

Chainlink CCIP Service Responsibility

The Chainlink Cross-Chain Interoperability Protocol (CCIP) is a secure, reliable, and easy-to-use interoperability protocol for building cross-chain applications and services. The use of CCIP involves application developers, blockchain development teams, and Chainlink node operators, among others. These participants share responsibility for ensuring that operation and performance match expectations. Please note that CCIP support of a particular blockchain, application, or token does not constitute endorsement of such blockchain, application, or token.

Application Developer Responsibilities

Application developers are responsible for the correctness, security, and reliability of their application. This includes:

- **Code and application audits:** Developers are responsible for auditing their code and applications before deploying to production. Developers must determine the quality of any audits and ensure that they meet the requirements for their application.
- **CCIP upgrades and best practices:** Developers are responsible for following CCIP documentation regarding implementing CCIP upgrades and best practices for integrating CCIP in their applications.
- **Code dependencies and imports:** Developers are responsible for ensuring the quality, reliability, and security of any dependencies or imported packages that they use with Chainlink CCIP, as well as reviewing and auditing these dependencies and packages.
- **Code quality and testing:** Developers are responsible for ensuring that their application code, onchain and offchain, meets the quality expectations and has undergone rigorous testing.
- **Application monitoring and alerting:** Developers must monitor their applications, inform their users of any abnormal activity, and take appropriate action to restore normal operations.
- **Blockchain risk assessment:** Developers are responsible for the risk assessment of any blockchain network where they choose to deploy their application on or decide to interoperate with, when using Chainlink CCIP.
- **Token risk assessment:** Developers are responsible for the risk assessment of any tokens they choose to support or list in their application and expose to their users.
- **Risk communication:** Developers must clearly articulate and communicate identified risks to their users.
- **Manual execution:** Developers must monitor their CCIP transactions and take action when transactions require manual execution. For example, informing their users and directing them to the appropriate page on the [CCIP Explorer](#).

Blockchain Development Team Responsibilities

Blockchain development teams are responsible for the correctness, security, and reliability of their blockchain software. This includes:

- **Block finality:** Blockchain development teams must ensure that blocks with [a commitment level](#) of finality are actually final. The properties of the finality mechanism, including underlying assumptions and conditions under which finality violations could occur, must be clearly documented and communicated to application developers in the blockchain ecosystem.
- **Governance model:** Blockchain development teams are responsible for setting up a clear and effective governance model and communicating its participants and processes clearly to its stakeholders and application developers.
- **Fixes and upgrades:** Blockchain development teams must communicate availability of fixes immediately and announce planned upgrades as much in advance as possible so blockchain validators and application developers can prepare themselves accordingly.
- **Incident management:** Blockchain development teams are responsible for clearly articulating and communicating any security, reliability and availability incidents to their community. This includes root cause analysis, post-mortem details and a clear plan of action to recover and prevent from happening in the future.
- **Blockchain liveness:** Blockchain development teams must take appropriate action to ensure their blockchain maintains a high degree of liveness and aligns with set expectations towards their community members and applications developers.

Chainlink Node Operator Responsibilities

High-quality Chainlink node operators participate in the decentralized oracle networks (DONs) that power CCIP and the Risk Management Network using a configuration specified in the Chainlink software. As participants in these deployments, Node Operators are responsible for the following components of Chainlink CCIP and the Risk Management Network:

- **Node operations:** Chainlink node operators must ensure the proper configuration, maintenance, and monitoring of their nodes participating in the Chainlink CCIP and Risk Management Network DONs.
- **Transaction execution:** Chainlink node operators must ensure that transactions execute onchain in a timely manner and that they apply gas bumping when necessary.
- **Blockchain client:** Chainlink node operators are responsible for selecting and properly employing blockchain clients, including latest fixes and upgrades, to connect to supported blockchain networks.
- **Consensus participation:** Chainlink node operators must maintain continuous uptime and active participation in OCR

consensus.

- Infrastructure security:Chainlink node operators must follow infrastructure security best practices. These include access control, configuration management, key management, software version & patch management, and (where applicable) physical security of the underlying hardware.
- Software version:Chainlink node operators are responsible for ensuring that Chainlink node deployments are running the latest software versions.
- Responsiveness:Chainlink node operators must respond to important communication from Chainlink Labs or from other node operators in a timely manner.