OP_Enterprise Code Quality Severity Matrix

Enterprise Code Quality Severity Matrix

qodo

QUALITY DOMAIN	LEVEL	DEFINITION	ENTERPRISE EXAMPLES
Functional	CRITICAL	Breaks core business logic, data integrity violations	Payment calculations off by 0.01%, user permissions bypassed, audit trail corruption
Functional	HIGH	Edge cases fail, integration contracts broken	API rate limiting ignored, null pointer exceptions on enterprise data, third-party service timeouts unhandled
Functional	MEDIUM	Performance degradation, minor behavioral gaps	Database queries inefficient at scale, caching strategies missing, error messages unclear
Functional	LOW	UX friction, non-essential features incomplete	Loading states missing, responsive design gaps, accessibility improvements
Non-Functional	CRITICAL	Security vulnerabilities, compliance violations, architectural violations	SQL injection in user inputs, PII exposure in logs, GDPR data retention violated, secrets hardcoded
Non-Functional	HIGH	Scalability bottlenecks, enterprise constraint violations	Memory leaks under load, single points of failure, dependency vulnerabilities, enterprise proxy incompatibility
Non-Functional	MEDIUM	Maintainability erosion, technical debt accumulation	Code duplication across modules, inconsistent patterns, missing observability, configuration scattered
Non-Functional	LOW	Style inconsistencies, minor structural improvements	Naming conventions, file organization, comment quality, dependency organization
Process	CRITICAL	Deployment blockers, complete test gaps	Zero test coverage, CI/CD pipeline breaks, deployment scripts fail, rollback impossible
Process	HIGH	Integration test gaps, documentation missing	Unit tests pass but integration fails, API contracts undocumented, runbook missing
Process	MEDIUM	Coverage insufficient, review process friction	60% test coverage, complex PR review cycles, manual deployment steps
Process	LOW	Workflow optimizations, tooling improvements	Linting warnings, outdated dependencies, IDE configuration, commit message format