REQUIREMENTS	SCOPE OF APPLICABILITY	Mechanisms
Establish a well-defined organisational structure from a security perspective	Organisation	Organisational diagram Key points: • Conflicts of interest are avoided • Key tasks are subject to 'two man-rule' approval • Separate role-holders and reporting lines for: (i) IT manager and System accreditors, and (ii) IT manager and system/ network testers
Establish a framework for addressing security matters on an on-going-basis		Key issues: • Resourcing • Identification of applicable security standards, legislation and regulations, Codes of connection • Management commitment in-place • Documentation templates • Security strategy and plan • Compliance checks (on-going) and 'independent'
Ensure that records are maintained to demonstrate compliance and 'good practice'		
Ensure that staff remain aware of their responsibilities and comply		• Security education and awareness plan
Provide returns / compliance statements to external parties as required demonstrating compliance		• Codes of connection • ISO 27001 (Security standard), ISO 20000 (IT service management), BS25999 (Business continuity)
Be pro-active in detecting security problems		• Security review, test, inspection regime, stakeholder interviews • Technical measures, e.g. Intrusion detection
Manage incidents in accordance with well-defined procedure		• Incident management procedure, including computer forensics capability