

PRE-PILOT WORKBOOK / V1

Secure AI Assessment

A structured, unclassified readiness workbook for governments, regulators, and critical institutions to complete before a 90-Day Pilot of Alliance Intelligence.

Secure AI. Under Your Control.

Before any model touches institutional data, the boundary, the policy, and the accountable owner must be established in writing. This workbook produces that record. Complete it internally — no sensitive material needs to leave your institution.

Stage	Timing	Output
Initial institutional contact	Week 0	Mandate, jurisdiction, candidate workflow
Secure AI Assessment	Weeks 1-3	Data boundaries, systems, policy constraints
Architecture and control model	Week 4	Written deployment and enforcement architecture
Pilot definition	Week 5	One workflow, success criteria, accountable owner

Institution record

Institution**Directorate / unit****Executive sponsor****Technical & security owner****Jurisdiction****Date completed**

SECTION 1

Workflow selection

Select one workflow. Pilots that succeed are narrow, repeated, and tied to a decision someone is accountable for.

Candidate workflow

Decision it supports

Frequency / volume

Current time to produce

Qualification checks

- ☐ The workflow is performed repeatedly, not once
- ☐ A named official is accountable for the output
- ☐ The output must be defensible to an oversight body
- ☐ Source material exists in systems we control
- ☐ Failure today has a measurable institutional cost
- ☐ No legal barrier prevents processing this material internally

SECTION 2

Data boundary and classification

List every data class the workflow touches. Record where it may reside and which handling rules apply.

Data class	Classification	May leave premises?	Handling rule / statute

SECTION 3

Systems of record

System	Owner	Access method	Read-only?

SECTION 4

Policy and governance constraints

- ☐ Residency: all processing must remain inside national territory
- ☐ Air-gapped or disconnected operation is required
- ☐ Model outputs must cite their institutional source
- ☐ Retention limits apply to prompts, outputs, and logs
- ☐ Specific data classes are prohibited from any external model
- ☐ Audit records must be exportable to an independent oversight function
- ☐ Role separation is required between operator, reviewer, and administrator

Governing statute / policy

Oversight body

Audit retention period

SECTION 5

Deployment posture

Posture	Applies	Notes
Sovereign on-premise	☐	
Air-gapped enclave	☐	
Government private cloud	☐	
Hybrid (control plane on-premise)	☐	

SECTION 6

Model and vendor neutrality

The control plane governs which models are permitted for which data classes. Record your permitted set and prohibitions.

Data class	Permitted models	Prohibited	Rationale

SECTION 7

Success criteria for the 90-Day Pilot

Criterion	Baseline today	Target at day 90	Evidence accepted

SECTION 8

Accountability and sign-off

Executive sponsor / date

Technical owner / date

Security owner / date

Legal or compliance / date

APPENDIX

What happens after the assessment

Phase	Days	Focus
Discover	0-30	Workflow instrumentation, data boundary enforcement, policy configuration
Deploy	30-60	Control plane in your environment, identity and audit integration
Validate	60-90	Measured outcomes against success criteria, acceptance evidence

Handling note

This template is unclassified. Once completed it may contain sensitive institutional detail — store and transmit it according to your own classification rules. Alliance Intelligence requires only the portions your policy permits you to share.

Next step

Return the sections you are permitted to share, or request a working session with your technical and security owners to complete the architecture and control model.

allianceintelligence.org · [/government-contact](#)