Secure Design Principles Checklist

Ten core principles for architecture reviews

Core Principles Verification

- ■ Least Privilege — Each component has minimum permissions needed?
- ■ Complete Mediation — Every access request is checked?
- ■ Fail-Safe Defaults — System denies access by default?
- ■ Economy of Mechanism — Security mechanisms are simple and verifiable?
- ■ Separation of Duties — Critical actions require multiple approvals?
- ■ Open Design — Security doesn't depend on secrecy of implementation?
- ■ Least Common Mechanism — Shared resources minimized between users?
- ■ Psychological Acceptability — Security controls are usable?
- ■ Defense in Depth — Multiple layers of security controls present?
- ■ Minimize Attack Surface — Unnecessary features/endpoints removed?

AI-Specific Design Considerations

- ■ AI-generated architecture validated against security requirements?
- ■ Trust boundaries explicitly defined around AI components?
- ■ Fallback mechanisms exist if AI services are unavailable?
- ■ Data classification enforced for AI training/inference data?