Annex A Controls				
Control	**Title**	**Control**	**Title**	**Theme**
		Access Control		
A.5.1.1	Policies for information security	A.5.1	Policies for information security	Organizational
A.5.1.2	Review of the policies for information security	A.5.1	Merged into A.5.1	
		Organization of Information		
A.6.1.1	Information security roles and responsibilities	A.5.2	Information security roles and responsibilities	Organizational
A.6.1.2	Segregation of duties	A.5.3	Segregation of duties	Organizational
A.6.1.3	Contact with authorities	A.5.5	Contact with authorities	Organizational
A.6.1.4	Contact with special interest groups	A.5.6	Contact with special interest groups	Organizational
		A.5.7	Threat intelligence	Organizational
A.6.1.5	Information security in project management	A.5.8	Information security in project management	Organizational
A.6.2.1	Mobile device policy	A.8.1	User end point devices	Technical
A.6.2.2	Teleworking	A.6.7	Remote working	People
		Human Resource Security		
A.7.1.1	Screening	A.6.1	Screening	People
A.7.1.2	Terms and conditions of employment	A.6.2	Terms and conditions of employment	People
A.7.2.1	Management responsibilities	A.5.4	Management responsibilities	Organizational
A.7.2.2	Information security awareness, education, and training	A.6.3	Information security awareness, education, and training	People
A.7.2.3	Disciplinary process	A.6.4	Disciplinary process	People
A.7.3.1	Termination or change of employment responsibilities	A.6.5	Termination or change of employment responsibilities	People

Asset Management				
A.8.1.1	Inventory of assets	A.5.9	Inventory of information and other associated assets	Organizational
A.8.1.2	Ownership of assets		Merged into A.5.9	
A.8.1.3	Acceptable use of assets	A.5.10	Acceptable use of information and other associated assets	Organizational
A.8.1.4	Return of assets	A.5.11	Return of assets	Organizational
A.8.2.1	Classification of information	A.5.12	Classification of information	Organizational
A.8.2.2	Labeling of information	A.5.13	Labeling of information	Organizational
A.8.2.3	Handling of assets		Merged into A.5.10	
A.8.3.1	Management of removable media	A.7.10	Storage media	Physical
A.8.3.2	Disposal of media		Merged into A.7.10	
A.8.3.3	Physical media transfer		Merged into A.7.10	

Access Control				
A.9.1.1	Access control policy	A.5.15	Access control	Organizational
A.9.1.2	Access to networks and network services		Merged into A.5.15	
A.9.2.1	User registration and de-registration	A.5.16	Identity management	Organizational
A.9.2.2	User access provisioning	A.5.18	Access rights	Organizational
A.9.2.3	Management of privileged access rights	A.8.2	Privileged access rights	Technical
A.9.2.4	Management of secret authentication information of users	A.5.17	Authentication information	Organizational
A.9.2.5	Review of user access rights		Merged into A.5.18	
A.9.2.6	Removal of adjustment of access rights		Merged into A.5.18	
A.9.3.1	Use of secret authentication information		Merged into A.5.17	
A.9.4.1	Information access restriction	A.8.3	Information access restriction	Technical
A.9.4.2	Secure log-in procedures	A.8.5	Secure authentication	Technical

A.9.4.3	Password management system		Merged into A.5.17	
A.9.4.4	Use of privileged utility programs	A.8.18	Use of privileged utility programs	Technical
A.9.4.5	Access control to program source code	A.8.4	Access to source code	Technical
		Cryptography		
A.10.1.1	Policy of the use of cryptographic controls	A.8.24	Use of cryptography	Technical
A.10.1.2	Key management		Merged into A.8.24 with A.10.1.1	
		Physical and Environmental Controls		
A.11.1.1	Physical security perimeter	A.7.1	Physical security perimeters	Physical
A.11.1.2	Physical entry controls	A.7.2	Physical entry	Physical
A.11.1.3	Securing offices, rooms, and facilities	A.7.3	Securing offices, rooms, and facilities	Physical
New		A.7.4	Physical security monitoring	Physical
A.11.1.4	Protecting against external and environmental threats	A.7.5	Protecting against external and environmental threats	Physical
A.11.1.5	Working in secure areas	A.7.6	Working in secure areas	Physical
A.11.1.6	Delivery and loading areas		Merged into A.7.2 with A.11.1.2	
A.11.2.1	Equipment siting and protection	A.7.8	Equipment siting and protection	Physical
A.11.2.2	Supporting utilities	A.7.11	Supporting utilities	Physical
A.11.2.3	Cabling security	A.7.12	Cabling security	Physical
A.11.2.4	Equipment maintenance	A.7.13	Equipment maintenance	Physical
A.11.2.5	Removal of assets		Merged into A.7.10	
A.11.2.6	Security of equipment and assets off-premises	A.7.9	Security of assets off-premises	Physical
A.11.2.7	Secure disposal or reuse of equipment	A.7.14	Secure disposal or reuse of equipment	Physical

A.11.2.8	Unattended user equipment		Merged into A.8.1 with A 6.2.1	
A.11.2.9	Clear desk and clear screen policy	A.7.7	Clear desk and clear screen	Physical
		Operations Security		
A.12.1.1	Documented operating procedures	A.5.37	Documented operating procedures	Organizational
A.12.1.2	Change management	A.8.32	Change management	Technical
A.12.1.3	Capacity management	A.8.6	Capacity management	Technical
A.12.1.4	Separation of development, testing, and operational environments	A.8.31	Separation of development, test, and operational environments	Technical
A.12.2.1	Controls against malware	A.8.7	Protection against malware	Technical
A.12.3.1	Information backup	A.8.13	Information backup	Technical
A.12.4.1	Event logging	A.8.15	Logging	Technical
A.12.4.2	Protection of log information		Merged into A.8.15	
A.12.4.3	Administrator and operator logs		Merged into A.8.15	
New		A.8.16	Monitoring activities	Technical
A.12.4.4	Clock Synchronization	A.8.17	Clock Synchronization	Technical
A.12.5.1	Installation of software on operational systems	A.8.19	Installation of software on operational systems	Technical
A.12.6.1	Management of technical vulnerabilities	A.8.8	Management of technical vulnerabilities	Technical
New		A.8.9	Configuration management	Technical
New		A.8.10	Information detection	Technical
New		A.8.11	Data masking	Technical
New		A.8.12	Data leakage prevention	Technical
A.12.6.2	Restrictions on software installation		Merged into A.8.19 with A.12.5.1	
A.12.7.1	Information systems audit controls	A.8.34	Protection of information systems during audit testing	Technical
		Communications Security		
A.13.1.1	Network controls	A.8.20	Networks security	Technical
A.13.1.2	Security of network services	A.8.21	Security of network services	Technical
A.13.1.3	Segregation in networks	A.8.22	Segregation of networks	Technical
New		A.8.23	Web filtering	Technical
A.13.2.1	Information transfer policies and procedures	A.5.14	Information transfer	Organizational
A.13.2.2	Agreements on information transfer		Merged into A.5.14	

A.13.2.3	Electronic messaging		Merged into A.5.14	
A.13.2.4	Confidentiality or nondisclosure agreements	A.6.6	Confidentiality or nondisclosure agreements	People
	System Acquisition, Development, and Maintenance			
A.14.1.1	Information security requirements analysis and specification		Merged into A.5.8 with A.6.1.5	
A.14.1.2	Securing application services on public networks	A.8.26	Application security requirements	Technical
A.14.1.3	Protecting application services transactions		Merged into A.8.26	
A.14.2.1	Secure development policy	A.8.25	Secure development policy	Technical
A.14.2.2	System change control procedures		Merged into A.8.32 with A.12.1.2, A.14.2.3, and A.14.2.4	
A.14.2.3	Technical review of applications after operating platform changes		Merged into A.8.32 with A.12.1.2, A.14.2.2, and A.14.2.4	
A.14.2.4	Restriction on changes to software packages		Merged into A. 8.32 with A.12.1.2, A.14.2.2, and A.14.2.3	
A.14.2.5	Secure system engineering packages	A.8.27	Secure system architecture and engineering principles	Technical
A.14.2.6	Secure development environment		Merged into A.8.31 with A.12.1.4	

A.14.2.6	Secure development environment		Merged into A.8.31 with A.12.1.4	
New		A.8.28	Secure coding	Technical
A.14.2.7	Outsourced development	A.8.30	Outsourced development	Technical
A.14.2.8	System security testing	A.8.29	Security testing in development and acceptance	Technical
A.14.2.9	System acceptance testing		Merged into A.8.29 with A.14.2.8	
A.14.3.1	Protection of test data	A.8.33	Test information	Technical
	Supplier Relationships			
A.15.1.1	Information security policy for supplier relationships	A.5.19	Information security in supplier relationships	Organizational
A.15.1.2	Addressing security within supplier agreements	A.5.20	Addressing information security within supplier agreements	Organizational
A.15.1.3	Information and communication technology supply chain	A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Organizational
A.15.2.1	Monitoring and review of supplier services	A.5.22	Monitoring, review, and change management of supplier services	Organizational
A.15.2.2	Managing changes to supplier services		Merged into A.5.22 with A.15.2.1	
New		A.5.23	Information security for use of cloud services	Organizational

Information Security Incident Management				
A.16.1.1	Responsibilities and procedures	A.5.24	Information security incident management planning and preparation	Organizational
A.16.1.2	Reporting information security events	A.6.8	Information security event reporting	People
A.16.1.3	Reporting information security weaknesses		Merged into A.6.8 with A.16.1.2	
A.16.1.4	Assessment and decision on information security events	A.5.25	Assessment and decision on information security events	Organizational
A.16.1.5	Response to information security incidents	A.5.26	Response to information security incidents	Organizational
A.16.1.6	Learning from information security incidents	A.5.27	Learning from information security incidents	Organizational
A.16.1.7	Collection of evidence	A.5.28	Collection of evidence	Organizational
Information Security Aspects of Business Continuity Management				
A.17.1.1	Planning information security continuity	A.5.29	Information security during disruption	Organizational
A.17.1.2	Implementing information security continuity		Merged into A.5.29 with A.17.1.1 and A.17.1.3	
A.17.1.3	Verify, review, and evaluate information security continuity		Merged into A.5.29 with A.17.1.1 and A.17.1.2	
New		A.5.30	ICT readiness for business continuity	Organizational
A.17.2.1	Availability of information processing facilities	A.8.14	Redundancy of information processing facilities	Technical
Compliance				
A.18.1.1	Identification of applicable legislation and contractual requirements	A.5.31	Legal, statutory, regulatory, and contractual requirements	Organizational
A.18.1.2	Intellectual property rights	A.5.32	Intellectual property rights	Organizational
A.18.1.3	Protection of records	A.5.33	Protection of records	Organizational
A.18.1.4	Privacy and protection of personally identifiable information	A.5.34	Privacy and protection of personally identifiable information	Organizational
A.18.1.5	Regulation of cryptographic controls		Merged into A.5.31 with A.18.1.1	
Information Security Reviews				
A.18.2.1	Independent review of information security	A.5.35	Independent review of information security	Organizational
A.18.2.2	Compliance with security policies and standards	A.5.36	Compliance with policies, rules, and standards for information security	Organizational

A.18.2.3 Technical compliance review	Merged into A.5.36 with A.18.2.2