Codec Networks

Coding Threats. Decoding Solutions.

INSURANCE & REINSURANCE

Protect Every Policyholder. Prove Every Control.

IRDAI cyber audits, SOC, privacy, cloud security, ransomware resilience and incident exercises for insurers and reinsurers



What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

IRDAI's 2026 Information and Cyber Security Guidelines

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



A new rulebook for insurance cybersecurity

IRDAI revised its cyber security guidelines in April 2026

6 Apr 2026

IRDAI's revised cyber security guidelines issued

6 hours

To report incidents to CERT-In, with copies to IRDAI

6-monthly

External PT by CERT-In empanelled auditors

Quarterly

ISRMC meetings under the 2026 guidelines

What this means: insurers must now run quarterly ISRMC oversight, keep the CISO independent, commission annual independent audits with auditor rotation, test externally every six months and report incidents within six hours.

Source: IRDAI Information and Cyber Security Guidelines, 2026 (6 April 2026), as reported in public sources.

Who we serve across insurance

Life insurers

Term, savings and annuity

General insurers

Motor, property and commercial

Health insurers

Health and personal accident

Reinsurers

Domestic reinsurance

Foreign Reinsurance Branches

Comply-or-explain approach

Government-scheme insurers

Crop and public schemes

Bancassurance channels

Insurers' bank partners

Insurance technology

Policy, claims and cloud vendors

The threats that cost insurers the most

Six priorities from our 18-threat insurance assessment

Ransomware

Claims, renewals and servicing stop

Health data leakage

Medical records exposed through partners

Claims fraud

Forged documents and insider collusion

Policyholder scams

Fake helplines and payout diversion

TPA & vendor compromise

Partners become the entry point

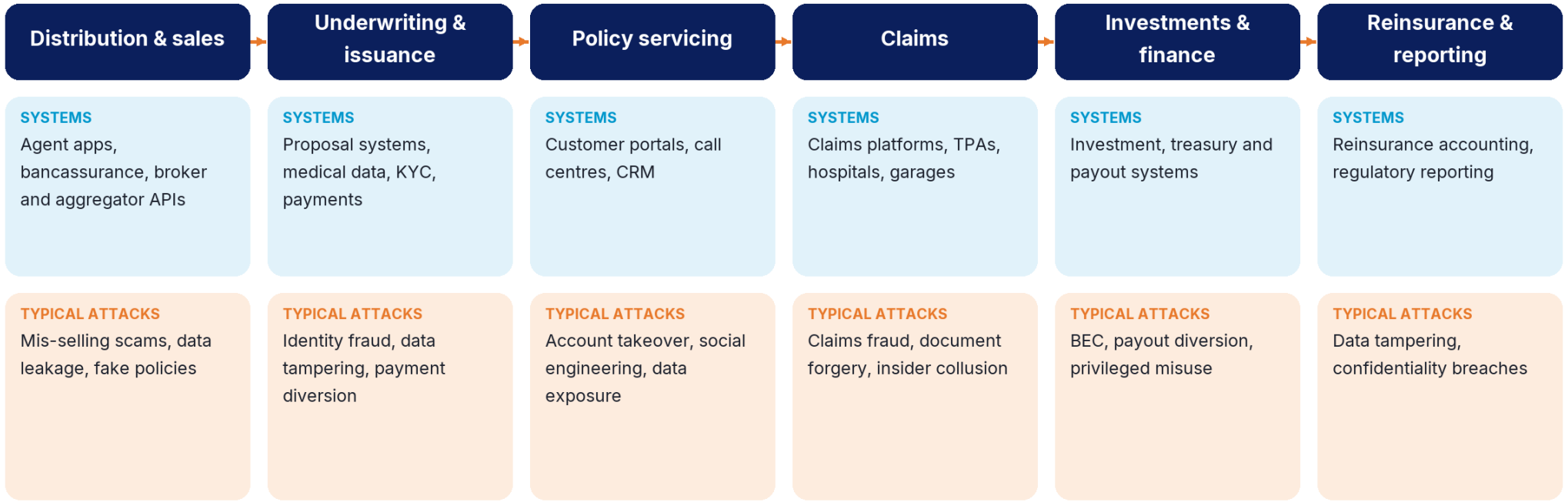
Slow detection & reporting

Missing the 6-hour window

Attacks target every stage of the policy lifecycle

Where Cyber Risk Sits in the Insurance Lifecycle

Every stage of a policy carries its own attack surface



Policyholder trust depends on every link—from the agent's phone to the hospital's billing system.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

IRDAI's revised guidelines apply from FY 2026-27

Codec Networks
Coding Threats. Decoding Solutions.

IRDAI 2026—and the calendar it sets

Requirement	Frequency / deadline	Source
ISRMC meetings	At least quarterly	IRDAI 2026 guidelines
Independent assurance audit	Annual; auditor rotated every 3 years	IRDAI 2026 guidelines
Audit report to IRDAI (insurers)	Within 90 days of FY end or 30 days of audit, if earlier	IRDAI 2026 guidelines
External penetration testing (grey/white box)	At least every six months, CERT-In empanelled	IRDAI 2026 guidelines
Cyber incident reporting	To CERT-In within 6 hours, copies to IRDAI	IRDAI 2026; CERT-In
BCP and DR testing	At least annually, real scenarios	IRDAI 2026 guidelines
Cloud providers	MeitY-empanelled with STQC audit status	IRDAI 2026 guidelines
DPDP safeguards and breach intimation	Most obligations from May 2027	DPDP Act 2023 and Rules 2025

Key dates on the regulatory timeline

Regulatory Timeline for Insurance Cybersecurity

Key IRDAI and cross-sector instruments shaping insurance cybersecurity



Apr 2022	CERT-In Directions: 6-hour incident reporting, 180-day ICT logs in India
Apr 2023	IRDAI Information and Cyber Security Guidelines, 2023
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Nov 2025	DPDP Rules, 2025 notified with phased commencement
Apr 2026	IRDAI Information and Cyber Security Guidelines, 2026 issued (6 April)
FY 2026-27	Compliance with the 2026 guidelines required from the current financial year
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**
Jun 2027	**First audit reports under the 2026 guidelines due (within 90 days of FY end, or earlier)**

Sources: IRDAI, CERT-In, MeitY. Confirm timelines against the official IRDAI circular.

Codec Networks

How Codec Networks helps

IRDAI audits · SOC · Privacy · Cloud · Ransomware resilience · Exercises

Codec Networks
Coding Threats. Decoding Solutions.

One partner across the policy lifecycle

IRDAI Cyber Audits

Gap assessment, annual audit support, ISRMC packs

24/7 SOC

Managed SOC, claims and payout anomaly detection

Privacy & DPDPA

Health data classification, DLP, encryption

Cloud Security

IRDAI cloud requirements, CSP terms, posture

Ransomware Resilience

Simulation, backups, annual BCP/DR drills

Testing & Exercises

Six-monthly external PT, API testing, tabletops

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **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

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

New and smaller insurers, FRBs

- Gap assessment (B4)
- Six-monthly external PT (B1)
- Policy and ISRMC pack (B5)
- BCP readiness check (B10)

Assurance

Mid-sized insurers

- Annual audit support (B4)
- App and API testing (B2)
- 24x7 managed SOC (B7)
- Cloud and DPDPA (B3, B6)

Continuous Resilience

Large insurers and reinsurers

- Red teaming and simulations (B1, B10)
- TPA and vendor assurance (B9)
- SOC with claims-fraud signals (B7)
- Board and ISRMC reporting

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**Ransomware Before Renewal Season**	Claims and renewals stop; EDR, segmentation, backups and drills limit the damage	**B7 · B10 · B8**
2	**The TPA Portal That Shared Too Much**	A partner API leaks medical records; authorisation testing and minimisation prevent it	**B2 · B9 · B6**
3	**The Claims Ring and the Forged Bills**	Forged bills and insider help pass checks; analytics and forensics expose the ring	**B8 · B7 · B9**
4	**The Policyholder Who Never Asked for a Refund**	Fake helplines divert surrender payouts; cooling periods and takedowns stop it	**B2 · B7 · B10**
5	**The Cloud Bucket of Proposal Forms**	A public bucket exposes medical histories; IRDAI cloud reviews and monitoring prevent it	**B3 · B6 · B8**

Example: breaking a ransomware chain

Case 1: Ransomware Before Renewal Season

ILLUSTRATIVE ATTACK PATH

Step 1
Phishing email compromises an employee of a health insurer

→

Step 2
Attacker reaches the policy and claims systems and backups

→

Step 3
Medical records are stolen and systems encrypted

→

Step 4
Cashless claims and renewals stop across the network

→

Step 5
6-hour CERT-In and IRDAI reporting, policyholder harm

WHERE CONTROLS BREAK THE CHAIN

- EDR with 24x7 SOC monitoring
- Segmentation of claims and medical data
- Isolated, tested backups and annual BCP/DR drills
- Rehearsed incident playbook with CERT-In and IRDAI reporting

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

Codec Networks

What we test: EDR coverage and 24x7 monitoring, segmentation of claims and medical data, backup isolation and restoration, annual BCP/DR drills on real scenarios and the 6-hour CERT-In and IRDAI reporting step.

Why insurers choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to IRDAI's 2026 guidelines, CERT-In and DPDP

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 MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

Insurer type, products, partners, critical systems 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.

Codec Networks
Coding Threats. Decoding Solutions.