OpenZeppelin Solution Architect, Financial Institutions – Work Trial Instructions

Thank you for your interest in the Solution Architect, Financial Institutions role at OpenZeppelin. This work trial has been designed to evaluate your ability to design security solutions and develop technical proofs-of-concept for tokenization use cases. It simulates the type of work you will be doing in this role.

Overview of the Work Trial

You will complete two exercises over one week (7 days). We expect a total effort of no more than 20-25 hours. Approximately 80% of your focus should be on the Defender Technical Implementation (now referred to as Open Source Security Tooling or OSS Tooling). You will present your deliverables to OpenZeppelin stakeholders during a live session.

We have provided the following resources for your use:

- OpenZeppelin Service Catalog for Financial Institutions (June 2025) – detailing our security services and open-source tooling. See the annex at the end of this document for a summary of key security services offered for financial institutions.
- Solution Architect Role Description – outlining the core responsibilities and expectations for this position.

Your task is to demonstrate how you would use OpenZeppelin's offerings to solve real-world challenges for financial institutions entering the Web3 space.

Exercise 1: Defender Technical Implementation for a Tokenized Bond (80%)

Scenario: A financial institution has issued a tokenized bond on Ethereum. They need an OSS Tooling (formerly Defender)-based monitoring solution for operational risks.

Your Task:

- Define key risks or events to monitor (e.g. missed interest payments, unauthorized transfers, regulatory thresholds).
- Design a Monitor and Relayer-based solution to detect these events and automate appropriate responses.
- Build a demo showcasing how monitors and relayers can interact with a deployed contract.
- Deploy a prototype contract to a testnet for use in the demo.
- Provide sample code/configuration (e.g. Relayer script, Monitor rule logic).
- Document the detection-response strategy and rationale.
- Prepare a presentation deck suitable for an institutional client (~10-15 minutes) to walk through your monitoring solution with an optional but highly recommended live demo
- Desired Outcome: A technical design and prototype showing how you would apply OSS Tooling's Monitors and Relayers (or their open-source equivalents) to deliver operational security for the tokenised bond.

Exercise 2: Solution Design for a Tokenized Money Market Fund (20%)

Scenario: The same financial institution is now looking to launch a tokenized Money Market Fund (MMF) on Ethereum. They are currently struggling to select their oracle tooling.

Your Task:

- Review our service offerings (see annex) and propose a bundled security solution to help the client with their oracle selection and overall MMF security stack.
- Identify and explain other security concerns they should be aware of in their tokenized MMF stack.
- Design an architecture diagram showing how your proposed components interact (e.g. smart contracts, monitoring, Relayers).
- Provide a high-level implementation roadmap.
- Prepare a client-facing presentation deck (10-15 minutes walkthrough).
- Desired Outcome: A coherent, well-justified architecture and service bundle that demonstrates your understanding of financial market security needs and OpenZeppelin's capabilities.

Deliverables Summary

For each exercise:

- Written documentation explaining your solution and rationale.
- Architecture diagram (Exercise 2) and sample code/configs/deployments (Exercise 1).
- Presentation slides suitable for institutional stakeholders.
- Final Presentation
- You will present both exercises in a live session (approximately 30-45 minutes total). This is your opportunity to demonstrate communication skills, defend your design choices, and engage with stakeholders as you would in the role.

How to Approach This Work Trial

- You are encouraged to research and be creative – we want to see independent thinking and initiative.
- Please indicate in your submission how many hours you spent on each exercise.
- Focus on clarity, logic, and relevance – both in design and presentation.

Annex: Key Security Services for Financial Institutions

- Smart Contract Security Audits – Comprehensive code reviews identifying vulnerabilities and recommending fixes.
- Blockchain Infrastructure Security Assessments – Reviews of node-level components, bridges, and backend systems.
- Monitors (OSS Tooling) – Real-time on-chain anomaly detection with customizable alerting.
- Relayers (OSS Tooling) – Secure transaction execution with policy enforcement and gas abstraction.
- Security Advisory & Consulting – Strategic design reviews, best practices, and architecture guidance.
- Incident Response Training & Simulations – Development of incident response plans and live simulation exercises.
- Operational Security Reviews – Assessment of key management, deployment, upgrade governance, and privileged role security.
- We look forward to seeing your solutions and appreciate the time and effort you put into this work test.
- If you have any clarifying questions during the exercise period, feel free to reach out.