

Appendix 2

BS 7799 control to UCISA Document mapping

BS 7799 control addressed		UCISA Toolkit document	
5.1.1	Information security policy document	A	Information security policy and infrastructure
5.1.2	Review of the information security policy	A	Information security policy and infrastructure
6.1.1	Management commitment to information security	A	Information security policy and infrastructure
6.1.2	Information security co-ordination	A	Information security policy and infrastructure
6.1.3	Allocation of information security responsibilities	A E K L	Information security policy and infrastructure Personnel System management Network management
6.1.4	Authorization process for information processing facilities	J	System planning
6.1.5	Confidentiality agreements	E	Personnel
6.1.6	Contact with authorities	A	Information security policy and infrastructure
6.1.7	Contact with special interest groups	A	Information security policy and infrastructure
6.1.8	Independent review of information security	A	Information security policy and infrastructure
6.2.1	Identification of risks related to external parties	D	Outsourcing and third party access
6.2.2	Addressing security when dealing with customers	D	Outsourcing and third party access
6.2.3	Addressing security in third party agreements	D E	Outsourcing and third party access Personnel
7.1.1	Inventory of assets	G J	Information handling System planning
7.1.2	Ownership of assets	G J	Information handling System planning
7.1.3	Acceptable use of assets	G	Information handling
7.2.1	Classification guidelines	G	Information handling
7.2.2	Information labelling and handling	G O	Information handling Teleworking
8.1.1	Roles and responsibilities	D E	Outsourcing and third party access Personnel
8.1.2	Screening	E	Personnel
8.1.3	Terms and conditions of employment	C E	Compliance Personnel
8.2.1	Management responsibilities	E	Personnel

BS 7799 control addressed		UCISA Toolkit document	
8.2.2	Information security awareness, education and training	E K	Personnel System management
8.2.3	Disciplinary process	E	Personnel
8.3.1	Termination responsibilities	E	Personnel
8.3.2	Return of assets	E O	Personnel Teleworking
8.3.3	Removal of access rights	E	Personnel
9.1.1	Physical security perimeter	F	Operations
9.1.2	Physical entry controls	F	Operations
9.1.3	Securing offices, rooms and facilities	F	Operations
9.1.4	Protecting against external and environmental threats	J L	System planning Network management
9.1.5	Working in secure areas	F	Operations
9.1.6	Public access, delivery and loading areas	F	Operations
9.2.1	Equipment siting and protection	J L	System planning Network management
9.2.2	Supporting utilities	J	System planning
9.2.3	Cabling security	L	Network management
9.2.4	Equipment maintenance	J L O	System planning Network management Teleworking
9.2.5	Security of equipment off-premises	N O	Mobile computing Teleworking
9.2.6	Secure disposal or re-use of equipment	G	Information handling
9.2.7	Removal of property	G O	Information handling Teleworking
10.1.1	Documented operating procedures	C F	Compliance Operations
10.1.2	Change management	F K	Operations System management
10.1.3	Segregation of duties	F	Operations
10.1.4	Separation of development, test and operational facilities	F	Operations
10.2.1	Service delivery	D	Outsourcing and third party access
10.2.2	Monitoring and review of third party services	D	Outsourcing and third party access
10.2.3	Managing changes to third party services	D	Outsourcing and third party access
10.3.1	Capacity management	J K	System planning System management
10.3.2	System acceptance	F J	Operations System planning
10.4.1	Controls against malicious code	I K	Use of computers System management
10.4.2	Controls against mobile code	I K M	Use of computers System management Software management

BS 7799 control addressed		UCISA Toolkit document	
10.5.1	Information back-up	G I O	Information handling Use of computers Teleworking
10.6.1	Network controls	L	Network management
10.6.2	Security of network services	L	Network management
10.7.1	Management of removable media	G	Information handling
10.7.2	Disposal of media	G	Information handling
10.7.3	Information handling procedures	G	Information handling
10.7.4	Security of system documentation	F	Operations
10.8.1	Information exchange policies and procedures	G	Information handling
10.8.2	Exchange agreements	G	Information handling
10.8.3	Physical media in transit	G	Information handling
10.8.4	Electronic messaging	I	Use of computers
10.8.5	Business information systems	G	Information handling
10.9.1	Electronic commerce	G	Information handling
10.9.2	On-line transactions	G	Information handling
10.9.3	Publicly available information	G	Information handling
10.10.1	Audit logging	K	System management
10.10.2	Monitoring system use	K	System management
10.10.3	Protection of log information	K	System management
10.10.4	Administrator and operator logs	F	Operations
10.10.5	Fault logging	F	Operations
10.10.6	Clock synchronization	K	System management
11.1.1	Access control policy	H	User management
11.2.1	User registration	E H	Personnel User management
11.2.2	Privilege management	E H	Personnel User management
11.2.3	User password management	H	User management
11.2.4	Review of user access rights	E H	Personnel User management
11.3.1	Password use	I O	Use of computers Teleworking
11.3.2	Unattended user equipment	I O	Use of computers Teleworking
11.3.3	Clear desk and clear screen policy	G O	Information handling Teleworking
11.4.1	Policy on use of network services	L	Network management
11.4.2	User authentication for external connections	L N O	Network management Mobile computing Teleworking
11.4.3	Equipment identification in networks	L	Network management
11.4.4	Remote diagnostic and configuration port protection	L	Network management

BS 7799 control addressed		UCISA Toolkit document	
11.4.5	Segregation in networks	L	Network management
11.4.6	Network connection control	L	Network management
11.4.7	Network routing control	L	Network management
11.5.1	Secure log-on procedures	K	System management
11.5.2	User identification and authentication	I K	Use of computers System management
11.5.3	Password management system	I	Use of computers
11.5.4	Use of system utilities	J K	System planning System management
11.5.5	Session time-out	K	System management
11.5.6	Limitation of connection time	K	System management
11.6.1	Information access restriction	J	System planning
11.6.2	Sensitive system isolation	J	System planning
11.7.1	Mobile computing and communications	N	Mobile computing
11.7.2	Teleworking	O	Teleworking
12.1.1	Security requirements analysis and specification	M	Software management
12.2.1	Input data validation	G	Information handling
12.2.2	Control of internal processing	G	Information handling
12.2.3	Message integrity	G	Information handling
12.2.4	Output data validation	G	Information handling
12.3.1	Policy on the use of cryptographic controls	P	Cryptography
12.3.2	Key management	P	Cryptography
12.4.1	Control of operational software	F	Operations
12.4.2	Protection of system test data	F	Operations
12.4.3	Access control to program source code	F	Operations
12.5.1	Change control procedures	L M	Network management Software management
12.5.2	Technical review of applications after operating system changes	M	Software management
12.5.3	Restrictions on changes to software packages	M	Software management
12.5.4	Information leakage	G K M	Information handling System management Software management
12.5.5	Outsourced software development	D	Outsourcing and third party access
12.6.1	Control of technical vulnerabilities	F	Operations
13.1.1	Reporting information security events	E F	Personnel Operations
13.1.2	Reporting security weaknesses	E F	Personnel Operations
13.2.1	Responsibilities and procedures	F	Operations
13.2.2	Learning from information security incidents	E F	Personnel Operations

BS 7799 control addressed		UCISA Toolkit document	
13.2.3	Collection of evidence	C	Compliance
14.1.1	Including information security in the business continuity management process	B	Business continuity management and planning
14.1.2	Business continuity and risk assessment	B	Business continuity management and planning
14.1.3	Developing and implementing continuity plans including information security	B	Business continuity management and planning
14.1.4	Business continuity planning framework	B	Business continuity management and planning
14.1.5	Testing, maintaining and re-assessing business continuity plans	B	Business continuity management and planning
15.1.1	Identification of applicable legislation	C	Compliance
15.1.2	Intellectual property rights (IPR)	C	Compliance
15.1.3	Protection of organisational records	C	Compliance
15.1.4	Data protection and privacy of personal information	C E O	Compliance Personnel Teleworking
15.1.5	Prevention of misuse of information processing facilities	C O	Compliance Teleworking
15.1.6	Regulation of cryptographic controls	P	Cryptography
15.2.1	Compliance with security policies and standards	C E	Compliance Personnel
15.2.2	Technical compliance checking	C	Compliance
15.3.1	Information systems audit controls	C	Compliance
15.3.2	Protection of information systems audit tools	C	Compliance

