# Sample statement of work — Authority Assurance Engagement

**Sample · final scope agreed per agency.** This document shows the shape of the engagement so an agency can scope and budget it. The executed statement of work names the agency, the actors in scope and the planned term, and goes through the agency's own contracting review.

### 1. The engagement

Cerydora delivers the Authority Assurance Engagement for one agency: a fixed fee of **$32,500**, a term of **six to ten weeks**, and the deliverables in §4. It is offered to Florida public entities. The 30–45-day collection-and-review phase runs inside the engagement, not as a separate service.

### 2. Scope

- **Where it runs.** In the agency's own Microsoft tenant: Entra ID, Azure and Microsoft Sentinel, through the collector bundle, under identities the agency creates. Nothing leaves the tenant.
- **Tier A, cloud,** is where the engagement starts. **Tier B, hybrid** (Active Directory, gMSA, Kerberos and LDAPS on a domain-joined Windows host) starts only when every agency prerequisite passes the preflight; otherwise it is a named follow-on.
- **Actors in scope.** A named set of AI systems and non-human actors — service accounts, app registrations, workload identities, agents — stated by reference to the agency's own configuration record.
- **Not in scope.** Collectors for anything other than Microsoft platforms; AI-policy stand-up; any free engagement; any price other than the fee above.
- **What Cerydora does not do.** Cerydora does not authorize any actor: an official of the agency authorizes, and Cerydora records that decision and shows whether operations stayed inside it. Cerydora does not certify legal or statutory compliance, and does not block, change or remediate anything in the agency's environment.

### 3. Schedule: six to ten weeks

The term runs from the first sealed cycle. Work from signature to that cycle is outside the term, and an open agency prerequisite stops the clock. **T+n** counts weeks of term.

| When | Activity and deliverable | Agency role |
|---|---|---|
| Week 0 | Kickoff. Confirm the Tier A prerequisites and their named owners. | Security lead; prerequisite owners |
| Weeks 0–1 | **Collectors and onboarding.** Install in the agency's tenant: the engine, one identity per collector, collector registration and approval by two different operators, collector start. | Entra and cloud administrators; the two operators |
| T+0 | **First sealed cycle.** The term starts; the date and time are recorded. | — |
| T+0 to T+6 | **Collection-and-review phase** (30–45 days). Observed activity is collected; the agency's reviewer works the review lane with Cerydora. | Reviewer; accountable official |
| T+2 to T+4 | **Authority-exposure baseline.** For each actor in scope: the official, the instrument and the scope of the grant as the agency states it, beside what was observed, with each actor's determination and its reason. | Accountable official; reviewer |
| T+4 to T+8 | **First evidence pack.** The Authorization (PDF/A) signed by the agency's official, the evidence sheets, and the agency's NHA Ledger export. | Accountable official signs |

| When | Activity and deliverable | Agency role |
|---|---|---|
| T+6 to T+10 | Executive findings summary, remediation list, and the reviewer-role definition that keeps the record current after the engagement. | Security lead; accountable official |

### 4. Deliverables

1. **Collectors**, installed in the agency's tenant under agency-created identities, approved by two different agency operators.
2. **Onboarding**: the install, the prerequisite checks, and the two operators and the reviewer in their roles.
3. **Authority-exposure baseline**: declared authority beside observed activity for every actor in scope, each with a determination and its reason. "Not evaluated", with its reason, is a correct outcome where the evidence cannot settle the question.
4. **First evidence pack**: the signed Authorization, the evidence sheets, the NHA Ledger export (the inventory of non-human actors with owners attributed from the agency's directory, gaps shown as gaps), the executive findings summary, the remediation list, and the reviewer-role definition.

### 5. What the agency provides

- **Tenant.** The tenant ID, an Azure subscription in it for the engine, and a subscription for the collectors to read, with Reader on it for their identity.
- **App identity.** Rights to create app registrations, managed identities and app-role assignments, and to grant admin consent for the read-only Graph permissions. The agency performs those consents itself.
- **Named accountable official.** The official who authorizes each actor in scope and signs the Authorization.
- **Named actors in scope.** The set of AI systems and non-human actors the engagement covers, by reference to the agency's configuration record.
- **Two operators who are different people.** One registers collectors, the other approves them; the engine refuses a self-approval.
- **A reviewer**, and an egress path from the collectors to Microsoft Graph, Azure Resource Manager and the engine.

### 6. Acceptance

The agency can run each test itself: a fresh deployment from the documented prerequisites; collection against the agency's tenant under the agency's identities; a determination for every actor in scope; a person the agency names, who is not an engineer, reads three actors' determinations and states what they are and why; and the evidence pack shows, for each finding, the records it rests on.

---

Fee $32,500, fixed, Florida public entities. Final scope, planned term, payment schedule and contract terms are agreed per agency in the executed statement of work. Questions: hello@cerydora.com.