

Codec Networks
Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · INSURANCE & REINSURANCE

Protect Every Policyholder. Prove Every Control.

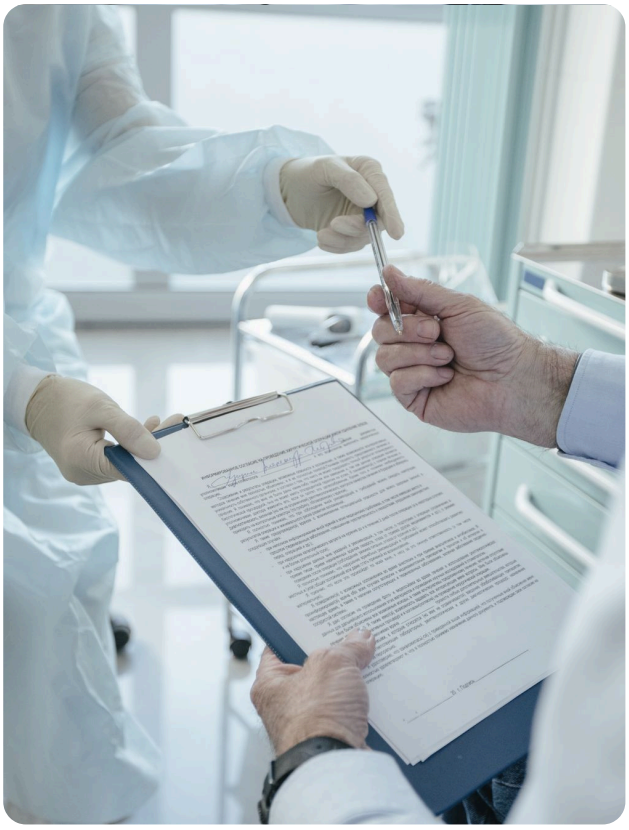
IRDAI cyber audits, 24/7 SOC, privacy, cloud security, ransomware resilience and incident exercises for life, general and health insurers, reinsurers and Foreign Reinsurance Branches.

- IRDAI Cyber Audits
- 24/7 SOC
- Privacy & DPDPA
- Cloud Security
- Ransomware Resilience
- Incident Exercises

THE CHALLENGE

Insurance runs on trust and data. Attackers want both.

Insurers hold some of the most sensitive data in the economy—health records, financial details and claims histories—under IRDAI's revised Information and Cyber Security Guidelines issued on 6 April 2026.



What keeps leadership teams awake

- Ransomware halting claims, renewals and servicing
- Leakage of health and personal data through TPAs and partners
- Policyholder scams and payout diversion
- Claims fraud combining forged documents and insiders
- Annual independent audits and half-yearly external PT
- Reporting incidents to CERT-In and IRDAI within six hours

6 Apr 2026
IRDAI's revised cyber security guidelines issued

6 hours
To report cyber incidents to CERT-In, with copies to IRDAI

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

Quarterly
ISRMC meetings under the 2026 guidelines

The rulebook has changed

Instrument	What it means for you
IRDAI Information and Cyber Security Guidelines (6 Apr 2026)	Apply to insurers, FRBs and intermediaries from FY 2026-27; ISRMC at least quarterly; CISO independent of IT; annual independent audit with auditor rotation
Testing and reporting under the 2026 guidelines	External PT at least six-monthly by CERT-In empanelled auditors; incidents to CERT-In within six hours with copies to IRDAI; BCP/DR tested annually
Cloud and vendor requirements	MeitY-empanelled cloud providers with STQC audit status; right-to-audit and sub-outsourcing approval in vendor contracts
CERT-In Directions · DPDP Act & Rules	180-day logs in India; technical and organisational measures for DPDP compliance; breach intimation from May 2027

OUR SERVICE OFFERINGS

One partner across the policy lifecycle

Built around our primary proposition for the sector: **IRDAI cyber audits, SOC, privacy, cloud security, ransomware resilience and incident exercises.**

IRDAI Cyber Audits

- Gap assessment against the 2026 guidelines
- Annual independent audit support
- Audit report and closure tracking
- ISRMC and Board reporting packs

24/7 SOC

- Managed SOC with SIEM and EDR/XDR
- Claims and payout anomaly detection
- Threat intelligence and hunting
- 6-hour CERT-In and IRDAI reporting support

Privacy & DPDPA

- Health and personal data classification
- DPDPA readiness and consent review
- DLP and encryption controls
- Breach response workflow

Cloud Security

- Review against IRDAI cloud requirements
- MeitY-empanelled CSP and exit terms
- Cloud posture and IAM reviews
- Continuous cloud assurance

Ransomware Resilience

- Ransomware simulation
- Backup isolation and restoration testing
- Annual BCP/DR drills on real scenarios
- Recovery objective validation

Incident Exercises & Testing

- Half-yearly external PT (grey/white box)
- Application and partner API testing
- Tabletop and crisis exercises
- Phishing and deepfake simulations

Who we serve: life insurers · general insurers · standalone health insurers · reinsurers · Foreign Reinsurance Branches · specialised and government-scheme insurers · insurance technology providers.

BUNDLED SERVICE MODELS

Packaged for how insurers actually buy

Eleven Codec Networks bundles apply directly to insurers and reinsurers:

- **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

New and smaller insurers, FRBs

- Gap assessment against the 2026 guidelines
- Half-yearly external PT
- Policy and ISRMC pack
- Backup and BCP readiness check

Assurance

Mid-sized insurers

- Annual independent audit support
- Application and partner API testing
- 24x7 managed SOC
- Cloud and DPDPA readiness

Continuous Resilience

Large insurers and reinsurers

- Continuous testing and red teaming
- TPA, hospital and vendor assurance
- 24x7 SOC with claims-fraud signals
- Board and ISRMC reporting

Mapped to your obligations

Requirement	How we help	Bundle
Annual audit by an independent assurance team; auditor rotation every three years (IRDAI 2026)	Independent audit support and closure tracking	B4
External penetration testing at least six-monthly by CERT-In empanelled auditors	Scheduled grey/white-box PT with retest	B1
Cyber incidents to CERT-In within six hours, with copies to IRDAI	IR retainer, playbooks and reporting support	B7, B8
BCP and DR tested at least annually on real scenarios; results to ISRMC	BCP/DR drill design and observation	B10
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 and TPA assurance programme	B9
DPDP measures, PII classification and encryption	DPDPA programme and DLP review	B6

THE CODEC NETWORKS VALUE ADD

Why insurers choose Codec Networks

CERT-In empanelled

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

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.

Claims and partner depth

Claims platforms, TPA portals, partner APIs and payout flows tested end to end.

Full stack, one partner

Audits, PT, SOC, forensics, BCP/DR and privacy connected from finding to closure.

Certified experts

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

How we engage

Discover & scope

Insurer type, products, distribution and claims partners, critical systems 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, renewal season and incident a non-event.

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