Science & Technology · GS - III

What is agentic Artificial Intelligence (AI)? Explain its working. Describe its applications with suitable examples. Discuss the advantages, risks and challenges associated with agentic AI systems.

EXAM YEAR	PAPER	SUBJECT
2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Autonomous agents, goal-oriented AI, planning, tool use, reasoning, feedback loop, AI agents, automation, cybersecurity, hallucination, prompt injection, accountability

Model Answer

Agentic AI refers to AI systems capable of pursuing specified goals with a degree of autonomy by planning tasks, using tools, interacting with external systems and adapting to changing conditions. NIST describes such systems as autonomous agents capable of independent decision-making and interaction with their environment.

Working:

1. Goal interpretation: Converts a user objective into actionable tasks.
2. Planning and reasoning: Breaks the objective into sequential or parallel steps.
3. Tool utilisation: Uses APIs, databases, software or other digital tools.
4. Feedback: Evaluates results and modifies subsequent actions.
5. Execution: Continues until the goal is achieved or a predefined control condition is reached.

Applications include autonomous coding and software testing, customer-service agents, enterprise workflow automation, cybersecurity monitoring, research assistance, logistics and personalised digital services.

Advantages include higher productivity, continuous operation, adaptive decision-making and automation of complex workflows.

However, greater autonomy creates distinctive risks: hallucinated actions, unauthorised transactions, privacy breaches, prompt injection, excessive permissions, goal misalignment and unclear liability. NIST specifically highlights the need for identification and authorisation controls because agents may access multiple datasets, tools and applications.

India therefore needs risk-based governance, human oversight for high-impact decisions, audit trails, identity and access controls, sandbox testing, cybersecurity standards and clear liability frameworks.

Thus, agentic AI can shift AI from “answer generation” towards “goal execution”, making governance and safety as important as technical capability.