BS7799 Annex A		Control		Exclusion	Justification
A3	**SECURITY POLICY**				
A3.1	**Information security policy**				
A3.1.1	Information Security Policy Document		QM1.2 Information Security Policy		
A3.1.2	Review & Evaluation				
A4	**ORGANISATIONAL SECURITY**				
A4.1	**Information security infrastructure**				
A4.1.1	Management information security forum				
A4.1.2	Information security coordination				
A4.1.3	Allocation of information security responsibilities				
A4.1.4	Authorisation process for information processing facilities				
A4.1.5	Specialist information security advice				
A4.1.6	Cooperation between organisations				
A4.1.7	Independent review of information security				
A4.2	**Security of third-party access**				
A4.2.1	Identification of risks from third party access				
A4.2.2	Security requirements in third-party contracts				
A4.3	**Outsourcing**				
A4.3.1	Security requirements in outsourcing contracts				
A5	**ASSET CLASSIFICATION & CONTROL**				
A5.1	**Accountability for assets**				
A5.1.1	Inventory of assets		Risk Assessment Report		
A5.2	**Information Classification**				
A5.2.1	Classification guidelines				
A5.2.2	Information labelling & handling				
A6	**PERSONNEL SECURITY**				
A6.1	**Security in job definition & resourcing**				
A6.1.1	Including security in job responsibilities				
A6.1.2	Personnel screening & policy				
A6.1.3	Confidentiality agreements				
A6.1.4	Terms & conditions of employment				
A6.2	**User training**				
A6.2.1	Information security education & training				
A6.3	**Responding to security incidents & malfunctions**				
A6.3.1	Reporting security incidents				
A6.3.2	Reporting security weaknesses				
A6.3.3	Reporting software malfunctions				
A6.3.4	Learning from incidents				
A6.3.5	Disciplinary process				
A7	**PHYSICAL & ENVIRONMENTAL SECURITY**				
A7.1	**Secure Areas**				
A7.1.1	Physical security perimeter				
A7.1.2	Physical entry controls				
A7.1.3	Securing offices, rooms & facilities				
A7.1.4	Working in secure areas				
A7.1.5	Isolated delivery & loading areas				
A7.2	**Equipment security**				
A7.2.1	Equipment siting & protection				
A7.2.2	Power supplies				
A7.2.3	Cabling security				
A7.2.4	Equipment maintenance				
A7.2.5	Security of equipment off-premises				
A7.2.6	Secure disposal or re-use of equipment				
A7.3	**General Controls**				
A7.3.1	Clear desk & clear screen policy				
A7.3.2	Removal of property				
A8	**COMMUNICATIONS & OPERATIONS MANAGEMENT**				
A8.1	**Operational procedures & responsibilities**				
A8.1.1	Documented operating procedures				
A8.1.2	Operational change controls				
A8.1.3	Incident management procedures				
A8.1.4	Segregation of duties				
A8.1.5	Segregation of development & operational facilities				
A8.1.6	External facilities management				
A8.2	**System planning & acceptance**				

BS7799 Annex A		Control		Exclusion	Justification
A8.2.1	Capacity planning				
A8.2.2	System acceptance				
A8.3	**Protection against malicious code**				
A8.3.1	Controls against malicious code				
A8.4	**Housekeeping**				
A8.4.1	Information back-up	1.2	Backup		
		2.8	Test restore		
A8.4.2	Operator logs				
A8.4.3	Fault logging				
A8.5	**Network management**				
A8.5.1	Network controls				
A8.6	**Media handling & security**				
A8.6.1	Management of removable computer media	2.1	Log of backups		
		2.3	Tapes stored in cupboard		
		2.4	One set of tapes stored off site		
		2.7	Obsolete media scrappped		
A8.6.2	Disposal of media	2.6	Media replaced		
		2.7	Obsolete media is scrappped		
A8.6.3	Information handling procedures	2.1	Log of backups		
		2.2	Tapes labelled		
		2.3	Tapes stored in cupboard		
		2.4	One set of tapes stored off site		
A8.6.4	Security of system documentation				
A8.7	**Exchanges of information & software**				
A8.7.1	Information & software exchange agreements				
A8.7.2	Security of media in transit				
A8.7.3	Electronic commerce security				
A8.7.4	Security of Electronic mail				
A8.7.5	Security of Electronic office systems				
A8.7.6	Publicly available systems				
A8.7.7	Other forms of information exchange				
A9	**ACCESS CONTROL**				
A9.1.	**Business requirement for access control**				
A9.1.1	Access control policy				
A9.2	**User access management**				
A9.2.1	User registration				
A9.2.2	Privilege management				
A9.2.3	User password management				
A9.2.4	Review of user access rights				
A9.3	**User responsibilities**				
A9.3.1	Password use				
A9.3.2	Unattended user equipment				
A9.4	**Network access control**				
A9.4.1	Policy on use of network services				
A9.4.2	Enforced path				
A9.4.3	User authentification for external connections				
A9.4.4	Node authentification				
A9.4.5	Remote diagnostic port protection				
A9.4.6	Segregation in networks				
A9.4.7	Network connection control				
A9.4.8	Network routeing control				
A9.4.9	Security of network services				
A9.5	**Operating system access control**				
A9.5.1	Automatic terminal identification				
A9.5.2	Terminal log-on procedures				
A9.5.3	User identification & authentification				
A9.5.4	Password management system				
A9.5.5	Use of system utilities				
A9.5.6	Duress alarm to safeguard users				
A9.5.7	Terminal time out				
A9.5.8	Limitation of connection time				
A9.6	**Application access control**				
A9.6.1	Information access restriction				
A9.6.2	Sensitive system isolation				
A9.7	**Monitoring system access**				
A9.7.1	Event logging				

BS7799 Annex A		Control		Exclusion	Justification
A9.7.2	Monitoring system use				
A9.7.3	Clock synchronization				
A9.8	**Mobile computing & teleworking**				
A9.8.1	Mobile computing		None	Yes	No laptops or PCs offsite
A9.8.2	Teleworking		None	Yes	No teleworking
A10	**SYSTEM DEVELOPMENT & MAINTENANCE**				
A10.1	**Security requirements of systems**				
A10.1.1	Security requirements analysis & specification				
A10.2	**Security in application systems**				
A10.2.1	Input data validation				
A10.2.2	Control of internal processing				
A10.2.3	Message authentification				
A10.2.4	Output data validation				
A10.3	**Cryptographic controls**				
A10.3.1	Policy on use of cryptographic controls				
A10.3.2	Encryption				
A10.3.3	Digital signatures				
A10.3.4	Non-repudiation services				
A10.3.5	Key management				
A10.4	**Security of system files**				
A10.4.1	Control of operational software				
A10.4.2	Protection of system test data				
A10.4.3	Access control to program source data				
A10.5	Security in development & support processes				
A10.5.1	Change control procedure				
A10.5.2	Technical review of operating system changes				
A10.5.3	Restrictions on changes to software packages				
A10.5.4	Covert channels & Trojan code				
A10.5.5	Outsourced software development				
A11	**BUSINESS CONTINUITY MANAGEMENT**				
A11.1	**Aspects of business continuity management**				
A11.1.1	Business continuity management process				
A11.1.2	Business continuity & impact analysis				
A11.1.3	Writing & implementing continuity plans				
A11.1.4	Business continuity planning framework				
A11.1.5	Testing, maintaining & re-assessing business continuity plans				
A12	**COMPLIANCE**				
A12.1	**Compliance with legal requirements**				
A12.1.1	Identification of applicable legislation				
A12.1.2	Intellectual property rights				
A12.1.3	Safeguarding of organisational records				
A12.1.4	Data protection & privacy of personal information				
A12.1.5	Prevention of misuse of information processing facilities				
A12.1.6	Regulation of cryptographic controls				
A12.1.7	Collection of evidence				
A12.2	**Reviews of security policy & technical compliance**				
A12.2.1	Compliance with security policy				
A12.2.2	Technical compliance checking				
A12.3	**System audit considerations**				
A12.3.1	System audit controls				
A12.3.2	Protection of system audit tools				