Sample. A real export of Sixi Assure from a demo design; the organisation and the vendor are fictional. Exports carry a detached Ed25519 signature, which is not included with this sample.

Handover pack — Claims assistant

Design-time handover pack from the architecture model. Sixi Assure assesses and evidences what the design declares about each agent and about who answers for it, at the version named below. It is not a sign-off of the handover and not a statement that an operated agent matches the design.

Field	Value
Organisation	example-insurance
Architecture	Claims assistant (arch_4lgq4v5puzezpiyw)
Version	1
Model hash	0d82f5fa7033a7cebd7099ce580ec6ddebda59d44af46c8122112ea77fd724f4
Evidence chain head	a1e45d770bce3e7289a85eba836bb6cb076e1f8e0c401c49f49f804b775c2c8e
Architecture owner	Acme Consulting (vendor)
Architecture sponsor	not declared
Generated	2026-11-20T12:39:32Z

Summary

What	Count
Agents	4
Agents with no owner declared	1
Agents that do not declare a kill switch	1
Parties the design names	4
Required owners that are empty	1
Open findings that concern an agent	1
Of those, critical or high	0

What the design declares about each agent and about who answers for it, with the open findings the rules raised. It records the declared design at one version; it is not a statement that an operated agent matches it.

Who is named, and for what

Every owner, sponsor and approver the design names, grouped by the name as written. "Nobody else named" marks a role that has no second name on the same element.

Acme Consulting (vendor)

23 roles; 14 where nobody else is named; bears on 4 agents.

Role	On	Type	Also named	Bears on	Can stop
owner	Claims assistant	architecture	nobody else named	—	—
owner	Agent evaluation (n_eval)	evaluation	nobody else named	—	—
owner	Agent log archive (n_logs)	log_sink	nobody else named	—	—
owner	Agent registry (n_registry)	agent_registry	nobody else named	—	—
owner	Analyst specialist (n_analyst)	agent	Head of Digital Operations	Analyst specialist	—
owner	Assistant web app (n_web)	app	Head of Digital Operations	—	—
owner	Calculation specialist (n_coder)	agent	Head of Digital Operations	Calculation specialist	—
owner	Case assistant (Microsoft Agent Framework) (n_system)	app	nobody else named	—	—
owner	Case records (n_records)	datastore	nobody else named	—	—
owner	Foundry hosted agent: Analyst specialist (n_analyst_host)	app	nobody else named	—	—
owner	Foundry hosted agent: Calculation specialist (n_coder_host)	app	nobody else named	—	—
owner	Foundry hosted agent: Case writer specialist (n_writer_host)	app	nobody else named	—	—
owner	Foundry hosted agent: Workflow orchestrator (n_orch_host)	app	nobody else named	—	—
owner	Key vault (n_secrets)	secret_store	nobody else named	—	—
owner	Market data MCP server (n_mcp_docs)	mcp_server	nobody else named	—	—
owner	Model endpoint (n_llm)	llm_endpoint	nobody else named	—	—
owner	Session store (Foundry hosting) (n_sessions)	datastore	nobody else named	—	—

Role	On	Type	Also named	Bears on	Can stop
owner	Workflow orchestrator (n_orch)	agent	Head of Digital Operations	Workflow orchestrator	—
owner	Analyst specialist identity (id_analyst)	agent_identity	Head of Digital Operations	Analyst specialist	—
owner	Calculation specialist identity (id_coder)	agent_identity	Head of Digital Operations	Calculation specialist	—
owner	Case writer specialist identity (id_writer)	agent_identity	Head of Digital Operations	Case writer specialist	—
owner	Web app workload identity (id_web)	workload_identity	Head of Digital Operations	—	—
owner	Workflow orchestrator identity (id_orch)	agent_identity	Head of Digital Operations	Workflow orchestrator	—

analyst

1 role; 1 where nobody else is named; bears on 1 agent.

Role	On	Type	Also named	Bears on	Can stop
approver	Code run approval (n_code_approval)	human_step	nobody else named	Calculation specialist	—

Head of Digital Operations

9 roles; 0 where nobody else is named; bears on 4 agents.

Role	On	Type	Also named	Bears on	Can stop
sponsor	Analyst specialist (n_analyst)	agent	Acme Consulting (vendor)	Analyst specialist	—
sponsor	Calculation specialist (n_coder)	agent	Acme Consulting (vendor)	Calculation specialist	—
sponsor	Case writer specialist (n_writer)	agent	Acme Consulting (vendor)	Case writer specialist	—
sponsor	Workflow orchestrator (n_orch)	agent	Acme Consulting (vendor)	Workflow orchestrator	—
sponsor	Analyst specialist identity (id_analyst)	agent_identity	Acme Consulting (vendor)	Analyst specialist	—
sponsor	Calculation specialist identity (id_coder)	agent_identity	Acme Consulting (vendor)	Calculation specialist	—
sponsor	Case writer specialist identity (id_writer)	agent_identity	Acme Consulting (vendor)	Case writer specialist	—
sponsor	Web app workload identity (id_web)	workload_identity	Acme Consulting (vendor)	—	—
sponsor	Workflow orchestrator identity (id_orch)	agent_identity	Acme Consulting (vendor)	Workflow orchestrator	—

operations

1 role; 1 where nobody else is named; bears on 1 agent.

Role	On	Type	Also named	Bears on	Can stop
approver	Action approval (n_approval)	human_step	nobody else named	Case writer specialist	—

Owners nobody is named for

Role	On	Type	Also named	Bears on	Can stop
owner	Case writer specialist (n_writer)	agent	Acme Consulting (vendor), Head of Digital Operations	Case writer specialist	—

Agent passports

Analyst specialist

Field	Value
Element	n_analyst
Purpose	Reads market data through the MCP gateway and drafts the analysis; it changes nothing.
Autonomy	semi
Owner	Acme Consulting (vendor)
Sponsor	Head of Digital Operations
Runs on	Foundry hosted agent: Analyst specialist
Framework	ms_agent_framework
Hosting	not declared
Environment	not declared
Identity type	agent_id
Runs as	Analyst specialist identity (id_analyst, agent_identity)
Identity reference	not declared
Identity issuer	https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555/v2.0
Credential	federated, lifetime 3600 s
Identity owner	Acme Consulting (vendor)

Field	Value
Identity sponsor	Head of Digital Operations
Tool scopes	not declared
Kill switch	yes
Rate limit	yes
Kill switch operated by	no identity named
max_instances	not declared
max_iterations	10
max_tool_calls	20
max_duration_s	300
max_token_budget	not declared
max_retries	not declared

Called by

Component	Type	Edge	Authentication
Foundry hosted agent: Analyst specialist	app	calls	managed_identity
Workflow orchestrator	agent	delegates	obo

Models

Endpoint	Provider	Model	Region	Through	Authentication
Model endpoint	azure	gpt-4.1	switzerlandnorth	AI gateway	managed_identity

Tools and MCP servers

Name	Type	Origin	Through	Authentication	Scopes on the call	Allowed tools	Capabilities	Write capable	Vetted
Market data MCP server	mcp_server	first_party	MCP gateway	token_exchange	not declared	not declared	queries_database	no	yes

Reaches (along declared edges; a reading aid, not the reachability the rules assess)

Name	Type	Through	Access	Authentication	Data classes	Holds credentials
Agent log archive	log_sink	direct	writes	agent_id	internal	not declared

Approvals

The design declares no human approval for this agent.

Hands work to

It hands work to no other agent.

Open findings of the rules

The rules raise no open finding that concerns this agent.

Calculation specialist

Field	Value
Element	n_coder
Purpose	Runs calculations as code in a WebAssembly sandbox after an operator approves the run.
Autonomy	semi
Owner	Acme Consulting (vendor)
Sponsor	Head of Digital Operations
Runs on	Foundry hosted agent: Calculation specialist
Framework	ms_agent_framework
Hosting	not declared
Environment	not declared
Identity type	agent_id
Runs as	Calculation specialist identity (id_coder, agent_identity)
Identity reference	not declared
Identity issuer	https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555/v2.0
Credential	federated, lifetime 3600 s
Identity owner	Acme Consulting (vendor)
Identity sponsor	Head of Digital Operations
Tool scopes	not declared
Kill switch	not declared

Field	Value
Rate limit	yes
Kill switch operated by	no identity named
max_instances	not declared
max_iterations	10
max_tool_calls	20
max_duration_s	300
max_token_budget	not declared
max_retries	not declared

Called by

Component	Type	Edge	Authentication
Foundry hosted agent: Calculation specialist	app	calls	managed_identity
Workflow orchestrator	agent	delegates	obo

Models

Endpoint	Provider	Model	Region	Through	Authentication
Model endpoint	azure	gpt-4.1	switzerlandnorth	AI gateway	managed_identity

Tools and MCP servers

Name	Type	Origin	Through	Authentication	Scopes on the call	Allowed tools	Capabilities	Write capable	Vetted
Hyperlight CodeAct	tool	first_party	Code run approval	managed_identity	not declared	not declared	executes_code	no	yes

Reaches (along declared edges; a reading aid, not the reachability the rules assess)

Name	Type	Through	Access	Authentication	Data classes	Holds credentials
Agent log archive	log_sink	direct	writes	agent_id	internal	not declared

Approvals

Kind	Tool class or step	Disposition or role	Approves	Stands in front of
Human step	Code run approval	analyst	code_run	Hyperlight CodeAct

Hands work to

It hands work to no other agent.

Open findings of the rules

The rules raise no open finding that concerns this agent.

Case writer specialist

Field	Value
Element	n_writer
Purpose	Proposes case record updates that an operator approves before they are written.
Autonomy	semi
Owner	not declared
Sponsor	Head of Digital Operations
Runs on	Foundry hosted agent: Case writer specialist
Framework	ms_agent_framework
Hosting	not declared
Environment	not declared
Identity type	agent_id
Runs as	Case writer specialist identity (id_writer, agent_identity)
Identity reference	not declared
Identity issuer	https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555/v2.0
Credential	federated, lifetime 3600 s
Identity owner	Acme Consulting (vendor)
Identity sponsor	Head of Digital Operations
Tool scopes	not declared
Kill switch	yes
Rate limit	yes
Kill switch operated by	no identity named

Field	Value
max_instances	not declared
max_iterations	10
max_tool_calls	20
max_duration_s	300
max_token_budget	not declared
max_retries	not declared

Called by

Component	Type	Edge	Authentication
Foundry hosted agent: Case writer specialist	app	calls	managed_identity
Workflow orchestrator	agent	delegates	obo

Models

Endpoint	Provider	Model	Region	Through	Authentication
Model endpoint	azure	gpt-4.1	switzerlandnorth	AI gateway	managed_identity

Tools and MCP servers

Name	Type	Origin	Through	Authentication	Scopes on the call	Allowed tools	Capabilities	Write capable	Vetted
Record update tool	tool	first_party	Action approval	managed_identity	not declared	not declared	modifies_state	yes	yes

Reaches (along declared edges; a reading aid, not the reachability the rules assess)

Name	Type	Through	Access	Authentication	Data classes	Holds credentials
Agent log archive	log_sink	direct	writes	agent_id	internal	not declared
Case records	datastore	Action approval → Record update tool	writes	managed_identity	internal	not declared

Approvals

Kind	Tool class or step	Disposition or role	Approves	Stands in front of
Human step	Action approval	operations	record_update	Record update tool

Hands work to

It hands work to no other agent.

Open findings of the rules

Severity	Rule	Finding	Clauses
medium	AI-005	Incomplete AI inventory fields	FINMA:08/2024:Inventory

Workflow orchestrator

Field	Value
Element	n_orch
Purpose	Runs the declarative workflow: routes each case to the specialists in a fixed order.
Autonomy	semi
Owner	Acme Consulting (vendor)
Sponsor	Head of Digital Operations
Runs on	Foundry hosted agent: Workflow orchestrator
Framework	ms_agent_framework
Hosting	not declared
Environment	not declared
Identity type	agent_id
Runs as	Workflow orchestrator identity (id_orch, agent_identity)
Identity reference	not declared
Identity issuer	https://login.microsoftonline.com/11111111-2222-3333-4444-555555555555/v2.0
Credential	federated, lifetime 3600 s
Identity owner	Acme Consulting (vendor)
Identity sponsor	Head of Digital Operations
Tool scopes	not declared
Kill switch	yes
Rate limit	yes
Kill switch operated by	no identity named

Field	Value
max_instances	not declared
max_iterations	10
max_tool_calls	20
max_duration_s	300
max_token_budget	not declared
max_retries	not declared

Called by

Component	Type	Edge	Authentication
Foundry hosted agent: Workflow orchestrator	app	calls	managed_identity

Models

Endpoint	Provider	Model	Region	Through	Authentication
Model endpoint	azure	gpt-4.1	switzerlandnorth	AI gateway	managed_identity

Tools and MCP servers

No tool or MCP server on a declared path.

Reaches (along declared edges; a reading aid, not the reachability the rules assess)

Name	Type	Through	Access	Authentication	Data classes	Holds credentials
Agent log archive	log_sink	direct	writes	agent_id	internal	not declared
Per-user session history	agent_memory	direct	reads, writes	agent_id	internal	not declared

Approvals

The design declares no human approval for this agent.

Hands work to

Agent	Type	Through	Edge	Authentication	Mode
Analyst specialist	agent	direct	delegates	obo	as_tool
Case writer specialist	agent	direct	delegates	obo	as_tool
Calculation specialist	agent	direct	delegates	obo	as_tool

Open findings of the rules

The rules raise no open finding that concerns this agent.

Citations

Clause	Title
FINMA:08/2024:Inventory	AI inventory and risk classification

Disclaimers

AIACT: Sixi Assure assesses your architecture against the cited provisions of Regulation (EU) 2024/1689 as amended and evidences the design decisions you record; it does not provide legal advice, conformity assessment or certification.

OWASP: Sixi Assure assesses your architecture against the cited OWASP guidance and evidences the design decisions you record; it does not provide legal advice, a security test or certification.

default: Sixi Assure assesses this design against the selected regulatory expectations and evidences the result. This is assessment support, not legal advice; the official source text prevails.

Sixi Assure assesses this design against the selected regulatory expectations and evidences the result. This is assessment support, not legal advice; the official source text prevails.