The addition or use of an online repository, such as GitHub, can increase security in several ways:

1. Access control and Code Sharing/Distribution: With an online repository, access to the source code can be controlled and limited to authorized individuals or teams, reducing the risk of unauthorized access or theft of intellectual property.
2. Network Security: Online repositories offer secure communication channels for developers to share and collaborate on code without risking the exposure of sensitive data.
3. Accounting Issues: With an online repository, it is possible to track who made changes to the code and when, which can be important for regulatory compliance and auditing purposes. Additionally, online repositories usually have features for tracking issues and bugs, enabling developers to prioritize and address security vulnerabilities far easier.

Security testing should be implemented to ensure that the code is secure and free of vulnerabilities. This can include various types of testing such as penetration testing, vulnerability scanning, and static code analysis.