Codec Networks
Coding Threats. Decoding Solutions.

AI, ANALYTICS & AUTOMATION CYBERSECURITY

Trusted AI. Tested AI.

AI/LLM security testing, data leakage testing, model risk, AI governance and privacy for AI builders and adopters.

Three questions every AI leader should be able to answer

What happens if our AI reads a malicious instruction?
Indirect prompt injection through emails, documents and web pages is the leading AI attack path.

What can our agents do without a human?
High-impact actions need scoped permissions, approvals and monitoring.

Do we have a lawful basis for our training data?
DPDP requires lawful processing of personal data, including data used to train and ground AI.

Nov 2025
India AI Governance Guidelines

20 Feb 2026
Synthetic-content IT Rules in force

6 hours
Incident reporting to CERT-In

May 2027
Most DPDP obligations take effect

Built for every AI team

AI product firms · chatbot and AI agent developers · analytics and data platform providers · automation and RPA providers · enterprise AI adopters, including banks, insurers, healthcare and government.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
India AI Governance Guidelines · IT Rules (2025, 2026)	Principles-based governance; labelling of synthetic content
DPDP · CERT-In	Lawful processing of personal data; 6-hour incident reporting
Sector and international	RBI FREE-AI; EU AI Act; ISO/IEC 42001; NIST AI RMF

WHAT WE DO

AI/LLM testing, data leakage, model risk, governance and privacy

AI / LLM Security Testing
Prompt injection, jailbreaks, RAG and AI API testing.

Data Leakage Testing
Output leakage, cross-user retrieval and memorisation tests.

Model Risk
Model provenance, supply chain, poisoning and extraction risk.

AI Governance
ISO/IEC 42001 readiness, AI policy, inventory and risk register.

Privacy & DPDPA
Lawful basis, PII redaction, consent and retention for AI data.

Agent Security
Tool scoping, approvals, sandboxing and action monitoring.

Choose your starting point

Foundation
LLM application test, data leakage quick test, AI usage policy, DPDPA quick assessment. For start-ups and pilot projects.

Assurance
RAG, agent and API testing, model supply-chain review, ISO/IEC 42001 readiness, AI usage monitoring. For scaling products and adopters.

Continuous Resilience
Continuous AI red teaming, model risk and governance programme, SOC with AI abuse signals, Board reporting. For large enterprises.

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 India's AI guidelines, IT Rules, DPDP, CERT-In and sector requirements.

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

Book a scoping session

Share your AI systems, data and customers. We will propose a practical AI security and governance 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: MeitY, CERT-In. Confirm obligations against the official instruments.