Authors

: Lido Audits Committee

Date

: 02/12/2024

Summary

The Lido Audits Committee proposes the creation of Guild for Review and Assessment of Protocols and Applications (GRAPPA), a dedicated security guild serving the Lido DAO. GRAPPA aims to enhance the review process for protocol development, incoming proposals related to network expansions (e.g., Base, zkSync Era, Linea, Mantle, Scroll, BNB, Mode, Zircuit, Starknet, Metis), and collaborations through the Lido Alliance (e.g.Mellow, Bolt).

GRAPPA is envisioned as an annually pledged role (contingent on proven success) assigned to a reputable third-party auditing provider with deep expertise in DeFi and smart contract auditing and familiarity with the Lido on Ethereum protocol. The initiative aims to start with a six-month pilot period from January 1st to June 30th, 2025.

Pilot with MixBytes: The Lido Audits Committee suggests thatMixBytes be the pilot party for GRAPPA. MixBytes specializes in smart contract auditing, security research, and technical consulting, and has been working with the Lido DAO since 2021. Their recent involvements include audits for Staking Router 2.0, CSM, Negative Rebase Protection [1, 2, 3], and Lido Multichain deployment verifications [1, 2, 3, 4, 5, 6]. MixBytes is extensively familiar with the Lido core protocol and has a proven track record from previous audits and reviews.

Key Points:

- Not a Formal Committee: GRAPPA operates as a workgroup without the authority to approve decisions or cast votes; it is not an official Lido DAO committee. Therefore, its creation does not require a governance vote.
- Guided by Lido Contributors: Lido Audits Committee will guide GRAPPA's activities and may propose changing the parties involved on behalf of GRAPPA based on performance, process and reports quality and DAO needs.

If you would like to suggest another option or disagree with the proposed one, share your vision in the comments section within the next 7 days.

Background and Motivation for GRAPPA:

As Lido continues to expand its ecosystem through new network integrations and collaborations, ensuring the security and integrity of the protocol is paramount.

The complexity of DeFi and smart contracts introduces significant risks that require expert assessment.

The issue to be addressed: The Lido contributors currently maintain a rigorous security process for the core protocol and key partnerships; however, it may lack sufficient transparency and scalability to meet the DAO's needs, especially given the increasing number of incoming proposals and recent launches (e.g., new staking modules, Lido Multichain, and Lido Alliance intents).

With the establishment of GRAPPA, the Lido DAO will be able to achieve the following improvements:

- Enhance security

: Provide thorough evaluations to mitigate potential vulnerabilities before they impact stETH token holders and the core protocol.

- Leverage proven expertise

: Utilize MixBytes' extensive experience and familiarity with the Lido on Ethereum protocol to ensure high-quality assessments.

- Maintain decision-making ground

: Maintain stakeholders' confidence by ensuring that all expansions meet the highest security standards.

- Streamline reviews

: Create a standardized process for evaluating proposals, improving efficiency and consistency.

- Provide transparency

: Publish summary review reports once completed to keep the community informed and engaged. These are public posts on the research forum for any project marked as GRAPPA-reviewed.

Note:

1. Complementary Role

: GRAPPA does not replace third-party audits, especially for protocol upgrades. It fills the gap for collaborations and joint launches with other networks and protocols, streamlining deployment verifications and quality checks.

1. Workgroup Approach

: GRAPPA operates as a workgroup guided by the Lido Audits Committee and does not bypass established governance processes.

Scope:

The GRAPPA within the Continuous Security Support Services for Lido DAO is responsible for the following areas:

- Manual Security Review

: This involves reviewing protocol (Lido on Ethereum) changes before they are deployed to the mainnet. Manual reviews allow for a deeper investigation of potential vulnerabilities that automated tools may not catch, providing a higher level of protection.

- Verification of Deployments for Lido Multichain

: This involves checking the correctness of deployments according to the internal checklist. This reduces the risk of errors and vulnerabilities when expanding the protocol across various blockchains.

- Consultations and Research on New Developments

: This involves consultations on the security of new features and developments to integrate safe solutions from the outset.

- Code review and adaptation of security best practices to new integrations

: All initiatives developing new protocols and applications under the Lido Alliance will be carefully guided to ensure the security and robustness of the final products.

- Enhancing security standards

: This will allow the Lido DAO to adapt faster to new initiatives and attract more security researchers and providers to boost protocol expansion.

- Research and education materials

: publish research and explanatory documents relevant to the Lido protocol integrations and features (“How it works”).

Reasons to choose MixBytes for the pilot

MixBytes is a blockchain company founded in 2017. Over the years, MixBytes has worked with some of the most prominent projects in the DeFi space (e.g., Aave, Curve, 1inch, Instadapp, Aragon, Yearn Finance). The complete list of security audits can be found in the public GitHub repo.

MixBytes has contributed to Lido DAO security since early 2021, providing security audits and technical support. MixBytes mainly helps to identify and resolve potential security issues, contributing to the overall resilience. This collaboration has ensured the protocol remains reliable as it grows across multiple blockchains (e.g., Ethereum, Base, OP Mainnet, Scroll, Linea, BNB).

MixBytes participated in the development of Lido on Polkadot\Kusama[link]. The team’s deep knowledge of Substrate allowed them to optimize Lido on Polkadot\Kusama architecture, ensuring scalability and security.

In 2023-2024, MixBytes contributed to developing and implementing a new framework for verifying Lido Multichain deployments. This enabled Lido DAO to launch more securely on new L2 networks, further boosting the adoption of stETH.

MixBytes proposes the DAO implement a GRAPPA role to ensure a continuous approach and set the reference pace. The GRAPPA will actively monitor and manage the security aspects of the Lido and developments at every stage. It will involve a full-time, dedicated team of security auditors who know the protocol codebase and its integrations.

This way, Lido DAO can confidently scale its operations and launch new products faster and more efficiently. This approach will protect Lido’s current operations and support its long-term expansion and broader adoption of stETH in the DeFi

ecosystem.

Terms of Work

Within the proposed format of continuous security support, MixBytes will allocate a team of three full-time senior auditors, a technical project manager (PM), and a Chief Technology Officer (CTO), who will perform quality assurance (QA) functions.

The format of continuous security support does not require 100% team allocation or on-demand auditing on the day of the request. The parties will agree on work plans at the beginning of each month.

In any case, Lido's security review requests and other demands will always be the highest priority when booking the closest possible time slot.

Success Criteria

The end-of-term review will evaluate the work against the criteria mentioned below and decide (using the standard proposal process) whether to continue the MixBytes' contract or implement changes for GRAPPA after the pilot period.

- Thorough assessments

: Proposals for joining the Alliance and expanding to new networks are evaluated for architectural soundness, trust models, audit completeness, and deployment accuracy.

- Timely Reviews

: The proposals mentioned are reviewed within 30 days to ensure prompt, informed decision-making for token holders. If necessary, extensions can be negotiated for up to an additional 15 days, with the total review period not exceeding 45 days.

- Transparency

: All reports are published on GitHub - lidofinance/audits, and summaries of everything reviewed are shared on the research forum.

Next Steps

1. Community Feedback

: This proposal is open for community feedback.

1. Establishment of GRAPPA

: If there are no significant objections, GRAPPA will be established as a workgroup starting in H1 2025. The Lido Audits Committee will engage MixBytes to execute services for GRAPPA during the six-month pilot period.

1. Pilot Period Review

: The Lido Audits Committee together with MixBytes will provide a summary of the pilot period, detailing the assessments made and participation in implemented initiatives, potentially suggesting future changes and improvements for GRAPPA.

By adopting GRAPPA, the Lido DAO can confidently scale its operations and launch new products faster and more efficiently. This approach will help to streamline current operations of protocol and support its long-term expansion and the wider adoption of stETH in the DeFi ecosystem.