AI security and agent governance check

Use these four questions with the person who owns the decision. Record evidence for each answer before changing a production setting.

01 **Do agents retrieve only what the caller can access?**
ANSWER AND EVIDENCE

02 **Are connected tools and their permissions inventoried?**
ANSWER AND EVIDENCE

03 **Does every production action have a human approval point?**
ANSWER AND EVIDENCE

04 **Can you revoke an agent and verify that access ended?**
ANSWER AND EVIDENCE

What to do next

01 Assign an owner to every unanswered question.
02 Collect the current policy, access and operating evidence.
03 Agree on a small test with a named human approval point.

No customer data is needed for any answer. When the answers point at work, a scoped review is quoted after a scoping call at simplicityitinc.com/scoping-session/. Every example Simplicity IT publishes is fictional and no client is named.