Fed Consideration Checklist

Technical

Smart Contract Code Review: Conduct a thorough code review of the smart contract code, including all smart contracts used by the project. Check for code quality, security vulnerabilities, and potential attack vectors.

Immutability: Ensure that the smart contract code is immutable, meaning that it cannot be changed or modified once deployed to the blockchain. Verify that no administrative privileges exist that could allow someone to alter the smart contract code.

Proxy Contract Review: Review any proxy contracts used by the project and check for potential security vulnerabilities. Ensure that proxy contracts are implemented in a secure and transparent way, and that they do not introduce additional risks or attack vectors.

EOA Management: Review the management of externally owned accounts (EOAs) used by the project. Ensure that EOAs are secured with strong passwords, two-factor authentication, or other secure authentication methods, and that access is granted only to authorized personnel.

Contract Interactions: Review the interactions between smart contracts used by the project to ensure that they are secure and properly implemented. Check for any potential vulnerabilities or attack vectors that could be exploited.

Upgradeability: Review the upgradeability mechanisms used by the project, such as proxy contracts or other mechanisms. Ensure that any upgradeability is implemented in a secure and transparent way, and that it does not introduce additional risks or attack vectors.

Audit Reports: Review any third-party audit reports or security assessments conducted on the smart contract code. Ensure that any identified vulnerabilities or issues have been addressed or mitigated.

Compliance: Review the project's compliance with relevant laws and regulations, such as data protection and financial regulations. Ensure that the smart contract code and EOAs are compliant with any relevant laws or regulations.

Documentation: Review the documentation for the smart contract code and EOAs. Ensure that it is complete, accurate, and up-to-date, and that it provides clear and concise instructions for how to interact with the smart contract code and EOAs.

Testing and Deployment: Review the testing and deployment processes used by the project to ensure that they are secure and reliable. Ensure that testing is thorough and covers all potential scenarios, and that deployment is done in a secure and transparent way.

Non-Technical

Project Overview: Review the project's whitepaper or documentation to understand the project's goals, architecture, and key features.

Team Background Check: Conduct a background check on the project's development team to ensure they have the necessary skills and experience to successfully execute the project.

Tokenomics and Economics: Review the project's tokenomics and economics, including the supply and distribution of tokens, the use cases for the token, and any potential economic risks.

Community Engagement: Review the project's community engagement, including the size and activity level of the community, and any potential risks associated with community sentiment or behavior.

Legal and Regulatory Compliance: Review the project's legal and regulatory compliance, including any potential legal or regulatory risks associated with the project.

Competitive Landscape: Review the project's competitive landscape, including any potential competitors or substitutes, and the project's competitive advantages and disadvantages.

Market Analysis: Conduct a market analysis to understand the potential demand for the project, the size of the target market, and any potential market risks.

Partnerships and Integrations: Review any existing or potential partnerships and integrations that the project has or plans to have, and assess the potential impact on the project's success.

Roadmap and Development Plan: Review the project's roadmap and development plan, and assess the feasibility and timeline of the project.