THINK B · THINK BEYOND

Securing Agentic AI

One issue. 4 GS papers. 3 dimensions. 1 digital control test.

14 NOVEMBER 2026

CURRENT AFFAIRS → MULTIDIMENSIONAL THINKING

⚡THE ISSUE IN 30 SECONDS

FACT	WHY IT MATTERS
CERT-In issued AI security audit norms	They cover AI that plans, uses tools and acts on its own
Autonomy, memory and delegation add risk	Persistent memory, tool use and delegation need closer scrutiny
Auditors test for permission overreach	Checks cover unapproved tool use, bypassed approvals and misused credentials
AI also automates cyber attacks	A CERT-In advisory says attackers use AI tools at machine speed

CORE IDEA: Agentic AI can plan, use tools and delegate on its own, so security must shift from checking outputs to auditing permissions, memory, approvals and emergency-stop controls, while the same automation is also being used to speed up cyber attacks.

🌍THINK BEYOND

AI agents act on their own → **Autonomy widens the attack surface** → **CERT-In sets audit guidelines** → **Permissions and memory get tested** → **Emergency stops are verified** → **Safe autonomy builds trust**

How much autonomy should an AI system get before humans lose meaningful control?

🔗UPSC CONNECT

🌍 GS1 · SOCIETY
Digital society, jobs and public trust in AI

Use in: Society • Trust

🏛 GS2 · GOVERNANCE
CERT-In norms, digital governance and regulation

Use in: Regulation • Governance

⚡ GS3 · TECH
AI security, cyber threats and critical systems

Use in: Cyber • AI

⚖ GS4 · ETHICS
Accountability, human oversight and responsible AI

Use in: Oversight • Responsibility

🎯OPTIONAL CONNECT

PUB ADMIN	LAW	SOCIOLOGY	ECONOMICS
Digital **governance** and cyber norms	AI **liability** and regulation	Technology, **trust** and society	AI and **financial** sector risk

✏HOW CAN I USE THIS IN MAINS?

ESSAY *"The more an AI can do, the more its limits must be defined."*

GS3 *Use this to discuss AI security, cyber threats and critical systems.*

GS2 *Use it to discuss CERT-In norms, digital governance and regulation.*

GS4 *Use it to discuss accountability, human oversight and responsible AI.*

👤THINK LIKE AN OFFICER

★ KEY SECTION

CASE: You are a CISO at a public sector bank. Your team plans to deploy an AI agent that can access systems and execute tasks, and you must decide the safeguards before launch.

YOU HAVE 60 SECONDS: WHAT DO YOU DO?

☐ Deploy first, audit later ☐ Ban all AI tools

☐ Limit permissions and test emergency stops ☐ Trust vendor claims

MODEL ADMINISTRATIVE APPROACH

1 · LIMIT PERMISSIONS
Give agents least-privilege access only

2 · REQUIRE APPROVALS
Keep human sign-off for high-risk actions

3 · TEST AND AUDIT
Test memory, delegation and emergency stops

4 · REPORT INCIDENTS
Log agent actions and report issues to CERT-In

🔑3 THINGS TO REMEMBER

01 · CONNECT
Audit what agents can do

02 · THINK
Keep humans in control

03 · APPLY
Apply this across GS1-4, Essay and optionals