



folium

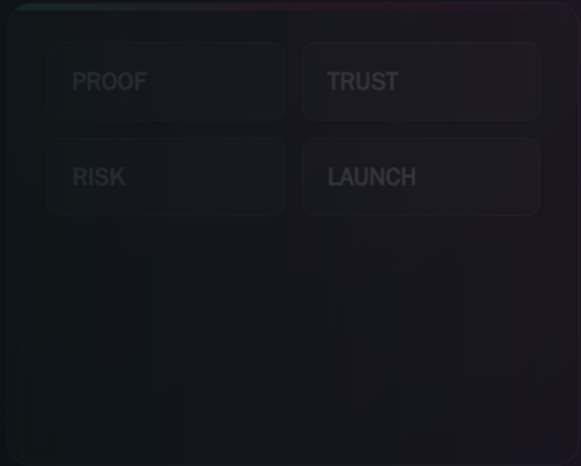
PUBLIC-FACING PDF

REVIEW BEFORE PRODUCTION

FOLIUM SYSTEMS

KNOWN-CLAIMS AND ACTION-MANIFEST ANSWER GUARD

Known-Claims And Action- Manifest Answer Guard



AI advisors drift when they are only governed by broad prompts. Folium can build known-claims registers and action manifests so an advisor knows what is approved, what is blocked, what the system state actually says, which tools it may use, and when a human must decide.

AUDIENCE

AI product owners, support leaders, sales teams, technical buyers, risk reviewers, and agentic-workflow teams

PURPOSE

Show how Folium controls both what an AI advisor may say and what it may do

UPDATED

May 2026

Approved facts, blocked claims, and source records should be explicit.

Action authority should be separated into read, draft, recommend, route, update, execute, block, and escalate states.

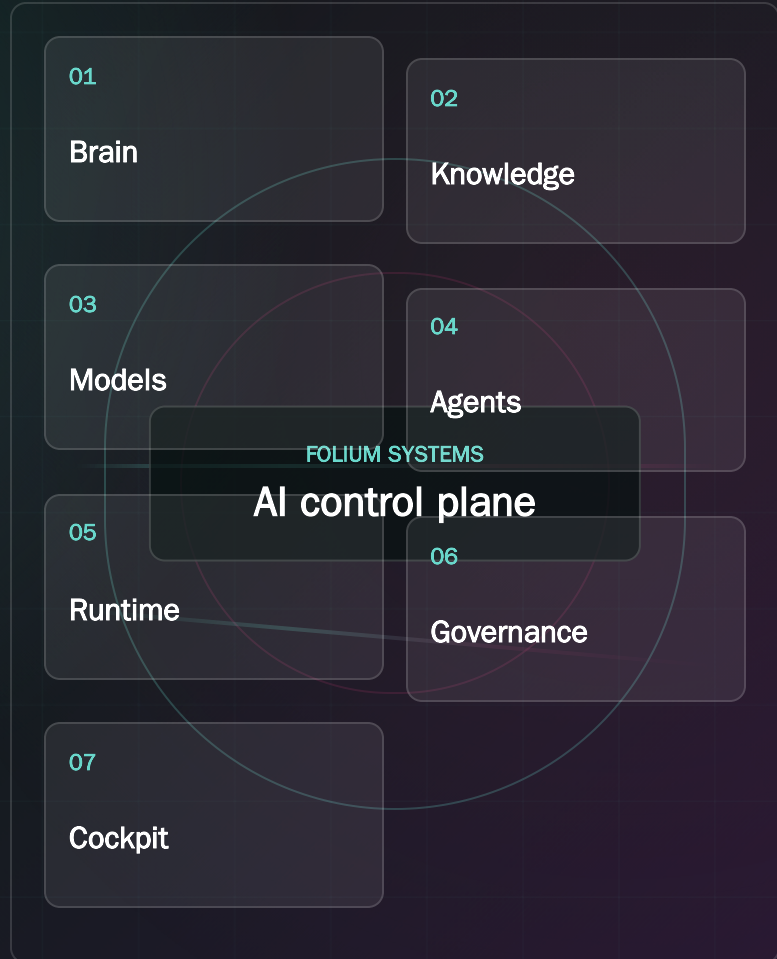
High-risk advisor behavior should pass deterministic scenarios and trace review before promotion.

AI CONTROL PLANE

AI orchestration becomes useful when the business owns the brain and the rules.

The control plane connects source truth, neural knowledge lanes, model routes, agent fleets, runtime placement, governance gates, and operating records into one reviewable system.

AI CONTROL PLANE



01

Shows Folium can coordinate many AI parts without selling unmanaged autonomy.

02

Makes mass agent management a controlled fleet discipline with roles, logs, and lifecycle records.

03

Connects cloud, local, private, containerized, virtualized, and hybrid placement patterns to public-safe workload routing.

Choose the review route before reading cover to cover.

This packet is meant to support a real decision meeting. Different reviewers should enter through different routes, then come back together around the same controlled next step.

DECISION ROUTE

EXECUTIVE ROUTE

Decision first

Start with the cover, visual summary, executive read, controls, first ninety days, and handoff. This route helps leaders decide whether the next move is education, audit, first build, pilot, or operations.

- Outcome
- Risk
- Owner
- Next gate

OPERATING ROUTE

OPERATIONS ROUTE

How the work will run

Read the workflow map, procedures, operating roles, metrics, first sprint, and buyer worksheet. This route shows whether staff can actually use, review, and improve the future process.

- Workflow
- Staff
- Support
- Improve

TRUST ROUTE

TECHNICAL AND TRUST ROUTE

Where the boundaries live

Focus on records and work products, controls, risk assumptions, reference work products, source truth, runtime placement, and launch conditions before any private access expands.

- Source
- Access
- Runtime
- Rollback

BUYER SESSION ROUTE

Turn reading into a working session

Use the discovery questions, role review route, buyer worksheet, and engagement fit ladder to prepare one process, one owner, one source map, and one next decision.

- Process
- Examples
- Questions
- Decision

Best use: bring one workflow, the people who own it, the systems it touches, the data classes involved, and the decision this packet should help leadership make.

Known-claims and action-manifest answer guard in plain language.

AI advisors drift when they are only governed by broad prompts. Folium can build known-claims registers and action manifests so an advisor knows what is approved, what is blocked, what the system state actually says, which tools it may use, and when a human must decide.

RECORD

BOUNDARY

ACTION

CLAIMS

Approved facts become records

The advisor answers from approved claims, source pointers, aliases, and current system-state fields.

- Fact
- Source
- State

BLOCKS

Unsupported claims stop

Private facts, regulated claims, missing sources, stale state, and risky promises route to refusal or escalation.

- Block
- Refuse
- Escalate

ACTIONS

Tool authority is visible

Read, draft, recommend, route, update, execute, block, and escalate actions are scoped.

- Read
- Draft
- Execute

TESTS

Scenarios hold the line

Deterministic scenario banks, trace logs, and eval gates test high-risk behavior.

- Scenario
- Trace
- Gate

This packet is public-facing. It is written for serious review without exposing private infrastructure, customer data, credentials, live provider wiring, or internal project labels.

The operating path should be visible before anyone trusts the outcome.

Folium uses workflow maps to turn broad AI ambition into inspectable work. Each phase names the procedure, the visible output, and the decision gate that prevents excitement from outrunning control.

DECISION GRID

REVIEW LENS

NEXT STEP

PHASE	PROCEDURE	VISIBLE OUTPUT	DECISION GATE
Register claims	List approved facts, source records, aliases, system-state fields, blocked claims, and sensitive topics.	Known-claims register.	The advisor has truth boundaries.
Map actions	Classify read, draft, recommend, route, update, execute, block, and escalate actions by role and data class.	Action manifest.	Tool authority is scoped.
Write refusal states	Define when the AI should say it does not know, ask for a source, refuse, qualify, or escalate.	Blocked-claim rules.	Unsupported output stops.
Build scenarios	Create deterministic tests for aliases, risky prompts, state changes, missing sources, and action boundaries.	Scenario bank.	Behavior can be verified.
Release with traces	Review logs, eval results, escalation notes, failed cases, and owner signoff before promotion.	Advisor release gate.	Promotion is evidence-backed.

The work should leave behind material a buyer can inspect.

A serious engagement should produce more than conversation. Folium packages records, diagrams, checklists, routes, system surfaces, launch gates, and handoff material so the buyer can keep control after the first win.

DECISION GRID

REVIEW LENS

NEXT STEP

WORK PRODUCT	WHAT IT CONTAINS	HOW THE REVIEWER USES IT
Known-claims register	Approved facts, sources, aliases, states, blocked claims, and update owners.	Controls answers.
Action manifest	Tool scopes, data classes, action classes, approvals, logs, and rollback expectations.	Controls authority.
Blocked-claim rules	Refusal, qualification, source request, escalation, and human review states.	Prevents unsupported claims.
Deterministic scenario bank	Expected behavior for high-risk questions, aliases, state changes, and action requests.	Makes behavior testable.
Trace log review	Prompt, retrieved source, claim used, action proposed, escalation, and decision.	Shows why the advisor behaved as it did.

The procedure is the product as much as the technology.

The goal is not to make AI look impressive for one meeting. The goal is to make the operating path repeatable, explainable, reviewable, and safe enough to improve.

CHECKLIST

OWNER PATH

RELEASE SIGNAL

- Do not rely on a prompt alone for high-risk advisor behavior.
- List approved facts and source records.
- List blocked claims, unsupported topics, private terms, and escalation triggers.
- Separate answer authority from action authority.
- Test aliases and state changes with deterministic scenarios.
- Keep private customer data, credentials, contracts, private topology, private model names, and internal project labels out of public review material.
- Use explicit public-safe boundaries when work touches providers, money, regulated-adjacent review, customer-impacting actions, or live operating authority.
- Leave behind records that a buyer can inspect: source, scope, owner, date, evidence class, known limits, blocked states, and next-stage gate.

Governance, quality, and launch gates keep speed honest.

Folium keeps the buyer's next decision tied to observable gates: source truth, authority, access, testing, ownership, support, rollback, and improvement cadence.

DECISION GRID

REVIEW LENS

NEXT STEP

GATE	WHAT MUST BE TRUE	STOP OR REFINE SIGNAL
Claim gate	Approved facts and sources exist.	Advisor can invent.
Block gate	Unsupported, private, stale, or regulated claims are blocked or escalated.	Risky claims pass.
Action gate	Tool calls have role, data, owner, approval, and log rules.	Tool authority is hidden.
Scenario gate	High-risk cases pass deterministic tests.	Only ad hoc prompts were tried.
Trace gate	Reviewers can inspect why the advisor answered or acted.	No behavior audit is possible.

The right questions expose the real project.

These prompts help a buyer and Folium decide whether the next step should be education, audit, first build, security review, pilot, or an operating support path.

CHECKLIST

OWNER PATH

RELEASE SIGNAL

- Which claims are approved?
- Which claims are blocked?
- Which system-state fields should ground answers?
- Which tools can the advisor use?
- Which scenarios must pass before release?
- Which proof can be public and which proof must stay private?
- Which owner can approve the next stage?
- What would make the workflow pause, rollback, or stay blocked?

Diagrams, charts, and overlays make the work easier to review.

Dense AI work should not only be explained in paragraphs. The reviewer should be able to inspect maps, scorecards, matrices, lanes, and before-after views that reveal where the value and risk live.

RECORD

BOUNDARY

ACTION

Claim guard map

Approved fact, source, alias, state, blocked claim, escalation.

- Fact
- Source
- Block
- Escalate

Action manifest ladder

Read, draft, recommend, route, update, execute, block, escalate.

- Read
- Draft
- Execute
- Block

Scenario release loop

Scenario, expected behavior, trace, eval, repair, owner signoff.

- Test
- Trace
- Repair
- Sign

Every serious AI path needs named owners before it becomes dependency.

The same technology can be safe or unsafe depending on who owns the workflow, data, quality, launch authority, support, and improvement loop. Folium makes those responsibilities explicit so no buyer inherits an orphaned system.

DECISION GRID

REVIEW LENS

NEXT STEP

ROLE	OWNS	RECORD TO INSPECT
Executive sponsor	Priority, budget, risk tolerance, stop/continue decision, and expansion timing.	Decision note, value hypothesis, and approval boundary.
Business process owner	The day-to-day work, acceptance criteria, staff impact, and operational usefulness.	Workflow map, user feedback, and adoption notes.
Technical owner	Systems, APIs, databases, runtime placement, deployment, monitoring, and fallback.	Architecture map, integration log, and support route.
Knowledge owner	Source truth, document freshness, policies, retrieval scope, and correction workflow.	Source inventory, freshness cadence, and review exceptions.
Security or risk reviewer	Data classes, credentials, access, logs, retention, blocked actions, and incident path.	Boundary map, permission table, and rollback trigger.
Folium delivery lead	Build coordination, review file, known limits, quality checks, and handoff completeness.	Launch room, eval record, and improvement backlog.

A max-detail packet should tell reviewers how to judge the work.

Folium uses scorecards to make a subjective AI conversation more inspectable. The score is not a substitute for judgment; it helps leadership see whether the next step is education, repair, sandbox, pilot, or operations.

DECISION GRID

REVIEW LENS

NEXT STEP

SCORE AREA	STRONG SIGNAL	WEAK SIGNAL
Business fit	The workflow is specific, painful, owned, and tied to measurable operational improvement.	The project is framed as adding AI generally.
Source truth	Approved sources are known, fresh, classified, and connected to the answer path.	The system mixes stale, unknown, or unapproved sources.
Behavior quality	Representative tasks pass, wrong-answer behavior is known, and edge cases are recorded.	The review build only shows a polished happy path.
Authority control	AI actions are separated into draft, retrieve, recommend, route, execute, block, and escalate.	The system can act without visible permission.
Staff readiness	Users can explain the tool, correct it, escalate, and understand their role.	Staff feel replaced, confused, or unsupported.
Operations readiness	Support, monitoring, rollback, release rhythm, and source refresh are owned.	No one knows who maintains the system after launch.

The work should have a believable first ninety days.

A controlled first ninety days keeps ambition high without turning uncertainty into production risk. Folium uses the period to move from understanding into a narrow working example, then into reviewable operating rhythm.

DECISION GRID

REVIEW LENS

NEXT STEP

WINDOW	FOCUS	EXPECTED OUTPUT
First 30 days	Discovery, source inventory, first-lane selection, staff interviews, data boundary, and build plan.	Process map, owner map, first-build scope, source list, and launch blockers.
Days 31-60	Working surface, RAG or agent behavior, integration stub, evaluation cases, browser checks, and staff review.	Sandbox, evaluation file, screenshots, known limits, and repair list.
Days 61-90	Architecture review, pilot conditions, governance layer, training guide, support path, and improvement cadence.	Launch room, go/no-go record, operations guide, and next-stage recommendation.

The hidden assumptions should be visible before they become expensive.

Every AI engagement contains assumptions about data, people, systems, cost, behavior, and authority. Folium treats those assumptions as review material, not background noise.

DECISION GRID

REVIEW LENS

NEXT STEP

ASSUMPTION	WHY IT MATTERS	HOW FOLIUM REVIEWS IT
The source is authoritative	AI can only be as reliable as the sources and business rules it is allowed to use.	Source inventory, owner confirmation, retrieval tests, freshness cadence.
The process is ready	A broken process can become a faster broken process when AI is added too early.	Workflow mapping, bottleneck review, owner interview, first-lane narrowing.
The runtime fits the data	Cloud, private, local, and hybrid routes carry different privacy, cost, latency, and support tradeoffs.	Runtime matrix, data classification, provider review, fallback plan.
Staff will adopt the tool	Adoption fails when users do not understand, trust, correct, or benefit from the system.	Training notes, staff review, feedback loop, manager visibility.
Authority is clear	The system can create harm if it sends, updates, approves, or routes without permission.	Permission table, blocked actions, human review, audit trail.
The system can be supported	A useful first build becomes fragile if nobody owns incidents, source updates, or cost review.	Support guide, owner map, release rhythm, rollback trigger.

The first sprint should produce something real and reviewable.

Folium prefers a narrow first sprint that creates a working surface or review file the buyer can challenge. The first sprint is not the final system; it is the safest way to make the future visible.

CHECKLIST

OWNER PATH

RELEASE SIGNAL

- Confirm the single process and the decision the sprint must support.
- Collect approved example material, redacted review records, public references, screenshots, workflow notes, and source rules.
- Define what will be built: portal, dashboard, RAG assistant, agent route, integration adapter, audit file, or launch room.
- Create the visual workflow: intake, source, model or agent route, human review, output, record, and next gate.
- Run representative tasks, edge cases, bad input, missing data, and blocked-action tests.
- Prepare browser screenshots, known limits, support questions, and next-stage blockers.
- Review with staff and leadership before expanding data, access, authority, or dependency.
- End with a decision: stop, refine, rebuild, pilot, or prepare an operating plan.

The packet should make the invisible work tangible.

AI work often fails because the important pieces are invisible until something breaks. Folium turns those pieces into work products the buyer can open, print, challenge, and improve.

RECORD

BOUNDARY

ACTION

Process map

A before-and-after workflow showing people, systems, data, decision points, blockers, and expected output.

- Before
- After
- Owner
- Gate

Data boundary map

A map of source classes, approved use, blocked use, retention, provider exposure, and custody.

- Public
- Internal
- Private
- Blocked

Model and agent route

A path showing which model, tool, retrieval source, or agent lane is used and where humans approve.

- Route
- Tool
- Review
- Escalate

Evaluation file

A record of tasks, expected outcomes, failures, repairs, known limits, and acceptance criteria.

- Cases
- Failures
- Repairs
- Limits

Launch room

A board for owners, support, training, rollback, incidents, go/no-go, and improvement backlog.

- Owner
- Support
- Rollback
- Backlog

Handoff guide

A plain-language guide staff can use to understand what the system does, cannot do, and how to report problems.

- Use
- Limit
- Correct
- Report

The business should know how improvement will be measured.

Folium keeps measurement practical. The first goal is not a perfect dashboard; it is a clear set of signals that shows whether the process is saving time, reducing risk, strengthening staff, or improving customer outcomes.

DECISION GRID

REVIEW LENS

NEXT STEP

SIGNAL	WHAT TO WATCH	DECISION IT SUPPORTS
Time recovered	Manual steps removed, average handling time, repeated work reduced, faster routing.	Should this workflow expand to more users or adjacent processes?
Quality improved	Wrong answers, missing sources, correction rate, review exceptions, customer rework.	Is behavior strong enough for pilot or does it need repair?
Risk reduced	Blocked unsafe actions, escalations, data-boundary violations avoided, rollback readiness.	Can authority expand or should controls remain tight?
Staff confidence	Training completion, feedback volume, adoption friction, override rate, manager notes.	Does the workforce need more support before launch?
Cost and runtime	Provider cost, local infrastructure cost, latency, uptime, fallback use, subscription sprawl.	Should runtime placement change?
Customer impact	Response speed, consistency, issue resolution, conversion support, satisfaction signals.	Is the capability improving the business outcome?

Each reviewer should know what to inspect first.

A max-detail packet is only useful when different reviewers can find their lane quickly. Folium separates executive, operations, technical, security, finance, and staff questions so the buyer can bring the right people into the right part of the review.

DECISION GRID

REVIEW LENS

NEXT STEP

REVIEWER	START WITH	DECISION THEY SUPPORT
Executive sponsor	Value hypothesis, launch gate, first ninety days, and stop/refine/continue choices.	Whether the process deserves a controlled engagement.
Operations lead	Workflow map, operating roles, support rhythm, and staff feedback loop.	Whether the future process can be run by the team.
Technical lead	Runtime placement, data path, integration surface, monitoring, and fallback.	Whether the architecture can be supported safely.
Security or risk reviewer	Data classes, permissions, blocked actions, logs, retention, and rollback.	Whether access can expand beyond public review.
Finance or owner	Cost signals, subscription overlap, runtime tradeoffs, labor impact, and support burden.	Whether the first build has a practical business case.
Staff user	Plain-language use, limits, escalation, correction path, and training expectations.	Whether the tool strengthens the job instead of confusing it.

The packet should turn into a working session, not only reading material.

Before a call, Folium wants the buyer to gather the real operating pieces that make the review useful. The worksheet keeps the conversation grounded in one process, one owner, one source map, and one next decision.

CHECKLIST

OWNER PATH

RELEASE SIGNAL

- Bring one workflow that is slow, risky, expensive, repetitive, customer-visible, or staff-heavy.
- Name the systems touched by the workflow: store, CRM, ERP, inbox, spreadsheet, database, portal, document folder, or legacy application.
- Separate approved public material from internal, customer, regulated, confidential, credential, and blocked material.
- Write down who owns the work today, who reviews exceptions, and who will own the AI-assisted version.
- List the decisions AI may draft, retrieve, recommend, route, block, or escalate, and the decisions that stay human-owned.
- Bring examples of good output, bad output, common exceptions, missing data, and customer-facing risk.
- Name the first useful working surface: dashboard, portal, assistant, queue, control room, commerce lane, integration, or review file.
- Decide what record would make leadership comfortable with the next stage.

The next step should match the maturity of the record.

Folium does not need every buyer to start at the same altitude. The right offer depends on how much process clarity, source truth, owner alignment, and launch readiness already exists.

DECISION GRID

REVIEW LENS

NEXT STEP

IF THE BUYER HAS	BEST NEXT FOLIUM MOVE	OUTPUT TO EXPECT
AI interest but no clear process	AI systems audit or first workflow finder.	Pressure map, source inventory, first-lane recommendation, and risk view.
A clear process but no working surface	Forward engineering first sprint.	Clickable surface, route map, known limits, and next-stage blockers.
A tool that works in parts but not in operations	Architecture and launch readiness review.	Permission map, runtime decision, support model, and go/no-go record.
A failed or frightening rollout	AI recovery and staff enablement path.	Issue register, staff training plan, repair roadmap, and confidence loop.
Sensitive data or cost pressure	Local, private, or hybrid AI placement review.	Runtime matrix, data custody plan, fallback route, and vendor-exit view.
A useful pilot that needs care	AI operations support.	Monitoring rhythm, source refresh, release notes, incident path, and improvement backlog.

The last page of a packet should create the next controlled move.

Folium's handoff view separates what can be done now, what needs customer records, what needs approval, and what should wait until the review file is stronger.

DECISION GRID

REVIEW LENS

NEXT STEP

HANDOFF LANE	OWNER	NEXT RECORD
Business owner	Known-claims and action-manifest guard priority, acceptance criteria, and stop/continue decision.	Workflow decision note and next-stage gate.
Technical owner	Architecture, integrations, runtime placement, data movement, monitoring, and fallback.	Architecture map, route contract, and support guide.
Risk or review owner	Data boundaries, authority classes, blocked actions, evidence, and release conditions.	Boundary map, gate table, and evidence packet.
Operator or support owner	Daily workflow state, exception handling, escalation, recovery, and improvement rhythm.	Queue map, incident route, and operating handoff.
Folium delivery lead	Public-safe build coordination, evaluation, known limits, launch room, and handoff completeness.	Review file, release notes, and improvement backlog.

The strongest next step is narrow: one process, one owner, one source map, one working surface, one review file, and one decision gate.

19

NEXT STEP

An advisor becomes safer when its claims and actions are inspectable.

Use this packet when a copilot, advisor, or agent needs more than prompt-only guardrails.

Bring the process

Name the business process, the systems involved, the people affected, and the decision this PDF should support.

Separate review from production

Keep public examples, sandbox review, pilot access, and production dependency in separate stages with clear owners.

Ask for the record

Request screenshots, browser checks, known limits, launch blockers, support plans, and the next approval path.