Codec Networks

Coding Threats. Decoding Solutions.

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 builders and adopters

What we will cover

The sector and its risks

Scale, players and the threats that matter most

What regulators now expect

India's AI guidelines, IT Rules on synthetic content, DPDP and sector rules

How Codec Networks helps

Services, bundles and packages built for the sector

Proof in scenarios

Five new case studies and the controls that break the chain

Why Codec Networks and next steps

Our value add and how to start

AI is moving from pilots to production—and to policy

India's guidelines, IT Rules and DPDP now shape AI risk

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

What this means: AI builders and adopters must test for prompt injection and data leakage, control what agents can do, use personal data lawfully, govern models and their supply chain, and be ready to report incidents.

Sources: MeitY, CERT-In.

Who we serve across AI, analytics and automation

AI product firms

Domain and vertical AI

Chatbot and agent developers

Assistants and copilots

Analytics providers

Data platforms and BI

Automation and RPA

Intelligent workflows

Enterprise AI adopters

AI inside the business

BFSI AI adopters

Regulated AI use

Healthcare AI

Clinical and admin AI

AI platforms and MLOps

Model hosting and pipelines

The threats that cost AI teams the most

Six priorities from our 18-threat AI assessment

Prompt injection

Hidden instructions take control

Data leakage

Secrets in AI answers

Excessive agency

Agents acting without limits

Training-data privacy

Personal data without lawful basis

Model supply chain

Malicious or tampered models

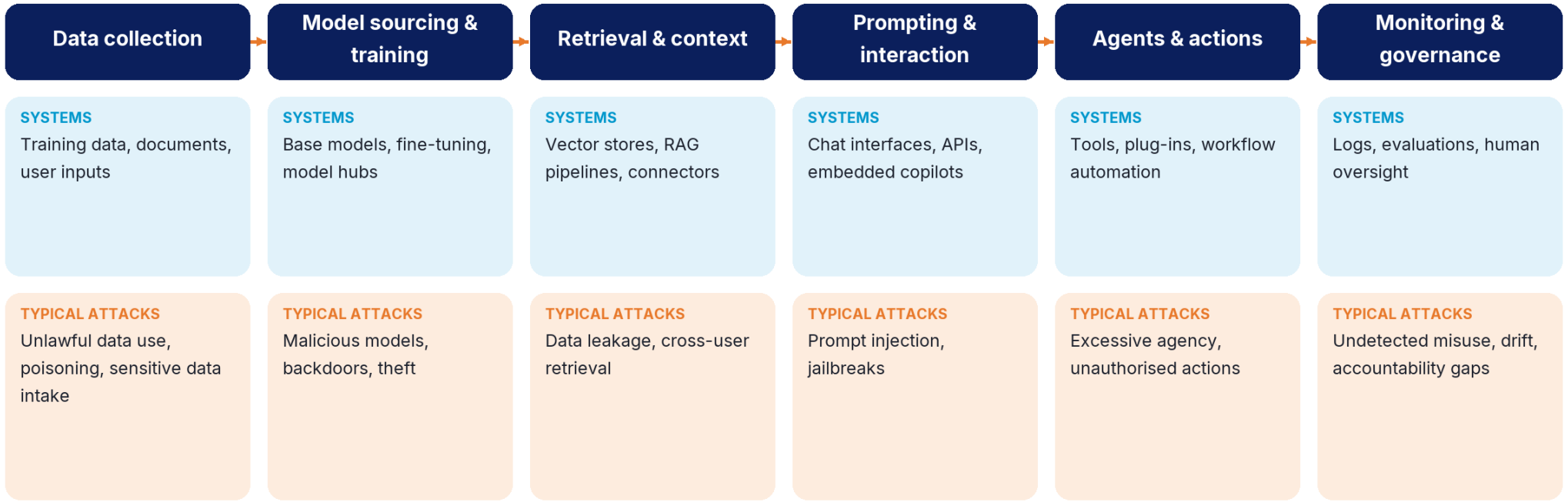
Deepfake fraud

Synthetic executives and voices

Attacks target every stage of the AI lifecycle

Where Cyber Risk Sits in the AI Lifecycle

Every stage from data to action carries its own attack surface



AI security is application security, data protection and identity control—applied to systems that read anything and act on it.

Source: Codec Networks analysis

Codec Networks

Codec Networks
Coding Threats. Decoding Solutions.

What regulators now expect

India's AI guidelines, IT Rules on synthetic content, DPDP and sector rules

Codec Networks
Coding Threats. Decoding Solutions.

The rules and standards shaping AI security

Requirement	Frequency / deadline	Source
AI governance principles	Released 5 Nov 2025	India AI Governance Guidelines (MeitY)
Synthetic content labelling	In force 20 Feb 2026	IT Rules amendment (G.S.R. 120(E))
Personal data in training and use	Most obligations from May 2027	DPDP Act 2023 and Rules 2025
Cyber incident reporting	To CERT-In within 6 hours	CERT-In Directions, 2022
AI in BFSI	Framework guidance	RBI FREE-AI framework
AI systems in EU markets	Phased obligations	EU AI Act
AI management systems	Certifiable standard	ISO/IEC 42001:2023
AI risk management	Voluntary framework	NIST AI RMF 1.0

Key dates on the regulatory timeline

Regulatory and Standards Timeline for AI Security

Indian, international and standards instruments shaping AI risk

Jan 2023	NIST AI Risk Management Framework 1.0 published
Aug 2023	Digital Personal Data Protection Act, 2023 enacted
Dec 2023	ISO/IEC 42001 AI management system standard published
Aug 2024	EU AI Act enters into force, with phased obligations
Nov 2025	India AI Governance Guidelines released; DPDP Rules notified
Feb 2026	IT Rules amendment on synthetically generated information in force (20 Feb)
May 2027	**Most DPDP Rules obligations, incl. breach intimation, take effect**

Sources: MeitY, NIST, ISO, European Union. Confirm obligations against the official instruments.

Codec Networks

How Codec Networks helps

AI/LLM testing · Data leakage · Model risk · Governance · Privacy · Agents

Codec Networks
Coding Threats. Decoding Solutions.

One partner from data to deployed agent

AI / LLM Security Testing

Prompt injection, jailbreaks, RAG

Data Leakage Testing

Outputs, retrieval, memorisation

Model Risk

Provenance, poisoning, extraction

AI Governance

ISO/IEC 42001, policy, risk register

Privacy & DPDPA

Lawful basis, redaction, consent

Agent Security

Tool scoping, approvals, monitoring

Eleven bundles from the Codec Networks catalogue

Business-ready bundles instead of 180 separate services

- **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

Bundle numbers follow the Codec Networks Bundled Service Models. Scope, frequency and pricing are confirmed during scoping.

Three packages, sized to where you are

Foundation

Start-ups and pilot projects

- LLM application test (B2, B11)
- Data leakage quick test (B6)
- AI usage policy pack (B5)
- DPDPA quick assessment (B6)

Assurance

Scaling AI products and adopters

- RAG, agent and API testing (B2, B11)
- Model supply-chain review (B9)
- ISO/IEC 42001 readiness (B5)
- AI usage monitoring (B7)

Continuous Resilience

Large enterprises and AI platforms

- Continuous AI red teaming (B10, B11)
- Model risk and governance (B11, B4)
- SOC with AI abuse signals (B7)
- Board and regulator reporting (B5)

Every obligation mapped to a bundle

Requirement	How Codec Networks helps	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

Five new case studies, five broken chains

Illustrative composite scenarios written for 2026—not client engagements

1	**The Support Bot That Followed Hidden Instructions**	Indirect prompt injection leaks data and issues refunds; injection testing stops it	**B11 · B2 · B7**
2	**The Agent With the Keys to Production**	An over-privileged agent deletes data; scoped tools and approvals prevent it	**B11 · B3 · B8**
3	**The Training Set That Included Customer Chats**	A model repeats personal data; lawful basis and redaction prevent it	**B6 · B11 · B5**
4	**The Deepfake CFO on the Video Call**	Deepfaked executives order transfers; out-of-band checks stop it	**B10 · B7 · B8**
5	**The Poisoned Model From a Public Hub**	A malicious model file runs code; provenance checks prevent it	**B9 · B3 · B7**

Example: breaking a prompt-injection chain

Case 1: The Support Bot That Followed Hidden Instructions

ILLUSTRATIVE ATTACK PATH

Step 1
A company's AI support bot reads incoming customer emails

→

Step 2
An attacker hides instructions inside an email

→

Step 3
The bot follows them and reveals other customers' details

→

Step 4
It also issues an unauthorised refund

→

Step 5
Data exposure, losses and loss of trust

WHERE CONTROLS BREAK THE CHAIN

- Indirect prompt injection testing
- Separation of instructions and untrusted content
- Least-privilege tools and human approval for refunds
- Monitoring of bot actions and outputs

Illustrative composite scenario prepared by Codec Networks. Not a client engagement.

Codec Networks

What we test: direct and indirect prompt injection through emails and documents, separation of instructions from untrusted content, tool permissions and approvals, output filtering, and monitoring of bot actions.

Why AI teams choose Codec Networks

CERT-In empanelled

For information security auditing services; NICSI empanelled for application audits

Certified

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

Regulation-mapped

Mapped to India's AI guidelines, IT Rules, DPDP, CERT-In and sector rules

Tests the whole chain

Technical, process and monitoring tests together

Full stack, one partner

VAPT, audits, SOC, forensics, privacy and Board advisory connected

Specialist experts

CEH, OSCP, CPENT, CISA, ISO 27001 LA/LI, CHFI; OWASP, MITRE ATT&CK, NIST

How we deliver, and what you receive

Codec Networks Delivery Methodology

Nine stages, from scoping to continuous improvement

Source: Codec Networks project and service delivery methodology

Codec Networks

- Executive summary for the Board or its committee
- Technical findings with evidence and CVSS ratings
- Compliance gap matrix mapped to your obligations
- Prioritised remediation roadmap and retest reports
- Audit evidence tracker for regulators and partners
- SOC dashboards with MTTD and MTTR metrics

Let's start with a scoping session

1 Scoping session

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

2 Proposal

Regulation-mapped scope, methodology, timeline and deliverables

3 Kick-off

Testing, audit or SOC onboarding, with Board-ready reporting

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

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

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.

Codec Networks
Coding Threats. Decoding Solutions.