MYTHOS AI SECURITY

AI risk: questions for the board

Use these questions when management proposes a new AI system, expands an existing one, or reports on cyber risk. None needs a technical background to ask.

	QUESTION	OUR ANSWER, AND WHO OWNS IT
1	Where do we use AI today, and who owns each use?	
2	What business benefit are we seeking from this AI?	
3	What information can it access?	
4	What actions can it take, such as sending messages, changing records or making payments?	
5	Which actions require a person's approval, and can that approval be bypassed?	
6	What could materially harm our customers or the business?	
7	Have our websites and systems been tested against attackers who use AI, even where we do not use AI ourselves?	
8	What has been tested, and what remains unknown?	
9	Who owns each unresolved issue?	
10	What evidence do we need before launch or expansion?	
11	Who can pause the system if something goes wrong?	
12	What changes require retesting?	

ONE SENTENCE TO REUSE

“Before approving this deployment, we need evidence of what the system can access and do, how approvals are enforced, what testing found, and who owns the remaining risks.”

A scoped assessment gives evidence about what was tested, under the conditions tested. It does not guarantee future safety, find every weakness or establish compliance on its own.