

We previously introduced the [new EigenLayer security model](#). This short post is to make clear that there is no global veto committee on EigenLayer

The original [security model](#) had the following structure: each operator can opt into a subset of AVSs, and the entire stake delegated to that operator could be slashed by any of those AVSs, which meant:

1. Less control over slashing risk

: An AVS sharing slashable stake could be inadvertently exposed to the risks of slashing by other AVSs. Additionally, the entirety of an operator's delegated stake is at risk of being slashed by any AVS it opted into.

1. No slashable stake assurances for AVSs

: AVSs had no assurance that they would have access to slashable stake when needed.

1. Needs a global slashing veto committee:

The system needed a global veto committee to buffer slashing events from becoming systemic.

1. Permissioned onboarding of AVSs

: Because of the need for a global veto committee, AVS onboarding needed to be permissioned otherwise the veto committee would be taking on uncalibrated risks.

The new EigenLayer security model has been specifically designed to address these shortcomings by offering greater flexibility and control:

1. Greater control over slashing risk

: With Unique Stake, the risk of slashing is isolated to the individual AVS, and operators can control how much of their stake any AVS can slash.

1. Guaranteed slashable stake

: Each AVS knows how much slashable stake they have by adding up the Unique Stake allocated to them across all its operators.

1. No need for a global veto committee

: Since slashing is localized to individual AVSs, there is no necessity for a global veto committee. Each AVS can specify its own mechanisms for slashing and governance.

1. Permissionless onboarding of AVSs

: AVS onboarding is permissionless and only requires operators to opt in.

There is no longer a need for a global veto committee on EigenLayer and thus it is not a part of the core protocol.