Executive Summary

This Executive Summary provides a high-level assessment of the quality, risks, and overall reliability of the **Sign-up Feature** evaluated during the QA process. The evaluation was performed using a combination of manual and automated testing strategies, with a total of **39 test cases** executed across functional, non-functional, usability, and security areas.

Overview of Findings

- **Total Test Cases Designed:** 39
- **Execution Summary:** 18 Passed, 3 Failed, 18 Not Executed
- **Pass Rate:** 46%
- **Fail Rate:** 8%
- **Not Executed:** 46%
- **Coverage:** Functional validation, input field policies, email & OAuth integration, password security, usability, cross-browser checks, accessibility, and performance.
- **Automation:** Selenium was used to automate the majority of functional and cross-browser tests, supplemented by JMeter for performance validation.

Quality Assessment

- The overall quality of the sign-up process is rated as **Good**, with smooth handling of the majority of critical user flows (OAuth logins, input validation, password policies).
- Critical security checks, such as password strength enforcement and OAuth authentication, functioned as expected.
- Usability features like clear error messages and password masking were validated successfully.
- A number of OTP-based scenarios could not be executed (**Not Executed**) due to the absence of OTP delivery, limiting the complete verification of email-based sign-ups.
- Failures were observed in **session timeout handling (TC034)**, **harmful content refusal (TC038)**, and **factual correctness validation (TC039)**, highlighting areas requiring urgent fixes.

Risk Assessment and Recommendations

- **High Risks:** Failures in harmful content refusal (TC038) and factual correctness validation (TC039) could lead to misinformation and policy non-compliance.
- **Medium Risks:** Session timeout handling failure (TC034) may expose user accounts to security concerns.
- **Execution Gaps:** OTP-related test cases remain unverified, representing a potential risk if email verification does not function correctly.
- **Recommendation:** Prioritize fixing failed cases and completing OTP-related test executions before production release; perform regression testing post-fix.

- Conduct stress and load testing to ensure consistent performance under high user volume.

Next Steps for QA Process

- Address and re-test the failed high-priority scenarios (TC034, TC038, TC039).
- Complete execution of OTP-dependent test cases once the email verification service is operational.
- Conduct additional exploratory testing for edge cases, particularly under slow or unstable network conditions.
- Enhance automation coverage by integrating Selenium test suites with CI/CD pipelines.
- Perform periodic regression and compliance checks to ensure long-term stability and adherence to evolving security standards.

This summary reflects the consolidated QA findings of the Sign-up Feature, clearly identifying executed, failed, and unexecuted test cases to ensure reliable deployment with actionable improvements.