Document Type: Control Requirement
Control ID: ISO27001-A5.15
Framework: ISO/IEC 27001:2022
Clause: Annex A.5.15
Domain: Access Control
Sub-Domain: Identity & Access Management
Risk Level: High
Control Statement:
Access to information and systems SHALL be restricted based on business requirements and role responsibilities.
Evidence Expected:
- Defined access control policy
- Role-based access definitions
- Access provisioning and de-provisioning process
- Periodic access reviews
Common Gaps:
- No formal access review
- Privileged access not controlled
- Access removal delays
Risk Impact:
Unauthorised access, data leakage, fraud