The development and acceptance process of Lido-on-X protocol (Lido on Solana, Polygon, Kusama/Polkadot) involves a pre-release security assessment. These assessments are expensive and are needed not only for the team building Lido-on-X, but for the Lido DAO as a method of acceptance test (so we could say that indeed, that version of the protocol is safe to deploy, use, promote and incentivize).

It's never boiled down to the point of contention, but the teams are extremely cognizant of the upfront costs of assessments (before they even know if their solution will have a PMF), and are de-incentivized to go for the best quality, more expensive firms. We should not put development teams in a situation where they have a conflict of interests on getting the best security practices.

My proposal here is for Lido at large, acting through LEGO, to bear all the costs of final security assessments of the Lido-on-X protocols, limited to two assessments with reputable firms per upgrade. With LEGO council in charge of judging what is a reputable firm.

I also propose to retroactively fund the security assessments for Mixbytes(), Shard Labs, and Chorus One.

The costs of doing this are quite substantial (audits costs for a full protocol are anywhere between \$30k to \$200k, might be even more), but I gather them to be less than bug bounty costs, which are topped at \$2M per bug currently.