

Introduction to Governance for Low Code

Mastering Governance in Low Code Development

DEFINITION

Governance for Low Code refers to the policies and practices that ensure effective management and control of low code applications. It helps organizations maintain quality, security, and compliance while enabling rapid development.

KEY CONCEPTS

Policy Framework

A set of guidelines that dictate how low code applications should be developed and maintained.

Compliance Standards

Regulations and requirements that low code applications must meet to ensure legal and operational integrity.

Risk Management

The process of identifying, assessing, and mitigating risks associated with low code application development.

User Access Control

Managing who can create, modify, or delete low code applications to prevent unauthorized changes.

Quality Assurance

Ensuring that low code applications meet defined standards for functionality, performance, and security.

EXAMPLES

- Implementing a policy for app approval before deployment.
- Regular audits to ensure compliance with data protection laws.
- Setting user roles to limit access to sensitive application features.

MEMORY TIPS

- ★ Remember 'P-C-R-Q' for Policy, Compliance, Risk, Quality.
- ★ Think of governance as the 'traffic lights' for low code development.
- ★ Use 'A-C-R' to recall Access, Compliance, and Risk management.

COMMON MISTAKES

- ✗ Neglecting to document governance policies.
- ✗ Overlooking user training on governance practices.
- ✗ Failing to regularly review and update governance frameworks.

QUICK RECAP

Governance for Low Code ensures that applications are developed responsibly and securely. Key elements include policies, compliance, risk management, and user access control. Remember to keep governance frameworks updated and well-documented.