ISO 27001:2013 Controls			Control Included	Reasons for selection			
Controls	Sec	Control Objective / Control		Legal requirements	Contractual obligations	Business requirements / Adopted best practices	Risk assessment
A.5 Information Security policies	5.1	Management direction for information security					
	5.1.1	Policies for information security	Yes			X	
	5.1.2	Review of the policies for information security	Yes			X	
A.6 Organization of Information security	6.1	Internal Organization					
	6.1.1	Information security roles and responsibilities	Yes			X	
	6.1.2	Segregation of duties	Yes			X	
	6.1.3	Contact with authorities	Yes	X			
	6.1.4	Contact with special interest groups	Yes			X	
	6.1.5	Information security in project management	Yes		X		
	6.2	Mobile Devices and teleworking					
	6.2.1	Mobile Devices policy	Yes				X
	6.2.2	Teleworking	Yes			X	X
A.7 Human resource security	7.1	Prior to employment					
	7.1.1	Screening	Yes				X
	7.1.2	Terms and conditions of employment	Yes	X			X
	7.2	During employment					
	7.2.1	Management responsibilities	Yes				X
	7.2.2	Information security, education and training	Yes				X
	7.2.3	Disciplinary process	Yes	X			X
	7.3	Termination and change of employment					

	7.3.1	Termination or change of employment responsibilities	Yes	X			
A.8 Asset management	8.1	Responsibility for Assets					
	8.1.1	Inventory of assets	Yes			X	
	8.1.2	Ownership of assets	Yes			X	
	8.1.3	Acceptable use of assets	Yes			X	
	8.1.4	Return of assets	Yes			X	
	8.2	Information classification					
	8.2.1	Classification of information	Yes			X	
	8.2.2	Labelling of information	Yes			X	
	8.2.3	Handling of assets	Yes			X	
	8.3	Media handling					
	8.3.1	Management of removable media	Yes			X	X
	8.3.2	Disposal of media	Yes			X	X
	8.3.3.	Physical media transfer	Yes			X	X
A.9 Access control	9.1	Business requirements of access control					
	9.1.1	Access control policy	Yes				X
	9.1.2	Access to networks and network services	Yes			X	
	9.2	User access management					
	9.2.1	User registration and de-registration	Yes			X	
	9.2.2	User access provisioning	Yes			X	
	9.2.3	Management of privileged access rights	Yes			X	
	9.2.4	Management of secret authentication information of users	Yes			X	X
	9.2.5	Review of user access rights	Yes			X	
	9.2.6	Removal or adjustment of access rights	Yes			X	
	9.3	User responsibilities					
	9.3.1	Use of secret authentication information	Yes				X
	9.4	System and application access control					

	9.4.1	Information access restriction	Yes			X	
	9.4.2	Secure log-on procedures	Yes			X	
	9.4.3	Password management system	Yes			X	
	9.4.4	Use of privileged utility programs	Yes			X	
	9.4.5	Access control to program source code	Yes			X	
A.10 Cryptography	10.1	Cryptographic controls					
	10.1.1	Policy on the use of cryptographic controls	Yes		X		X
	10.1.2	Key management	Yes			X	
A.11 Physical and environmental security	11.1	Secure areas					
	11.1.1	Physical security perimeter	Yes				X
	11.1.2	Physical entry controls	Yes				
	11.1.3	Securing offices, rooms and facilities	Yes				X
	11.1.4	Protecting against external and environmental threats	Yes				X
	11.1.5	Working in secure areas	Yes				X
	11.1.6	Delivery and loading areas	N/A				
	11.2	Equipment					
	11.2.1	Equipment siting and protection	Yes				X
	11.2.2	Supporting utilities	Yes				X
	11.2.3	Cabling security	Yes				X
	11.2.4	Equipment maintenance	Yes				X
	11.2.5	Removal of assets	Yes				X
	11.2.6	Security of equipment and assets off- premises	Yes				X
	11.2.7	Secure disposal or re-use of equipment	Yes				X
	11.2.8	Unattended user equipment	Yes				X
	11.2.9	Clear desk and clear screen policy	Yes				X
A.12 Operations	12.1	Operational procedures and responsibilities					

security	12.1.1	Documented operating procedures	Yes			X	
	12.1.2	Change management	Yes			X	
	12.1.3	Capacity management	Yes			X	
	12.1.4	Separation of development, testing and operational environments	Yes			X	X
	12.2	Protection from malware					
	12.2.1	Controls against malware	Yes				X
	12.3	Backup					
	12.3.1	Information backup	Yes				X
	12.4	Logging and monitoring					
	12.4.1	Event logging	Yes			X	
	12.4.2	Protection of log information	Yes	X			
	12.4.3	Administrator and operator logs	Yes			X	
	14.4.4	Clock synchronisation	Yes			X	
	12.5	Control of operational software					
	12.5.1	Installation of software on operational systems	Yes			X	
	12.6	Technical Vulnerability Management					
	12.6.1	Management of Technical vulnerabilities	Yes				X
	12.6.2	Restrictions on software installation	Yes			X	
	12.7	Information systems audit considerations					
	12.7.1	Information systems audit controls	Yes			X	
A.13 Communications security	13.1	network security management					
	13.1.1	Network controls	Yes			X	X
	13.1.2	Security of network services	Yes				X
	13.1.3	Segregation of networks	Yes				X
	13.2	Information transfer					
	13.2.1	Information transfer policies and procedures	Yes			X	X
	13.2.2	Agreements on information transfer	Yes		X		
	13.2.3	Electronic messaging	Yes			X	X

	13.2.4	Confidentiality or non-disclosure agreements	Yes				X
A.14 system acquisition, development and maintenance	14.1	Security requirements of information systems					
	14.1.1	Information security requirements analysis and specification	Yes			X	X
	14.1.2	Securing application services on public networks	Yes			X	X
	14.1.3	Protecting application services transactions	Yes			X	X
	14.2	Security in development and support processes					
	14.2.1	Secure development policy	Yes			X	X
	14.2.2	System change control procedures	Yes			X	X
	14.2.3	Technical review of applications after operating platform	Yes			X	X
	14.2.4	Restrictions on changes to software	Yes			X	X
	14.2.5	Secure system engineering principles	Yes			X	
	14.2.6	Secure development environment	Yes			X	
	14.2.7	Outsourced development	Yes			X	
	14.2.8	System security testing	Yes			X	
	14.2.9	System acceptance testing	Yes			X	
	14.3	Test data					
	14.3.1	Protection of test data	Yes			X	
A.15 Supplier relationships	15.1	Information security in supplier relationships					
	15.1.1	Information security policy for supplier relationships	Yes			X	
	15.1.2	Addressing security within supplier agreements	Yes			X	
	15.1.3	Information and communication technology supply chain	Yes			X	
	15.2	Supplier service delivery management					

	15.2.1	Monitoring and review of supplier services	Yes				X
	15.2.2	Managing changes to supplier services	Yes				X
A.16 Information security incident management	16.1	Management of Information security incidents and improvements					
	16.1.1	Responsibilities and procedures	Yes			X	X
	16.1.2	Reporting information security events	Yes			X	
	16.1.3	Reporting information security weaknesses	Yes			X	X
	16.1.4	Assessment of and decision on information security events	Yes			X	
	16.1.5	Response to information security incidents	Yes			X	
	16.1.6	Learning from information security incidents	Yes			X	
	16.1.7	Collection of evidence	Yes			X	X
A.17 Information security aspects of business continuity management	17.1	Information security continuity					
	17.1.1	Planning information security continuity	Yes				X
	17.1.2	Implementing information security continuity	Yes				X
	17.1.3	Verify, review and evaluate information security continuity	Yes				X
	17.2	Redundancies					
	17.2.1	Availability of information processing facilities	Yes				X
A.18 Compliance	18.1	Compliance with legal and contractual requirements					
	18.1.1	Identification of applicable legislation and contractual requirements	Yes	X			
	18.1.2	Intellectual property rights	Yes	X			
	18.1.3	Protection of records	Yes	X			
	18.1.4	Privacy and protection of personally identifiable information	Yes	X			
	18.1.5	Regulation of cryptographic controls	Yes	X			X

18.2	information security reviews					
18.2.1	Independent review of information security	Yes				X
18.2.2	Compliance with security policies and standards	Yes	X	X		
18.2.3	Technical compliance review	Yes			X	X

Means of implementation