FOR BOARD MEMBERS AND THE EXECUTIVES WHO BRIEF THEM

AI agents in 2027: a board briefing

What changed, what it costs, which rules apply and the questions to ask management. Ten pages, written to be read before a board meeting.

01 What changed

02 Where the money goes

03 The rules

04 The risks

05 The questions

Aman Khanna · Gautam Mehra

Whiteboxx AI

THE BRIEFING IN ONE PAGE

Five things a board should know.

01 **AI has moved from answering to acting.**

Agents now take steps in business systems: they query data, prepare actions and pass results on. The question for boards is no longer whether to use AI, but how its work is checked.

02 **Many projects will not survive.**

Gartner expects more than 40% of agentic AI projects to be cancelled by the end of 2027, mainly because of rising costs, unclear value or weak risk controls.

03 **The model is a small part of the cost.**

In a typical worked example, model usage is 3% of the monthly cost. People checking the results are 82%.

04 **Accountability is the gap.**

In a 2026 survey, only 49% of security leaders could fully reconstruct what their AI agents had done over the previous 30 days.

05 **The rules have dates.**

EU AI Act high-risk rules now apply to uses such as hiring and credit from 2 December 2027, after amendments in 2026.

What to ask for at the next meeting

A list of AI workflows in production, with the owner, the monthly cost per workflow including review, and whether each run can be reconstructed from records.

WHAT CHANGED IN 2026

From answers to actions.

In 2024 most enterprise AI answered questions. By the end of 2026 it increasingly does work: it reads documents, queries systems, prepares actions and hands results to people or other software.

33%

of enterprise software applications will include agentic AI by 2028, up from less than 1% in 2024.

GARTNER, JUNE 2025

40%+

of agentic AI projects will be cancelled by the end of 2027.

GARTNER, JUNE 2025

45%

of security leaders had an AI-related incident where it was unclear who was accountable.

SECURITYHQ AND DATADOG, 2026

8 in 10

enterprises in Europe, the Middle East and Africa escalate AI incidents to the board or C-suite.

IBM, OCTOBER 2026

Why it matters to the board

When AI only answered, a person decided what to do next. When AI acts, the organisation needs to know what it did, with which data, and who approved it. That is a governance question, not only a technology question.

COST

Where the money goes.

Budgets for AI usually start with licences and model usage. In production, the larger costs are the people who check results, the data and integrations, and maintenance.

Worked example: one agent in production, per month



- Human review $10,000 · 82%
- Maintenance $1,333 · 11%
- Hosting, monitoring and data $500 · 4%
- Model usage $384 · 3%

An agent that runs 2,000 times a month, with eight model calls per run on a mid-size model and five minutes of review per result. Monthly cost $12,217, or $6.11 per run. Over three years, including an assumed $80,000 build, $519,824.

COST THE BOARD SHOULD SEE	WHY IT IS OFTEN MISSING
Human review	Rarely budgeted, and it grows with volume
Data access and integration	Each system and source needs its own connection
Testing	Needed again every time the model, data or process changes
Maintenance	Often left out of the first business case

> Ask for the cost per run, including review, for every workflow in production. It is the single most useful number for comparing AI projects.

REGULATION

The rules have dates.

The EU AI Act applies to organisations that place AI systems on the EU market or use them in the EU, wherever they are based. Amendments adopted in 2026 moved the main high-risk deadlines.

1 Aug 2024
The AI Act comes into force

2 Aug 2025
Rules for general-purpose AI models apply

27 Jul 2026
AI Omnibus amendments come into force

2 Dec 2026
Some machine-readable marking duties for AI-generated content

2 Dec 2027
High-risk rules apply to Annex III systems, such as hiring, credit and essential services

2 Aug 2028
High-risk rules apply to AI in regulated products (Annex I)

What boards should make sure exists

1. An inventory of AI systems in use, including tools bought by business teams.
2. A classification of each system by risk, with a named owner.
3. For any high-risk use, such as hiring or credit decisions, a plan to meet the requirements by 2 December 2027.
4. Human oversight that works in practice: people who can understand, override or stop the system (Article 14).
5. Records that show what each system did and with which data.

Dates as amended by Regulation (EU) 2026/1744. Other jurisdictions have their own rules. This is not legal advice: ask counsel which rules apply to your organisation.

RISK

Six risks to track.

Each risk has a control management can put in place and evidence the board can ask to see.

RISK	WHAT IT LOOKS LIKE	THE CONTROL	EVIDENCE TO ASK FOR
Unchecked results	Decisions made on AI output nobody reviewed	A review pattern for each workflow	Share of results reviewed, by workflow
Too much access	An agent can reach data or actions its task does not need	Per-agent limits on tools, data and spend	The list of permissions for each agent
Hidden instructions	Text the agent reads changes what it does (prompt injection)	Input checks and least-privilege access	Results of the last security test
Shadow AI	AI tools and AI-built apps in use without review	An inventory with an owner for each tool	The inventory, and what changed since last quarter
Cost overrun	Usage and review costs grow faster than value	A budget limit per workflow	Cost per run against budget
Weak records	Nobody can say what an agent did last month	A run record for every workflow	A reconstruction of one past run

Prompt injection and excessive agency are among the top risks in the 2025 OWASP Top 10 for LLM Applications.

GOVERNANCE

Twelve questions for management.

Use these at the next board or risk committee meeting. Clear answers usually mean the basics are in place.

VALUE

1. Which AI workflows are in production, and what does each one save?
2. How was the saving measured?
3. Which projects will we stop if they do not show results by a set date?

CONTROL

1. Who owns each workflow, and who reviews its results?
2. Could we reconstruct what an agent did last month, step by step?
3. What is each agent allowed to access and do?

COST

1. What does each workflow cost per run, including review?
2. What will it cost over three years, including maintenance?
3. What do we own if we change vendor?

COMPLIANCE

1. Which of our AI uses could count as high-risk under the EU AI Act?
2. Are we on track for 2 December 2027?
3. Which AI tools are in use that IT has not reviewed?

MATURITY

What good looks like by the end of 2027.

Most organisations are somewhere between the first two columns. The aim for 2027 is the third.

	EXPERIMENTING	PRODUCING	ACCOUNTABLE
Workflows	Many pilots, few in use	Some workflows in daily use	Workflows chosen and measured against a plan
Review	Ad hoc	Reviewed when someone has time	A review pattern for each workflow, with time budgeted
Records	Chat transcripts, if any	Logs kept by each tool	A run record for every workflow: data, steps, approval
Cost	Licences only	Licences and usage	Full cost per run, including review and maintenance
Ownership	The enthusiast who built it	A team	A named owner and reviewer for each workflow
Compliance	Not assessed	Assessed once	An inventory, risk classes and dates tracked quarterly

REPORTING

A quarterly AI dashboard.

Ask management to report these eight measures every quarter, in the same format, so trends are visible.

Workflows in production vs. in pilot	**Hours saved per month** measured, not estimated
Accuracy on test set per workflow	**Results reviewed** share, by pattern
Cost per run including review	**Monthly cost vs budget** all workflows
Incidents and how resolved	**Workflows with owner and records** share of total

> A blank cell is itself a finding. If management cannot fill in a measure, ask what it would take to start recording it.

ABOUT WHITEBOXX

Evidence OS, extended for your workflows.

Whiteboxx builds Evidence OS, an enterprise AI platform, and extends it for each customer with forward deployed engineers. Each run keeps a record of its inputs, sources, steps, calculations and results, so the questions in this briefing can be answered from records.

START WITH THE ARCHITECTURE SPRINT

30 days · USD 15,000, fixed

We review your AI tools and pilots, choose one workflow with you and deliver a build plan with costs. You can use the plan with us, with your own team or with another partner.

Book a scope call: **whiteboxx.ai/contact** · info@whiteboxx.ai

Sources and method

1. Gartner, “Gartner Predicts Over 40% of Agentic AI Projects Will Be Canceled by End of 2027”, 25 June 2025
https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027
2. SecurityHQ, “The accountability gap”, survey of 204 security leaders with Datadog, 2026
https://www.securityhq.com/blog/research-the-accountability-gap/
3. IBM, “Eight in ten EMEA enterprises escalate AI incidents to board or C-suite”, 14 October 2026
https://newsroom.ibm.com/2026-10-14-ibm-study-eight-in-ten-emea-enterprises-escalate-ai-incidents-to-board-or-c-suite-as-ai-agents-test-governance
4. Retool, State of AI Governance 2026 (vendor survey)
https://retool.com/blog/ai-governance-report-2026
5. OWASP, Top 10 for LLM Applications, 2025 edition
https://genai.owasp.org/llm-top-10/
6. Loyens & Loeff, “EU AI Act: key amendments adopted under Digital Omnibus package”, 2026
https://www.loyensloeff.com/insights/news--events/news/eu-ai-act-key-amendments-adopted-under-digital-omnibus-package/
7. EU AI Act, Article 14: human oversight
https://artificialintelligenceact.eu/article/14/
8. Whiteboxx, AI agent cost calculator, November 2026 list prices
https://whiteboxx.ai/resources/ai-agent-cost-calculator/

Method

Statistics are quoted from each publisher’s own summary; surveys run by vendors are marked. The worked cost example uses the Whiteboxx AI agent cost calculator with its default inputs and representative November 2026 list prices. Regulatory dates reflect the EU AI Act as amended by Regulation (EU) 2026/1744.

This document is general guidance, not legal, financial or investment advice. Edition 1 · November 2026, published 2026-11-20. Authors: Aman Khanna and Gautam Mehra, Whiteboxx AI.

You may share this document in full, unchanged, with attribution to Whiteboxx AI. The latest edition is at whiteboxx.ai/resources/ai-agents-board-briefing-2027.