This document is to be considered the source of truth for the latest version of the Risk Rosette framework. Note that it might not account for every possible scenario and for this reason it gets frequently updated based on new circumstances.

A changelog can be found at the bottom of the document.

The Framework contains 5 dimensions which are reviewed independently (where possible), meaning that each one is reviewed as if the others were green. For a summary of the risks as a whole, see the Stages Framework.

Specification

State Validation

How is the validity of the system state checked?

Green

A fully functional proof system is deployed. Performing challenges in fraud proof systems is permissionless and delay attacks are reasonably bounded.

Yellow

The proof system should be safe under any circumstance but can be subject to delay attacks. If a fraud proof system is used with a whitelist, there should be at least 5 external actors that can submit challenges.

Red

The requirements to be Yellow are not met. This includes using non source available software, or in general if it is not possible to verify what it is being proven onchain.

Data Availability

Is the data needed to reconstruct the state available?

Green

DA is posted on Ethereum and the L2 derivation fully depends on such data. In this case the system is classified as a Rollup.

Yellow

Data is not posted on Ethereum, but on a DAC or an external DA layer. If a DAC is used, it must contain at least 5 external actors and the threshold should be set such that no more than 1/3 is required to be honest for safety, at the expense of liveness. DA fallback mechanisms can be implemented in the case of a DAC liveness failure (see Arbitrum Nova as an example). To calculate the amount of honest actors required for safety the following formula is used: #honest = size - threshold + 1

which is the number of members required not to meet the threshold.

In the case of an external DA layer, the attestations bridge must follow the correct attestations and there should be at least a 7d upgrade delay on it. These requirements are still debated and will be more precisely defined based on the WIP Data Availability Risk Framework.

Red

DA is not posted on Ethereum and the requirements for being Yellow are not met.

Exit Window

How much time do users have to exit the system in case of unwanted upgrades. This value takes into account upgrade delays minus the delays needed to exit. Having a non-zero exit window requires at least Sequencer failure and Proposer failure risks to be green.

Green

Users are provided with at least 30d to exit in case of unwanted upgrades, excluding in the case of onchain attributable bugs.

Yellow

Users are provided with at least 7d to exit in case of unwanted regular upgrades, but less than 30d.

Red

Less than a 7d exit window is provided to users for regular upgrades.

Warning

There is a Security Council that can perform instant emergency upgrades.

Proposer Failure

Green

Users can self propose state roots permissionlessly if centralized operators fail to do so, or freeze the chain to exit with the latest available state root (escape hatch). Note that the latter mechanism is only possible on app specific systems.

Yellow

TBD, currently not used.

Red

Proposing state roots is centralized.

Sequencer Failure

Green

Users can self sequence blocks permissionlessly if centralized operators fail to do so, or force request a transaction on L1. If the request is not satisfied within a certain time limit, the system gets frozen and users can exit with the latest available root. Note that the latter mechanism is only possible on app specific systems.

Yellow

Users can submit transactions to an L1 queue, but can't force them. The sequencer cannot selectively skip transactions but can stop processing the queue entirely. In other words, if the sequencer censors or is down, it is so for everyone.

Red

Users have no way to independently push transactions to L2 if censored by the permissioned operators.

Changelog

- Jun 6, 2024: Yellow state validation is stricter by disallowing proof systems that are not safe. Kroma is declassified from Yellow to Red since it can fail in certain edge cases (see audit, in particular KROMA-020

) (PR).

- Jun 5, 2024: Clarified red and yellow designations for the Exit window to refer to regular upgrades.
- Dec 21, 2023: The Upgradeability column is turned into the Exit window column, with new math that takes into account delays needed to exit. (PR)
- Jun 8, 2023: Validator Failure column is renamed to Proposer Failure, and updated designations to either "Self propose", "Use escape hatch" or "Cannot withdraw" (PR).
- Jun 5, 2023: Sequencer Failure designation updated to "Self sequence", "Enqueue via L1" or "No mechanism" (PR).