a. Passwords not stored in plain text
b. Access control with Roles & Responsibilities
c. The requirement, enhancement or defect has been addressed as per the expected behavior.
d. The code is readable, maintainable and follows agreed naming and coding conventions.
e. Unnecessary duplication, hardcoding and magic values have been avoided.
f. Existing tests/build validations are passing.
g. Security impact has been considered, especially for authentication, authorization, personal data, file upload/download, payment and sensitive operations.
h. Error handling is appropriate, with user-friendly messages and proper technical logging.
i. No sensitive information such as passwords, tokens, API keys, OTPs or personal data is exposed in code, logs, UI messages or API responses.
j. API changes, database changes, configuration changes or integration impacts are clearly documented where applicable.
k. Configuration values are externalized and no environment-specific values are hardcoded.
l. Code review comments have been addressed and resolved.
m. Deployment steps, database scripts, rollback notes or post-deployment validation steps are provided where required.
n. Documentation is updated if the change affects behavior, setup, API contract, database structure, configuration, deployment or operational support.