Hello everyone,

Immutablelawyer (Joseph) here from [axis advisory]. By way of context, I was recently leading a focus group together with @dk3 so as to spearhead a proposal aimed at creating a 'Procurement Framework' for security-oriented service providers in the ArbitrumDAO. Below, please find our public call for your participation in a public consultation phase so as to solicit input on what you, the ArbitrumDAO community member, think of how the Procurement Framework should be structured.

IMP: The Procurement Framework detailed below is merely a base-line framework aimed at being thought-provoking in nature so as to give some context to community members intending on participating in the public consultation.

Your submissions can be made on the following Google Form:ArbitrumDAO [Security Service Provider Procurement Framework] [Public Consultation]

THE CONSULTATION PERIOD: 10/11/2023 - 22/11/2023 (UPDATED)

(MIDNIGHT)

If you prefer to submit a document-based submission, please do so by sending it to: joseph@axisadvisory.xyz

Introduction

On the 3rd of November, DK (Premia) posted a proposal on the Arbitrum DAO Forums aimed at establishing a framework for security-oriented proposals via a consolidated framework (Proposal: The Arbitrum Coalition). By way of a summary, the proposal on the Arbitrum DAO forum discusses establishing a Request for Proposal (RFP) process to consolidate the selection of auditors and security service providers within the Arbitrum ecosystem (for the purposes of this endeavor, we shall be referring to this consolidated framework as the 'Procurement Framework).

The Snapshot Vote for the establishment of the aforementioned Procurement Framework has since passed Snapshot).

The intent is to replace the current piecemeal approach with a structured, transparent, and fair framework, involving stakeholder participation and administered/facilitated by a Procurement Committee (hereinafter referred to as 'PC). This would involve clear criteria for security professionals' experience, qualifications, and pricing to ensure the ecosystem's security. The process is designed to be inclusive and efficient, open to all security engineers, researchers, and organizations. The committee's role is not one that will involve any form of gatekeeping, but will merely be there to facilitate this process and carry out certain key functions which are part and parcel of the Procurement Process

.

GOALS

1. Draft a preliminary procurement framework that will be used as a baseline to solicit stakeholder input through a public consultation process. The public consultation period will be initiated on the 10th of November and be open for submissions until the 17th of November.
2. During the public consultation period (and immediately following the conclusion thereof) , the intermittent focus group will assess submissions, and iterate on the baseline procurement framework provided in [1] so as to propose an optimised procurement framework in line with stakeholder feedback.
3. Following [1] and [2], the intermittent focus group will submit two proposals to the ArbitrumDAO:
4. The creation & nomination of members to form part of a procurement committee (referred to as 'PC') that will administer & facilitate the checks & balances as envisaged in the procurement process; and
5. The submission of the final procurement framework for ratification by the ArbitrumDAO through a governance vote.
6. Following the conclusion of the above mentioned matters, the appointed members of the PC will signal the beginning of the procurement process in line with the ratified procurement framework and administered by the appointed PC.

[Public Consultation Procurement Framework]

1. 'Needs' Assessment

Define and document the security needs of the Arbitrum Ecosystem:

- What type of security services do projects within the Arbitrum Ecosystem need?
- Will different services necessitate different procurement processes?
- Defining Eligibility Criteria

- Technical Expertise: Providers must demonstrate expertise in blockchain security, including prior experience with smart contracts, the Ethereum network, and Layer 2 solutions like Arbitrum.
- Reputation: A track record of successful security audits, with references and case studies.
- Certifications: Relevant industry certifications (e.g., CISA, CISSP, or equivalent).
- Compliance: Adherence to international standards for cybersecurity (e.g., ISO/IEC 27001).
- Tools and Techniques: Tools for detecting vulnerabilities, including static and dynamic analysis, and formal verification methods.
- Financial Stability: Proof of financial stability to ensure the longevity and reliability of the service provider.
- Innovation: Evidence of ongoing research and development in the field of blockchain security.
- Insurance: Adequate insurance cover for errors and omissions.
- Publication of the Request for Proposal (RFP)
- Scope of Work: Following the conclusion of the 'Needs Assessment' in [1], the PC will publish a request for submissions. This will be done via the ArbitrumDAO Forums wherein a detailed description of services required, including security audit scope, frequency, and expected deliverables will be provided by the PC.
- Submission Guidelines: Clear instructions on how to apply, including formats and submission channels.
- Evaluation Criteria: Metrics on how proposals will be assessed.
- Timeline: Submission deadlines and timeline for the evaluation process.
- Proposal Submission
- Documentation: Proposers must submit comprehensive documentation, including company profiles, client testimonials, and detailed descriptions of methodologies.
- Demonstration: Providers may be asked to demonstrate their capabilities via a test audit or presentation.
- The goal is to establish fair submission periods & submission criteria.
- Ideally, submissions should be effected on a dedicated section of the ArbitrumDAO Forums. This way, the PC can already get a sense of community feedback prior to putting the security service provider through the procurement process.
- Evaluation of Proposals
- Initial Screening: Verification of compliance with the minimum eligibility criteria.
- Technical Evaluation: In-depth review of technical capabilities, methodologies, and tools.
- Commercial Evaluation: Assessment of cost-effectiveness and value for money.
- References Check: Verification of the provider's references and past performance.
- Interviews: The PC may conduct interviews with the top candidates.
- Emphasis should be placed on documenting each step of the procurement process and communicating select steps in a consolidated manner to the community for review & input.
- In this regard, the PC can set up a dedicated notion page wherein the aforementioned details can be inputted, and then linked from the Forum updates posted by the PC.
- Whitelisting, Onboarding & Contracting
- Selection: The PC will select the most suitable providers to be whitelisted for service-subsidies based on them validly passing the procurement process.
- The PC will facilitate Know-Your-Business processes so as to make sure that all prospectively whitelisted service providers pass standard KYB checks.
- Contract Negotiation: The PC will facilitate & administer the process for the finalization of the contractual provisions regulating the engagement between the service provider chosen by the projects & the project itself. Most importantly, the PC has to ensure that the pricing 'advertised' by the service provider for the service requested is consistent with the agreement.

- Approval: Final agreements will be reviewed and approved by the PC before signing.
- Performance Monitoring and Review
- Regular Audits: Random checks by the PC during the audit process so as to ensure compliance with SLAs.
- Feedback Loop: A system for feedback from the projects utilizing the subsidised services. This will be pivotal in ensuring that the PC maintains a certain level of quality assurance so as to consistently assess whether any factors that led to the service provider passing the procurement process have changed.
- Renewal and Exit Procedures
- Renewal Criteria: Should the PC establish a quarterly/longer time period review process to reassess whitelisted service providers?
- Exit Strategy: Process for orderly termination of the service provider from the whitelist? (Example: if a service provider's performance is unsatisfactory or if they no longer meet the eligibility criteria)
- Documentation and Record Keeping
- Audit Trail: All stages of the procurement process will be documented and records maintained for accountability and transparency.
- Public Disclosure
- Transparency: Key details of the procurement process and the list of whitelisted providers will be made publicly available, respecting confidentiality agreements.
- This procurement process is designed to ensure that only the most qualified and reliable security service providers are selected, thereby safeguarding the integrity and security of the projects within the Arbitrum Ecosystem.

We look forward to your participation in the public consultation process & will be active to answer any questions or queries you may have in relation thereto. To reiterate, this is nowhere near the final procurement framework that will be provided for community ratification, but rather a Draft [1] base-level framework so as to solicit community input.

We look forward to receiving your submissions!

Feel free to reach out to me on Telegram@immutablelawyer should you have any questions, queries, or issues with the Google Form!

Kind regards,

Immutablelawyer

Axis Advisory