

Codec Networks
Coding Threats. Decoding Solutions.

INSURANCE & REINSURANCE CYBERSECURITY

IRDAI-ready. Ransomware-ready. Every day.

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

Three questions every insurer's leadership should be able to answer

Are we compliant with IRDAI's 2026 guidelines?
The revised guidelines apply from FY 2026-27, with annual independent audits and auditor rotation.

Is our external PT done every six months by an empanelled auditor?
The 2026 guidelines require grey- or white-box external PT at least half-yearly by CERT-In empanelled auditors.

Could we report an incident within six hours?
Incidents go to CERT-In within six hours, with copies to IRDAI and other regulators.

6 Apr 2026
IRDAI cyber security guidelines issued

6 hours
Incident reporting to CERT-In and IRDAI

6-monthly
External penetration testing

May 2027
Most DPDP obligations take effect

Built for every insurer

Life insurers · general insurers · standalone health insurers · reinsurers · Foreign Reinsurance Branches · specialised and government-scheme insurers · insurance technology providers.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
IRDAI Information and Cyber Security Guidelines (Apr 2026)	ISRMC quarterly; independent CISO; annual independent audit with rotation; six-monthly external PT
Incident, BCP and cloud requirements	6-hour CERT-In reporting with copies to IRDAI; annual BCP/DR tests; MeitY-empanelled CSPs
CERT-In · DPDP	180-day logs; DPDP measures, PII classification and encryption

WHAT WE DO

IRDAI audits, SOC, privacy, cloud, ransomware resilience and exercises

IRDAI Cyber Audits
Gap assessment against the 2026 guidelines, annual audit support, closure tracking, ISRMC packs.

24/7 SOC
Managed SOC, claims and payout anomaly detection, 6-hour reporting support.

Privacy & DPDPA
Health and personal data classification, DPDPA readiness, DLP and encryption.

Cloud Security
Review against IRDAI cloud requirements, CSP terms, posture and IAM reviews.

Ransomware Resilience
Ransomware simulation, backup testing, annual BCP/DR drills, recovery validation.

Testing & Exercises
Six-monthly external PT, application and API testing, tabletop and phishing exercises.

Choose your starting point

Foundation
Gap assessment against the 2026 guidelines, six-monthly external PT, policy and ISRMC pack, BCP check. For new and smaller insurers and FRBs.

Assurance
Annual audit support, application and API testing, 24x7 managed SOC, cloud and DPDPA readiness. For mid-sized insurers.

Continuous Resilience
Continuous testing and red teaming, TPA and vendor assurance, 24x7 SOC with claims-fraud signals, Board reporting. For large insurers and reinsurers.

Why Codec Networks

CERT-In empanelled
for information security auditing services, and empanelled with NICSI for application audit services.

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

Regulation-mapped
Every finding mapped to IRDAI's 2026 guidelines, CERT-In and DPDP.

One connected partner
Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your products, partners and audit deadlines. We will propose an IRDAI-mapped assessment and assurance plan.

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
Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220
Email: 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. 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.