

Build securely. Deliver confidently.

Secure code review, DevSecOps, infrastructure testing, ISO readiness, SOC and supply chain security for IT service firms.

Three questions every IT services leader should be able to answer

Could a compromised build reach our clients?

Pipelines, signing keys and developer endpoints decide whether one breach becomes many.

Who can use our remote-management tools?

RMM and privileged tools need phishing-resistant MFA, approvals and 24x7 monitoring.

Could we report an incident within six hours?

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

6 hours

Incident reporting to CERT-In

Annual

Third-party cyber audits (CERT-In 2025)

Sep 2026

EU CRA reporting obligations

May 2027

Most DPDP obligations take effect

Built for every IT service firm

Software developers and product engineering firms · IT consultancies · system integrators · managed service providers · staffing and subcontracting partners.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; annual risk-based third-party audits
Client regulator flow-down	RBI, SEBI and IRDAI vendor controls; audit rights and incident clauses
DPDP · international	Processor safeguards; GDPR, NIS2, DORA and EU CRA for European clients

WHAT WE DO

Secure code, DevSecOps, infrastructure testing, ISO, SOC and supply chain

Secure Code Review

Manual and automated code review, SAST, DAST, SCA and secrets scanning.

DevSecOps

CI/CD security, build integrity and signing, SBOM governance.

Infrastructure Testing

VAPT, jump hosts, RMM tools, Active Directory and red teaming.

ISO Readiness

ISO/IEC 27001:2022 and SOC 2 readiness, client evidence packs.

24/7 SOC

Managed SOC, privileged and RMM monitoring, 6-hour reporting support.

Supply Chain Security

Subcontractor assessments, dependency risk, access lifecycle reviews.

Choose your starting point

Foundation

Secure code review and SCA, external VAPT, ISO 27001 gap assessment, policy pack. For smaller developers and consultancies.

Assurance

DevSecOps review, infrastructure and RMM testing, ISO 27001 or SOC 2 readiness, managed SOC. For mid-sized SIs and MSPs.

Continuous Resilience

Continuous testing and red teaming, supply-chain assurance, SOC with privileged-access signals, client reporting. For large SIs and MSPs.

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 CERT-In, DPDP, client regulator and international requirements.

One connected partner

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

Book a scoping session

Share your delivery model, clients and certifications. We will propose a practical 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. Sources: CERT-In, MeitY, European Union. Confirm obligations against the official instruments.