

Audit-ready. API-secure. Insurer-trusted.

Cyber audits, IRDAI-aligned assessments, API security, claims platform testing and vendor risk for intermediaries and insurtechs.

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

Is our audit done by a CERT-In empanelled auditor?

The 2026 guidelines expect audits by CERT-In empanelled auditors, with compliance reports within 30 days (as reported).

Are our insurer APIs tested against real attacks?

Broken authorisation in quote, policy and claims APIs is the most common cause of mass data exposure.

Could we report an incident within six hours?

CERT-In requires reporting within six hours of noticing an incident; insurer partners will expect prompt notice too.

6 Apr 2026

IRDAI cyber security guidelines issued

6 hours

Incident reporting to CERT-In

6-monthly

External penetration testing

May 2027

Most DPDP obligations take effect

Built for every intermediary

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

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
IRDAI Information and Cyber Security Guidelines (Apr 2026)	Cover brokers, corporate agents, web aggregators and TPAs; CERT-In empanelled auditors; six-monthly external PT
Incident, cloud and vendor requirements	6-hour CERT-In reporting; MeitY-empanelled CSPs; vendor right-to-audit
CERT-In · DPDP	180-day logs; safeguards for customer and health data

Cyber audits, platform assessments, API security, claims testing and vendor risk

IRDAI Cyber Audits

Gap assessment against the 2026 guidelines, audit by a CERT-In empanelled auditor, compliance report.

Platform Assessments

Website, app, distributor portal and e-KYC testing; six-monthly external PT.

API Security

Quote, issuance, payment and claims APIs; authorisation and abuse testing.

Claims Platform Testing

TPA portals, hospital interfaces, document uploads and health data protection.

Vendor Risk

Cloud, SaaS and KYC vendor assessments, contract reviews, privileged access.

24/7 SOC & Response

Managed SOC, API abuse signals, brand monitoring, 6-hour reporting support.

Choose your starting point

Foundation

Gap assessment, annual audit and compliance report, half-yearly external PT, policy pack. For smaller brokers and corporate agents.

Assurance

Audit support, application, API and claims portal testing, cloud and DPDPA readiness, managed SOC. For aggregators, TPAs and growing platforms.

Continuous Resilience

Continuous testing and red teaming, vendor assurance, SOC with API abuse signals, AI security. For large intermediaries and insurtechs.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI 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 DPDPA.

One connected partner

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

Book a scoping session

Share your licence type, platforms and insurer partners. We will propose an IRDAI-mapped audit 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.