



Appendix F2-5

Security Components (Generic)

Component Type	Common Features / Mechanisms
Anti-piracy tools	Preventing the illegal copying and distribution of software.
Anti-theft devices	Preventing the theft of equipment items such as PCs.
Anti-virus scanners	Scanning for known viruses and other malicious software, and repairing any damaged files (although the repair may not be perfect and therefore may not be the correct way to proceed).
Biometric devices	Providing personal authentication based on measurement of a bodily feature – such as fingerprint, retina pattern, facial geometry, etc.
Boot-protection software	Preventing the booting of a PC from a diskette to get unauthorised access to the hard drive.
Business continuity planning and disaster recovery planning tools	Supporting the collection and management of planning information.
CCTV monitoring	Physical site surveillance.
Computer forensics tools	Recovering deleted data and piecing together a history of activity.
Content filtering for e-mail	Detecting and filtering out unacceptable content.
Content filtering for web browsing	Detecting and filtering out unacceptable content.
Cryptographic hardware	Providing high-performance cryptographic processing, high-security key storage, secure time source, random number generation for key management, tamper resistant enclosures.
Cryptographic software tool-kits	Run-time libraries for data encryption, authentication, digital signatures, certificate processing, etc.
Data back-up management systems	Copying and storage management, and restoration to a previous business position.
Directory products	Providing directory services.
Document safes	Protecting documents from theft and/or fire damage.
E-mail encryption and authentication products	Providing privacy and authentication for e-mail messages.
Enterprise security management tools	Managing a wide range of security services across multiple platforms.
Fault-tolerant computing	Resilient computing platforms that will survive failure of

Component Type	Common Features / Mechanisms
solutions	components.
File encryption products	Encrypting files either for transmission or for storage.
Firewalls	Filtering network traffic according to source, destination and content to allow only authorised traffic.
Intrusion detection systems	Looking for unauthorised activity from intruders both in the network and on host platforms.
LAN security products	Providing security functionality in local area networks.
Operating platforms	Logical access control and integrity protection.
Personal authentication tokens and devices	Multi-factor authentication of users.
Physical security alarms	Intruder alarms and fire alarms in buildings and computer suites.
PKI software	Digital certificate management and the cryptographic services that it supports.
Risk assessment tools	Software packages to capture and process risk data.
Role-based access control solutions	Centralised role-based access control management and authentication of users.
Secure middleware products	Providing secure node-to-node communications and an API for applications to call security services.
Security auditing tools	Automated inspection tools to check the configuration of an operating platform or application.
Security shells	Add-on software products to provide additional levels of access control to standard operating systems.
Single-sign-on authentication service solutions	Centralised authentication servers integrating distributed applications and providing an authentication front-end with single-sign-on.
Smart cards	A self-contained computer on a plastic card with its own on-board authentication and access control functions.
Software licence management tools	Managing the distribution of licensed software to ensure compliance with the licence.
Uninterruptible power supplies	Protecting against electrical power failure.
VPN products	Virtual private networks built using IPSec or SSL.

Component Type	Common Features / Mechanisms
Vulnerability scanning tools	Looking for ‘holes’ in the network or host configurations.
Wireless security products	Preventing eavesdropping and authenticating nodes.