Security & Compliance in DevOps

# 1. Risk: Hardcoded Secrets in Code Repositories

Problem:  
Developers may accidentally commit sensitive credentials or API keys into version control systems like GitHub, exposing them publicly or internally.

Mitigation Strategies:  
• Use GitHub Secrets or Azure Key Vault to securely store and access credentials.  
• Integrate secret scanning tools like git-secrets, TruffleHog, or GitHub Advanced Security.  
• Implement code reviews and pre-commit hooks to detect secrets.

Compliance Mapping:  
• ISO 27001 A.9.4.1 – Information access control.  
• SOC 2 – Enforces data protection and access management policies.

# 2. Risk: Lack of Access Control & Role Separation

Problem:  
Excessive permissions or shared accounts in CI/CD tools and cloud platforms can lead to privilege escalation or insider threats.

Mitigation Strategies:  
• Apply the Principle of Least Privilege using Role-Based Access Control (RBAC).  
• Use Identity and Access Management (IAM) policies to restrict access.  
• Enable audit logs to monitor access attempts.

Compliance Mapping:  
• ISO 27001 A.9.2.3 – Management of privileged access rights.  
• GDPR Article 32 – Ensures data is accessed only by authorized personnel.

# 3. Risk: Use of Vulnerable or Outdated Dependencies

Problem:  
CI/CD pipelines may use packages with known security vulnerabilities that go undetected.

Mitigation Strategies:  
• Integrate automated dependency scanning tools such as OWASP Dependency-Check, Trivy, or Snyk.  
• Regularly update and patch dependencies.  
• Fail builds when critical vulnerabilities are found.

Compliance Mapping:  
• ISO 27001 A.12.6.1 – Control against malware.  
• SOC 2 – Maintains a secure software supply chain.

# Cloud Security Best Practices

• Encrypt data at rest and in transit using HTTPS and Azure Disk Encryption.  
• Restrict traffic using firewalls, NSGs (Network Security Groups), and private endpoints.  
• Enable MFA (Multi-Factor Authentication) for all accounts.  
• Enable logging and monitor using Azure Monitor or ELK Stack.  
• Schedule automated security audits and compliance scans.  
• Regularly review and rotate secrets, keys, and access tokens.