

THE ELIOS ENGAGEMENT PACKAGE

# Executive AI Roadmap

What you get when you engage Elios: the standards we bring to every engagement, and the questions each standard puts in front of a named owner before AI touches your work.

## WHAT'S INSIDE

- 01 **ARCHITECTURE**
- 02 **SECURITY · GUARDRAILS · DATA**
- 03 **IDENTITY · ACCESS**
- 04 **MEASUREMENT**
- 05 **COMPLIANCE**
- 06 **CAPABILITY TRANSFER**

# Most organizations see no P&L return from AI.

## Our engagements are designed to show one.

---

### THE EVIDENCE

MIT's Project NANDA reported in 2025 that 95% of organizations were getting zero return from their enterprise investment in generative AI, and that the vast majority of pilots showed no measurable P&L impact over the study's six-month window. BCG's 2025 study of more than 1,250 firms, The Widening AI Value Gap, puts the share of companies consistently generating substantial value from AI at 5%.

### WHAT WE SEE

In our experience the model is rarely what failed. The failed pilots we are brought in after ran without an agreed architecture, a security standard, an identity model, or a baseline anyone had signed before the work started.

---

### WHAT THIS DOCUMENT DOES

This roadmap is the set of considerations we bring on day one, written from the chair of the executive who answers for the result. It names the questions, including the considerations no one has put in front of you yet.

The answers get decided with you, in your environment, against your policies. Where you already run standards of your own, we meet you where you are and work inside them. Where you run none, ours apply, and where the two differ, we recommend the stricter rule and your named owner makes the call. The standards in this roadmap are ours.

# One rule allocates every workflow.

SOFTWARE

DETERMINISTIC

## Software runs the rules.

Deterministic software performs rules, formulas, thresholds, validation, permissions, deduplication, reconciliation, and exact writes.

AI

INTERPRETIVE

## AI weighs the evidence.

AI interprets bounded, messy evidence and prepares a cited assessment. Bounded means deterministic software selects the exact records the model sees, and nothing else.

PEOPLE

ACCOUNTABLE

## People own the call.

A named, qualified human decides when the model is uncertain or the action is consequential.

Every standard on the following pages exists to hold that allocation in place. How the allocation runs step by step, with worked examples, is the AI-native Journey at [eliosai.com/ai-native-journey](https://eliosai.com/ai-native-journey).

# Where each workflow runs, and how it reaches your systems.

THE QUESTIONS THIS STANDARD SETTLES

- 01 Where do agents run, and in whose tenancy?
- 02 How do they reach your systems: which MCP (Model Context Protocol) connectors or typed APIs, approved by whom?
- 03 Which steps stay in deterministic software, and which systems stay out of reach entirely?
- 04 What happens on a timeout, an unconfirmed write, or an unknown result?

WHAT YOU GET

A written architecture standard for the engagement, agreed between your named owners and Elios before anything runs: where each workflow executes, how it reaches each system, and where deterministic software stays authoritative.

# What a workflow may touch, and what it may never.

THE QUESTIONS THIS STANDARD SETTLES

- 01

What may each workflow read, prepare, or change, and what may it never touch?
- 02

Where do credentials live, and who rotates them?
- 03

What are the schedule, timeout, retry rule, and stop switch for each managed workflow?
- 04

Which model providers process each workflow's data, what do they retain, and is any of it used to train models?
- 05

Which data stays inside which boundary, and how is evidence content handled?

The standard treats it as data, never as instruction, and takes approved values from the deterministic path rather than from model-written text.

WHAT YOU GET

Documented security and guardrail minimum standards for each workflow. Enforcement stays with your identity provider, agent platform, and business systems. These are the control rules a workflow is designed to, not properties of an installed system.

DEPLOYMENT SURFACES WE WORK WITH

HIPAA-eligible model deployments through Azure AI Foundry or Amazon Bedrock under a business associate agreement. Zero-data-retention model options through the Vercel AI Gateway. For on-premises or air-gapped estates, local models delivered with partners who specialize in those engagements.

# Who starts the work, and what it is allowed to do.

An agent's skills are its packaged instructions. Skills tell an agent how to do the work. Its identity, tools, permissions, policies, and approvals decide what it is allowed to do.

THE QUESTIONS THIS STANDARD SETTLES

- 01 Who starts the work: a signed-in person, or an approved event or schedule?
- 02 Which identity does each workflow run under, and with which entitlements?
- 03 Who approves connectors, and which actions need a person's approval before they happen?
- 04 Who owns each workflow by name, and who handles what it cannot resolve?

WHAT YOU GET

An identity model for each workflow, with a named owner, before it runs.

# A baseline before anything changes. A decision date after.

THE QUESTIONS THIS STANDARD SETTLES

- 01
- What does the workflow run at today: time, quality, cost, exceptions, and effort?
- 02
- Who signs that baseline?
- 03
- What standards must the pilot meet, and on what date is the decision made?
- 04
- How do we measure the return: time saved, cost removed, and value created, in terms your CFO accepts?

WHAT YOU GET

A baseline signed by the named business owner before anything changes, pilot standards the business owner and system owner agree before the pilot starts, and a decision date on which those same two owners read the results and choose.

THE DECISION ON THAT DATE

- EXPAND
- REVISE
- KEEP LIMITED
- STOP



# The questions your counsel decides before a workflow runs.

THE QUESTIONS THIS REGISTER NAMES

- 01 Which privacy regimes apply to the data each workflow touches, and in which jurisdictions?
- 02 Where must that data reside, and what may cross which border?
- 03 Does any workflow touch health information covered by HIPAA, or data covered by other sector regulation?
- 04 Do AI-specific rules, such as automated-decision obligations, apply to any workflow, and who classifies it?
- 05 What records must you retain to show who acted, what changed, and under whose approval?

WHAT YOU GET

A compliance consideration register with a named owner for each determination. The determinations belong to your counsel and compliance owners, made before a workflow runs. We bring the questions and the record-keeping standard. We do not practice law.



# Your team runs it after we leave.

That is the design goal, set on day one under Elios OS: Diagnose, Embed & Solve, Transfer.

THE QUESTIONS THIS STANDARD SETTLES

- 01 Who on your team owns each workflow after handover, by name?
- 02 Who operates the approvals, and who handles exceptions?
- 03 What do the runbooks cover, and who gets trained on them?
- 04 Who owns changes after handover: model updates, connector changes, and re-testing against the pilot standards?

WHAT YOU GET

The runbooks, the approval configuration, and the training your people use to operate the workflow, with us alongside for an agreed period. The handover is designed so the capability stays with your team, with no ongoing dependency on Elios.

ELIOS OS

DIAGNOSE

EMBED & SOLVE

TRANSFER

# Give us one problem. Let us prove it.

Start with the workflow whose cycle time or rework rate you can already quote.

## THE ENGAGEMENT

The engagement is fixed-fee. The fee covers the discovery, the access and approval design, the pilot, and the handover. Your AI tool licences and seats stay yours. We quote it after the discovery call, and re-quote it if the scope changes. Everything the engagement writes down, from the baseline to the compliance register, stays yours, whatever the pilot decision.

Your first engagement typically runs four to six weeks. In that time, we stand up your managed agent platform, put agents in your employees' hands, and embed them into at least one real workflow. We price each engagement to where you are on that journey rather than publishing a rate card, because no two clients start from the same place. And we work the way you need us to: embedded alongside your team, or operating as your team. Either way, the capability transfers before we leave.

From you: a named business owner, a system owner, and an approver. A managed workflow also needs an enterprise agent workspace, an identity provider with delegated access, a named authority for approving connectors, a secret store, and a scheduler owner. Discovery confirms what you already have, and a missing prerequisite becomes part of the quoted scope.

## BRING THIS TO THE FIRST CONVERSATION

The workflow, and where it hurts today

Its current cycle time or rework rate

The system owner and the approver by name

**Talk with Elios**

[eliosai.com/talk](https://eliosai.com/talk) · [eliosai.com/executive-ai-roadmap](https://eliosai.com/executive-ai-roadmap)