ONE PAGE SUMMARY

IT & Software › Low Code / No Code › Governance for Low Code

Introduction to Governance for Low Code

Mastering Governance in Low Code Environments

DEFINITION

> Governance for low code refers to the frameworks and policies 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 managed.

Risk Management

Identifying and mitigating potential risks associated with low code development to protect data and resources.

Compliance Standards

Ensuring that low code applications meet legal and regulatory requirements relevant to the organization.

User Access Control

Managing who can create, modify, or access low code applications to prevent unauthorized use.

Quality Assurance

Processes to ensure that low code applications meet performance and functionality standards before deployment.

EXAMPLES

→ Implementing a policy framework for low code development teams.

→ Conducting regular audits to ensure compliance with data protection regulations.

→ Establishing user roles to control access to sensitive application features.

MEMORY TIPS

★ Remember 'PRUQ' for Policy, Risk, User access, Quality.

★ Think of governance as a safety net for low code applications.

★ Visualize a traffic light: green for compliant, yellow for caution, red for stop.

COMMON MISTAKES

✗ Neglecting to document governance policies.

✗ Overlooking user access controls leading to security risks.

✗ Failing to regularly update compliance standards.

QUICK RECAP

Governance for low code is essential for managing applications effectively and securely. Key elements include policy frameworks, risk management, and compliance standards. Remember to focus on user access and quality assurance to ensure successful low code development.