Document Type: Control Requirement
Control ID: ISO27001-A5.25
Framework: ISO/IEC 27001:2022
Clause: Annex A.5.25
Domain: Incident Management
Sub-Domain: Security Incident Response
Risk Level: High
Control Statement:
Information security incidents SHALL be assessed, prioritised, responded to, and documented in a timely manner.
Evidence Expected:
- Incident response procedures
- Incident classification criteria
- Defined escalation timelines
- Post-incident review records
Common Gaps:
- No defined response timeline
- Incident handling informal
- No root cause analysis
Risk Impact:
Delayed response, increased breach impact, regulatory penalties