monitoring and takedown
- 6-hour CERT-In reporting support

Who we serve: insurance brokers · corporate agents including banks and NBFCs · web aggregators · third-party administrators · insurance repositories · digital insurance and insurtech platforms.

BUNDLED SERVICE MODELS

Packaged for how intermediaries buy

Eleven Codec Networks bundles apply directly to intermediaries and insurtechs:

- **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 brokers and corporate agents

- Gap assessment against the 2026 guidelines
- Annual audit and compliance report
- Half-yearly external PT
- Policy pack and awareness

Assurance

Aggregators, TPAs and growing platforms

- Audit support and closure tracking
- Application, API and claims portal testing
- Cloud and DPDPA readiness
- 24x7 managed SOC

Continuous Resilience

Large intermediaries and insurtechs

- Continuous testing and red teaming
- Vendor and partner assurance
- SOC with API abuse and fraud signals
- AI and chatbot security

Mapped to your obligations

Requirement	How we help	Bundle
Audit by a CERT-In empanelled auditor; compliance report within 30 days of audit completion (IRDAI 2026, as reported)	Audit, compliance report and closure tracking	B4
External penetration testing at least six-monthly, grey or white box	Scheduled PT with retest	B1
Cyber incidents to CERT-In within six hours	IR retainer, playbooks and reporting support	B7, B8
Secure applications and APIs connected to insurers	Application and API security testing	B2
MeitY-empanelled CSPs with STQC audit status; data erasure on exit	Cloud review against IRDAI requirements	B3
Vendor right-to-audit, sub-outsourcing approval, supervised privileged access	Vendor risk programme	B9
DPDP safeguards for customer and health data	DPDPA programme and DLP review	B6

THE CODEC NETWORKS VALUE ADD

Why intermediaries choose Codec Networks

CERT-In empanelled

Meets IRDAI's requirement for CERT-In empanelled auditors for audits and external penetration testing.

Certified and accountable

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

Aligned to IRDAI 2026

Every finding mapped to the 2026 guidelines, CERT-In and DPDP requirements.

API and platform depth

Quote, issuance, payment and claims APIs tested the way attackers use them.

Insurer-ready evidence

Reports and closure evidence that answer insurer due-diligence questions.

Certified experts

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

How we engage

Discover & scope

Intermediary type, insurer partners, platforms and APIs, critical vendors and your 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, insurer review and incident a non-event.

Tell us your licence type, platforms and insurer partners. We will propose a practical, IRDAI-mapped audit 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. Source: IRDAI Information and Cyber Security Guidelines, 2026, as reported; confirm against the official circular.