

AI YOU CAN
TRUST:
INFOSYS
AI ASSURANCE
FOR SECURE,
RESPONSIBLE
AND SCALABLE
ADOPTION



Why AI Demands a New Assurance Paradigm

AI is transforming how enterprises operate, but it also introduces risks that traditional software controls were never designed to manage. Generative and agentic AI systems are adaptive, non-deterministic, and continuously evolving, creating new challenges around trust, security, compliance, and governance. As AI adoption accelerates, organizations need a proactive assurance approach that continuously evaluates and manages risk across the AI lifecycle.

Where traditional testing falls short

AI systems are dynamic, probabilistic, and continuously evolving, introducing risks that extend beyond the scope of conventional quality assurance. As AI adoption scales, enterprises need assurance capabilities that continuously assess, monitor, and govern AI systems throughout their lifecycle.

- Point-in-time testing cannot uncover emerging risks such as model drift, changing data patterns, and evolving AI behaviors.
- Conventional validation approaches struggle to address AI specific risks including hallucinations, prompt injection, emergent behavior, and tool side effects.
- Security and compliance assessments are often disconnected from ongoing AI operations, limiting visibility into production risks.
- Limited observability and traceability make it difficult to explain AI decisions, demonstrate compliance, and maintain audit readiness.
- Governance is frequently applied after deployment rather than being embedded across the AI lifecycle.

Infosys AI Assurance: AI Risk Underwriting Powered by AI3S

Infosys AI Assurance delivers an AI-first value framework that enables enterprises to scale AI adoption with confidence. Powered by Infosys Topaz™, our generative and agentic AI suite, it extends assurance beyond traditional testing to help organizations proactively identify, mitigate, and govern AI risks across the enterprise.

At the core of the offering is the AI3S Framework:

Scan | Shield | Steer

The framework continuously identifies AI risks, establishes enterprise defenses, and enables responsible governance so organizations can innovate with confidence while maintaining trust, compliance, and resilience.

SCAN

Identify and Assess
AI Risks Continuously



AI risks evolve as models, regulations, and business environments change. Scan provides continuous visibility into AI risk exposure, helping organizations detect vulnerabilities, monitor drift, ensure compliance, and maintain production readiness.

KEY CAPABILITIES

- AI risk, vulnerability, and compliance assessment
- Continuous monitoring and drift detection
- Production observability and traceability
- Threat remediation and re-certification

OUTCOMES

- Early detection of AI vulnerabilities
- Continuous compliance readiness
- Improved AI reliability and performance
- End-to-end AI visibility and auditability

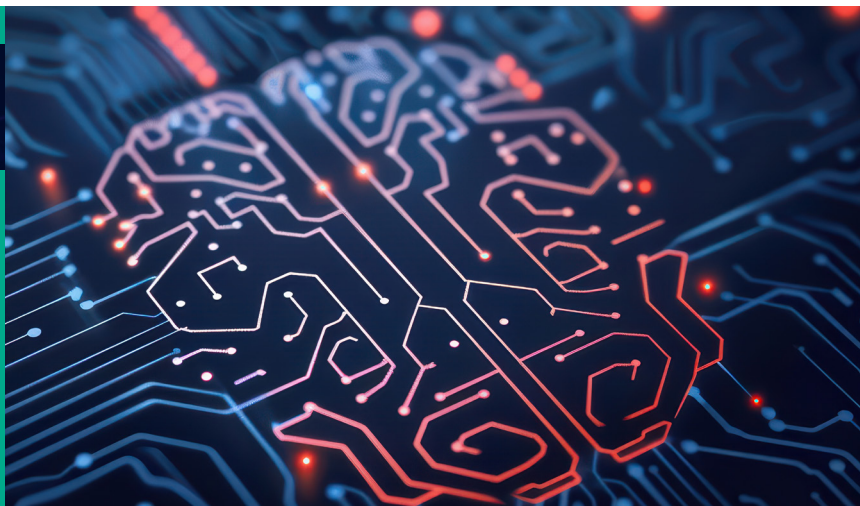
SHIELD

Build Defenses into
the AI Assurance Lifecycle



Shield establishes comprehensive AI protection mechanisms across business, technology, security, and governance dimensions.

No single testing approach can adequately address the unique challenges posed by AI systems. Infosys Shield embeds assurance controls throughout the AI lifecycle using our **BR² FRAMEWORK**.



KEY CAPABILITIES

BR² FRAMEWORK



Business Assurance

Ensures AI aligns with enterprise goals and adapts to real-world data



Benchmarking

Validates AI performance against industry and custom metrics



Red Teaming

Simulates adversarial attacks to uncover vulnerabilities



Responsible AI

Promotes fairness, transparency, and responsible governance

OUTCOMES

- Reduced AI operational risk
- Improved security and resilience
- Increased business trust and adoption
- Enterprise-ready responsible AI controls

STEER

Govern AI Responsibly
at Enterprise Scale



Steer combines Infosys' Responsible Agent Framework with governance, advisory, and industry expertise to help enterprises establish trusted and scalable AI governance. It enables organizations to define policies, manage AI risks, ensure regulatory readiness, and operationalize Responsible AI across the enterprise.

KEY CAPABILITIES

- AI governance, policy, and risk management frameworks
- Responsible AI strategy and maturity assessments
- Responsible AI Office setup and operating models
- Customized governance frameworks and platform services
- Cloud-native Responsible AI services

OUTCOMES

- Enterprise-wide AI governance
- Enhanced regulatory readiness
- Responsible AI operating model
- Sustainable AI adoption at scale

Infosys helps enterprises establish and operationalize AI governance through policies, risk management frameworks, Responsible AI practices, and advisory services. This enables organizations to scale AI confidently while maintaining trust, accountability, and regulatory compliance.

Infosys AI Assurance Platform Capabilities

- Golden repository creation for ground truth validation
- Automated benchmark execution across LLMs and agents
- Variant data generation to simulate diverse real-world scenarios
- RAI metrics and custom evaluations for fairness, transparency and governance
- Security and performance testing, including hallucination detection, jailbreak checks and bias analysis



Making an impact across industries

1. Building trust and protecting margins at scale

A leading global consulting firm turned to Infosys AI Assurance to bring greater trust, accuracy, and consistency to its delivery. By applying AI Assurance to document intelligence across 800–1,200 engagements per quarter, the firm significantly reduced rework and safeguarded margins.

THE OUTCOME

- **6–12 hours** of rework eliminated per engagement
- **USD 0.6–1.7 million** saved per quarter through reduced rework
- **USD 0.3–1.25 million** protected per quarter by cutting write-offs and margin erosion
- **USD 1.2–2.5 million** total quarterly value delivered

AI Assurance impact: USD 8-11 million exposure avoided annually

2. Strengthening customer operations

A major electric utility in the Southwestern United States leveraged Infosys AI Assurance for its customer engagement operations, where it manages ~1.3 million accounts and 150k monthly chat interactions. By ensuring reliability and accuracy in AI-driven customer interactions, the utility reduced repeat contacts, minimized regulatory escalations, and avoided costly remediation events.

THE OUTCOME

- Base volumes: **~1.3 million accounts**; ~150k chat interactions/month
- Repeat contact (rehit) avoidance: 8–12% failed chats avoided → 15k–18k calls/month saved → **USD 1.1–1.3 million/year**
- Regulatory escalations avoided: ~100–200/month avoided; handling cost USD 300–600 each → **USD 0.4–1.4 million/year**
- Remediation/consent-order-style uplift avoided: **USD 0.8–1.5 million** (one-off)
- Total impact: **~USD 3–6 million** annual savings/avoidance across operating cost, escalations, and remediation (excluding fines)

AI Assurance impact: USD 5.5–8 million annual exposure avoided in cost-to-serve and compliance overhead

3. Enhancing Reliability in Digital Payments

One of the largest US electric utilities, serving ~5 million accounts with 65% of payments made online, turned to Infosys AI Assurance to safeguard its digital payment infrastructure. With 3.25 million digital payments monthly, AI Assurance mitigated risks of conversion loss, call surges, late-fee waivers, and costly IT fixes, ensuring resilient operations and cash flow stability.

THE OUTCOME

- Scale: **~5.0 million accounts**; 65% pay online
- Monthly digital payments: **≈ 3.25 million**; average bill USD 120
- Self-service drop: 10–20% decline over 0.5–1.0 day → deferred payments **USD 0.7–2.6 million** (cash timing impact)
- Working capital cost: 6–8% APR → **USD 12–45k**
- Contact surge: 30–60k extra calls × USD 6 ≈ **USD 180–360k**
- Late-fee waivers: 50–100k accounts × USD 5 ≈ **USD 250–500k**
- Ops/IT remediation (hotfix + testing): **USD 0.2–0.5 million**
- Total per incident: **USD 1.2–3.0 million** (quarterly impact)

AI Assurance impact: USD 8.5–12 million annual exposure avoided in fee credits, cash flow timing, and call volume

Why Infosys? Proven, Tested, Trusted.

Infosys brings together quality engineering discipline, real-world AI delivery experience, and an informed view of the modern AI value chain, enabling organizations to adopt AI with confidence and control.

Grounded in how modern AI is built

Experience across the AI lifecycle, from data and human feedback to models, agents, and enterprise adoption, brings a practical understanding of where risks emerge and how they compound.

Assurance beyond point-in-time testing

AI systems are validated continuously across evolution, scale, and drift, reflecting the realities of probabilistic outputs, dynamic behavior, and changing data.

Balanced rigor and pragmatism

Automation and benchmarking are applied at scale, complemented by human judgment where domain context, safety, and responsibility matter most.

Integrated assurance capability

Business alignment, model performance, security resilience, and responsible AI considerations are addressed together, supported by structured methods and platform-led enablement rather than disconnected checks.

Enterprise-grade delivery and accountability

Global scale, operating discipline, and experience in regulated environments allow AI assurance to move from experimentation into production with confidence.

The bottom line and the path forward

As enterprises accelerate AI adoption, they must go beyond testing AI the old way. Infosys AI Assurance delivers a comprehensive, automated, and responsible QE approach that makes AI trustworthy, secure and enterprise-ready.

Reach out to us [IQE Marketing](#) to learn more about Infosys AI Assurance.



For more information, contact askus@infosys.com

Infosys
Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.

Infosys.com | NYSE: INFY

Stay Connected   