Highlights

- **Reduce AI risk before deployment** – Identify security gaps and validate agents in sandboxed environments before they touch production systems
- **Compliance by Design** – Evidence packs, dashboards, lineage, and immutable audit trails aligned to EU AI Act, NIST, ISO.
- **Meet regulatory requirements faster** – Build compliant AI foundations with formal governance frameworks, ethical standards, and Zero-Trust principles built in from day one
- **Prevent AI-specific threats** – Proactively test against adversarial attacks, model vulnerabilities, and misuse scenarios using offensive security techniques designed for AI

kyndryl

Kyndryl Consult Agentic AI Digital Trust Services

Closing the Enterprise AI trust gap

Introduction

Enterprises face a parallel challenge with the rise of **Agentic AI** — autonomous systems capable of setting goals, making decisions, and executing actions with minimal human oversight. Unlike traditional IT systems, these agents are active participants in enterprise operations.

Without effective governance, enterprises risk undermining the very trust and value AI is meant to create.

The Kyndryl Solution

To address this challenge, Kyndryl has developed Kyndryl Consult Agentic AI Digital Trust Services, to make AI adoption safe, transparent, and compliant. It provides the governance services that enterprises demand as they adopt custom, third-party, and enterprise AI agents.

The offering effectively addresses market needs through a comprehensive solution anchored in two strategic modules.

- **Trusted Foundations-** Develop a comprehensive AI security strategy and governance framework to establish trust and compliance from the start.
- **Build Smart-** Accelerate secure adoption of Agentic AI with built-in resilience, transparency, and control.

Ensure continuous protection, compliance, and trust across your AI ecosystem using the **Run Safe** module as part of managed service.

Core Service Components

Module 1: Trusted Foundations
Build on secure ground

Expert guidance to help clients design, assess, and operationalize secure and compliant AI foundations:

- **AI Security & Governance Assessment –** Identify maturity gaps, risks, and improvement opportunities using *Kyndryl Consult Responsible AI Maturity Assessment* offering.
- **Responsible AI & Security Policy Development –** Define formal governance framework, principles, controls, and accountability models using *Kyndryl Consult Data Security Posture Management for AI* Offering and *Policy & Compliance support services* as part of *Security Assurance Management program* for AI.
- **Digital Twin & Data Ontology Modeling –**Define the ontologies, processes, and assets for client environments.

Module 2: Build Smart
Design and Implement Secure Agentic AI

Specialized services and accelerators to embed security from design to deployment:

- **Secure Agent Development & AI Threat Modeling –** Engineer and test AI agents for integrity, safety, and confidentiality using the *Kyndryl Continuous Security Controls Validation* offering for DevSecOps for AI. Anticipate misuse, adversarial attacks, and model vulnerabilities using *Kyndryl Offensive Security services*.
- **AI Red Teaming & Penetration Testing –** Validate defenses against real-world AI-specific threats using *Kyndryl Offensive Security services*.
- **Agent Certification (in the Sandbox) –** Test & validate before deployment against global regulatory and ethical standards and Zero-Trust principles using the various automated *IAM Services for AI*.

Why Kyndryl?

Kyndryl is the world's largest IT infrastructure services provider serving thousands of enterprise customers in more than 60 countries. The company designs, builds, manages and modernizes the complex, mission-critical information systems that the world depends on every day.

Kyndryl has deep expertise in designing, running, and managing the most modern, efficient, and reliable technology infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We are building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side by side with our customers to unlock potential.

Competitive Differentiators

- End-to-End Expertise: Proven consulting, implementation, and managed services for efficient operations.
- Vendor-Agnostic Approach: Works across platforms to drive modernization and excellence.
- Global Reach: Presence in 60+ countries with deep industry experience.
- Cybersecurity Leadership: 7,500+ experts in AI, privacy, and risk management.
- Trusted by Enterprises: Supporting 60% of Fortune Global 100 clients.

For More Information

To learn more about Kyndryl Governance, Risk & Compliance please contact your Kyndryl business partner or visit www.kyndryl.com

kyndryl