Architecture-to-Records Worksheet

One governance question per layer. Name the owner, the record and its date, and the next review. Adjust the roles to your organization. Every row keeps exactly one Accountable owner.

Architecture layer	Governance question	Observe and control (by category)	SanctumShield record	Accountable owner	Our system	Owner name	Record and date	Next review
Users and channels	Who may use AI, for what, with which data, and on which accounts and devices (including personal ones)?	Identity and access, usage telemetry, device posture	AI Acceptable Use Policy; role-based training record	CISO				
AI application and agent	What may the agent decide alone, and where is that line written?	Guardrails, execution monitoring	Executive Risk Report (decision boundary); Board Memo	Business owner of the use case				
Agent actions	Which changes may each agent make, who approves them, and who can stop it mid-task (with the date that stop last worked)?	Agent inventory, execution monitoring, approval workflow	Executive Risk Report (agent permissions and stop lines); Board AI Register	Business owner of the use case				
Tools and MCP	Which tools may the agent call, under whose authority, and which systems sit behind each gateway or connector?	MCP gateway, runtime AI security	Executive Risk Report (tool and gateway findings); AI Acceptable Use Policy	CISO				
External services	Which outside parties receive our data, and on what terms?	Data loss prevention, egress monitoring	Executive Risk Report (sub-processors); Verification URL	Legal counsel				
LLM provider	Which models are approved, and who signs off on a change?	Model inventory, usage telemetry	Executive Risk Report (model register); Board Memo	CTO or CIO				
Knowledge and RAG	Which sources are trusted, and does each answer cite the document, version and page it relied on?	Retrieval logging, content filtering	Executive Risk Report (retrieval provenance)	Data owner				
Whole system	Can we show all of this to a board, auditor or insurer?	SOC dashboards and audit logs	All five records, dated and verifiable	CEO, with board oversight				

Generate these records in one guided session at https://sanctumshield.com. Terms: sanctumshield.com/glossary (Proven Stop, MCP Gateway, Retrieval Provenance Record). Training: Academy module M20, academy.sanctumshield.com/curriculum. Last updated October 27, 2026. Educational template, not legal advice.

Starter RACI

R = responsible, A = accountable, C = consulted, I = informed. Each row needs exactly one A.

Decision	Board	CEO	CISO	Legal	Engineering lead	Business owner
Approve an AI use case to run	I	A	C	C	R	R
Set an agent's decision boundary	I	C	C	C	R	A
Approve a new tool or MCP server		I	A	C	R	C
Approve an agent's write actions, schedule or past-quota running		I	C	I	R	A
Name who can stop each agent and record the last proven stop	I	I	A	I	R	C
Sign the report when an agent causes an incident	I	C	A	C	C	R
Approve an outside data recipient		I	C	A	R	C
Approve a model change		I	C	I	R	A
Publish the AI Acceptable Use Policy	I	C	A	R	C	C
Accept the Executive Risk Report	A	R	R	C	C	C
Confirm role-based training completion	I	I	A	I	R	R

Each row needs exactly one A.

Generate these records in one guided session at https://sanctumshield.com. Terms: sanctumshield.com/glossary (Proven Stop, MCP Gateway, Retrieval Provenance Record). Training: Academy module M20, academy.sanctumshield.com/curriculum. Last updated October 27, 2026. Educational template, not legal advice.