REQUIREMENTS	SCOPE OF APPLICABILITY	MECHANISMS
Authentication	Controlling access to: • Corporate network from within the Office • Corporate network via the Internet and mobile networks • Business application(s) • WiFi	• Two-factor, e.g. cards, tokens, soft-tokens • User id / passwords • Certificates • Biometrics, e.g. IRIS, fingerprint, facial recognition
Network access control	• Feeds into corporate networks from GPRS / 3G providers • Internet	• Firewalls, e.g. EAL 4 ‘enterprise’ firewall, ‘packet filtering’ routers, personal firewalls • Intrusion detection / prevention systems (IDS / IPS)
Protect data in transmission	• Network traffic	• Virtual private network (VPN), e.g. IPSEC, SSH, or SSL / TLS
Protection against malicious / Trojan code	• Servers • Workstations and laptops (Windows and Linux) • Smart phones (Windows and Android)	• Anti-virus software • Content checkers
End-device protection	• Smart phone • Laptop (mobile environment)	• Hard disk encryption • USB control software
‘Lockdown’ system, including administration rights and utilities	• Servers	• Integrity-style products, e.g. Solid Core • Role-based access controls
Monitoring and audit	• Intrusion detection system, Firewalls, end-user devices, servers, communication devices.	• Events-raised by end-user devices, servers, network infrastructure and collated by central application, e.g. system, security and application logs.