



Codec Networks

Coding Threats. Decoding Solutions.

INDUSTRY BROCHURE · AI, ANALYTICS & AUTOMATION

Build AI You Can Trust. Deploy AI You Can Defend.

AI/LLM security testing, data leakage testing, model risk, AI governance and privacy for AI product firms, enterprise AI adopters, analytics providers and chatbot and AI agent developers.

AI / LLM Security Testing

Data Leakage Testing

Model Risk

AI Governance

Privacy & DPDPA

Agent Security

Coding Threats. Decoding Solutions.

www.codecnetworks.com

THE CHALLENGE

Your AI reads anything and acts on it. Attackers write what it reads.

AI assistants, RAG applications and agents now handle sensitive data and take real actions. India's AI Governance Guidelines, the 2026 IT Rules amendment on synthetic content and the DPDP framework set expectations—and enterprise buyers ask for proof.

What keeps leadership teams awake

- Prompt injection hijacking assistants and agents
- Sensitive data leaking through AI outputs
- Agents with too much access taking unsafe actions
- Training data collected without a lawful basis
- Malicious or tampered models in the supply chain
- Deepfake fraud and DPDP, IT Rules and sector obligations



Nov 2025

India AI Governance
Guidelines released

20 Feb 2026

IT Rules amendment on
synthetic content in force

6 hours

To report cyber incidents
to CERT-In

May 2027

Most DPDP obligations
take effect

The rulebook has changed

Instrument	What it means for you
India AI Governance Guidelines (Nov 2025)	Principles-based approach relying on existing laws and sector regulators; trust, accountability and safety
IT Rules amendment on synthetic content (in force 20 Feb 2026)	Labelling of synthetically generated information and faster takedowns for intermediaries
DPDP Act & Rules · CERT-In	Lawful processing of personal data in training and use; 6-hour incident reporting and 180-day logs
Sector rules and international standards	RBI FREE-AI framework for BFSI; EU AI Act for EU markets; ISO/IEC 42001 and NIST AI RMF

One partner from data to deployed agent

Built around our primary proposition for the sector: **AI/LLM security testing, data leakage testing, model risk, AI governance and privacy.**

AI / LLM Security Testing

- Direct and indirect prompt injection
- Jailbreak and guardrail testing
- RAG and connector security
- AI API and application testing

Data Leakage Testing

- Sensitive data in outputs
- Cross-user and cross-tenant retrieval
- Training-data memorisation tests
- System prompt and secret exposure

Model Risk

- Model provenance and supply chain
- Poisoning and backdoor review
- Model theft and extraction risk
- Evaluation and red-team results

AI Governance

- ISO/IEC 42001 readiness
- AI policy, inventory and risk register
- Alignment to India's AI guidelines
- Human oversight and accountability

Privacy & DPDPA

- Lawful basis for training and use
- PII detection and redaction
- Consent and notice reviews
- Data retention and deletion

Agent Security

- Tool and permission scoping
- Human-in-the-loop for high-impact actions
- Sandboxed execution
- Agent action monitoring

Who we serve: 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.

Packaged for how AI teams buy

Eleven Codec Networks bundles apply directly to AI builders and adopters:

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	

Foundation

Start-ups and pilot projects

- LLM application security test
- Data leakage quick test
- AI usage policy pack
- DPDPA quick assessment

Assurance

Scaling AI products and adopters

- RAG, agent and API testing
- Model supply-chain review
- ISO/IEC 42001 readiness
- AI usage monitoring

Continuous Resilience

Large enterprises and AI platforms

- Continuous AI red teaming
- Model risk and governance programme
- SOC with AI abuse signals
- Board and regulator reporting

Mapped to your obligations

Requirement	How we help	Bundle
Principles-based AI governance (India AI Governance Guidelines, 2025)	AI governance framework and risk register	B5, B11
Labelling of synthetic content by intermediaries (IT Rules amendment, 2026)	Content-labelling and takedown process review	B4
Lawful processing of personal data in training and use (DPDP)	DPDPA programme for AI data	B6
Cyber incidents to CERT-In within six hours; 180-day logs	AI usage monitoring and IR support	B7, B8
AI risk management for BFSI adopters (RBI FREE-AI)	Model risk and governance assessment	B4, B11
AI management systems (ISO/IEC 42001)	Readiness and implementation	B5
Secure AI applications and agents (customer contracts)	AI/LLM and agent security testing	B2, B11

Why AI teams choose Codec Networks

CERT-In empanelled

Independent testing and audits recognised by enterprise buyers and regulators.

Certified and accountable

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

AI-native testing

Prompt injection, RAG, agent and model supply-chain testing aligned to OWASP LLM guidance.

Governance that fits India

AI governance mapped to India's guidelines, DPDP and sector regulators.

Full stack, one partner

Application, cloud, SOC, forensics and privacy connected from finding to closure.

Certified experts

OSCP, CEH, CISA, ISO 27001 LA/LI and CHFI professionals.

How we engage

Discover & scope

AI use cases, models and data sources, agent permissions, customers and your governance calendar.

Assess & test

Threat-led testing and regulatory audits executed by certified specialists.

Report in business terms

Findings, risk ratings and a compliance gap matrix for the Board and regulators.

Remediate

Practical, prioritised fixes with technology and compliance teams.

Validate & prove

Retesting and an evidence tracker for auditors, regulators and partners.

Monitor & improve

Managed SOC, recurring testing and quarterly governance reviews.

What you receive: executive summary for the Board or its committee · technical findings with evidence and CVSS ratings · compliance gap matrix · prioritised remediation roadmap · retest reports · audit evidence tracker · SOC dashboards and MTTD/MTTR metrics.



START WITH A SCOPING SESSION

Let's make your next AI launch, audit and incident a non-event.

Tell us 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, New Delhi – 110001

Gurugram

707, 7th Floor, Silverton Tower, Golf Course
Extension Road, Sector 50, Gurugram – 122018,
Haryana

Call

011 430 496 96 · 011 437 522 99
+91 99716 76124 · +91 88007 88220 · +91 88003
31124

Write

mktg@codecnetworks.com
www.codecnetworks.com

Codec Networks

Coding Threats. Decoding Solutions.

Secure Today. Innovate Tomorrow. Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Packages are proposed groupings of Codec Networks bundles, finalised through scoping. 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.