ISO 27001 / WLA Controls			ISMS Applicable	Reasons for Selection		
				LR/CO	BR/BP	RA
Clause	**Sec**	**Control Objective / Control**				
1-10 Mandatory Clauses	Mandatory Clauses					
	1	Scope	Yes		X	
	2	Normative References	Yes		X	
	3	Terms and Definitions	Yes		X	
	4	Context of the Organization	Yes		X	
	5	Leadership	Yes		X	
	6	Planning	Yes		X	
	7	Support	Yes		X	
	8	Operation	Yes		X	
	9	Performance Evaluation	Yes		X	
	10	Improvement	Yes		X	
5.0 Security Policy	5.1	Information Security Policy				
	5.1.1	Information Security Policy Document	Yes		X	
	5.1.2	Review of Information Security Policy	Yes		X	
6.0 Organization of Information Security	6.1	Internal Organization				
	6.1.1	Information Security roles and responsibilties	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 device policy	Yes		X	
	6.2.2	Teleworking	Yes		X	
7.0 Human Resource Security	7.1	Prior to Employment				
	7.1.1	Screening	Yes		X	X
	7.1.2	Terms and conditions of employment	Yes	X	X	X
	7.2	During Employment				
	7.2.1	Management Responsibility	Yes		X	
	7.2.2	Information security awareness, education and training	Yes		X	X
	7.2.3	Disciplinary process	Yes	X	X	
	7.3	Termination or change of employment				
	7.3.1	Termination or change of employment responsibilities	Yes		X	
8.0 Asset Management	8.1	Responsibility for Assets			X	
	8.1.1	Inventory of assets	Yes		X	
	8.1.2	Ownership of Assets	Yes	X	X	
	8.1.3	Acceptable use of assets	Yes	X	X	
	8.1.4	Return of assets	Yes			
	8.2	Information classification			X	
	8.2.1	Classification Guidelines	Yes		X	
	8.2.2	Information Labeling and Handling	Yes			
	8.3	Media Handling			X	
	8.3.1	Management of removable media	Yes		X	
	8.3.2	Disposal of media	Yes		X	
	8.3.3	Physical media transfer	Yes			
	9.1	Business Requirement for Access Control				
	9.1.1	Access control Policy	Yes	X	X	
	9.1.2	Access to networks and network service	Yes	X	X	

9.0 Access Control	9.2	User Access Management				
	9.2.1	User Registration and de-registration	Yes		X	X
	9.2.2	User access provisioning	Yes		X	X
	9.2.3	Management of priviledged access rights	Yes		X	X
	9.2.4	Management of secret authentication information for	Yes		X	X
	9.2.5	Review of user access rights	Yes		X	X
	9.2.6	Removal of access rights	Yes		X	X
	9.3	User Responsibilities				
	9.3.1	Use of secret authentication information	Yes		X	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	X	X
	9.4.4	Use of priviledged utility programs	Yes		X	
	9.4.5	Access control to program source code	Yes		X	
A.10 Cryptographic Controls	10.1	Cryptographic Controls				
	10.1.1	Policy on use of cryptographic controls	Yes		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	X	
	11.1.2	Physical Entry Controls	Yes		X	
	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	Yes		X	
	11.2	Equipment				
	11.2.1	Equipment sitting and protection	Yes		X	
	11.2.2	Support utilities	Yes		X	
	11.2.3	Cabling security	Yes		X	
	11.2.4	Equipment Maintenance	Yes		X	X
	11.2.5	Removal of assets	Yes		X	
	11.2.6	Security of equipment and assets off-premises	Yes		X	X
	11.2.7	Secure disposal or reuse of equipment	Yes	X	X	
	11.2.8	Unattended user equipment	Yes		X	X
	11.2.9	Clear Desk and Clear Screen Policy	Yes		X	
A.12 Operations Security	12.1	Operational Procedures and responsibilties				
	12.1.1	Documented operating Procedures	Yes		X	
	12.1.2	Change Management	Yes		X	
	12.1.3	Capacity management	Yes	X	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	X	
	12.4	Logging and monitoring				
	12.4.1	Event Logging	Yes		X	X
	12.4.2	Protection of log information	Yes		X	X
	12.4.3	Administrator and operator logs	Yes		X	
	12.4.4	Clock synchronization	Yes		X	
	12.5	Control of operational software				
	12.5.1	Installation of software on operational systems	Yes		X	X
	12.6	Technical Vulnerabilty management				
	12.6.1	Management of technical vulnerabilties	Yes		X	
	12.6.2	Restrictions on software installation	Yes		X	

	12.7					
	12.7.1	Information Systems audit controls	Yes		X	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	Segretion of networks	Yes		X	X
	13.2	Information Transfer				
	13.2.1	Information Transfer policies and procedures	Yes		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	
	14.1.2	Securing application services on public networks	Yes		X	
	14.1.3	Protecting Application Services transactions	Yes		X	
	14.2	Security in Development & Support Processes				
	14.2.1	Secure development policy	Yes		X	
	14.2.2	System change Control Procedures	Yes		X	X
	14.2.3	Technical review of applications after Operating system	Yes		X	X
	14.2.4	Restrictions on changes to software packages	Yes		X	X
	14.2.5	Secure system engineering principles	Yes		X	X
	14.2.6	Secure development environment	Yes		X	X
	14.2.7	Outsourced development	No			
	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 system test data	Yes	X	X	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	
	16.1.2	Reporting Information security events	Yes		X	
	16.1.3	Reporting security weaknesses	Yes		X	
	16.1.4	Assesment of and decision on information security incidents	Yes		X	
	16.1.5	Response to information security events	Yes		X	
	16.1.6	Learning for Information security incidents	Yes		X	
	16.1.7	Collection of evidence	Yes	X	X	
A.17 Information	17.1	Information Security continuity				
	17.1.1	Planning information security continuity	Yes		X	
	17.1.2	Business continuity and Risk Assessment	Yes	X	X	

Security Aspects of Business Continuity Management	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 legislations and contractual requirements	Yes	X	X	
	18.1.2	Intellectual Property Rights (IPR)	Yes	X	X	
	18.1.3	Protection of records	Yes	X	X	
	18.1.4	Privacy and protection of personally identifiable	Yes	X	X	
	18.1.5	Regulation of cryptographic controls	Yes		X	
	18.2	Information Security Reviews				
	18.2.1	Independent review of information security	Yes		X	X
	18.2.2	Compliance with security policies and standards	Yes		X	
	18.2.3	Technical compliance checking	Yes	X	X	X
ISO 27018 Annex A Controls			**ISMS Applicable**	**Reasons for Selectio**		
				LR/CO	**BR/BP**	**RA**
Clause	**Sec**	**Control Objective / Control**				
A.1 Consent	1.1	Obligation to co-operate regarding PII principals' rights	Yes		X	
A.2 Purpose,	2.1	Public Cloud PII Processors Purpose	Yes		X	
Legitimacy and	2.2	Public Cloud PII processors commercial use	Yes		X	
A.3 Collection Limitation	3	Limitation of collection	Yes		X	
A.4 Data Minimization	4.1	Secure erasure of temporary files	Yes		X	
A.5 Use, Retention and Disclosure	5.1	PII disclosure notification	Yes		X	
	5.2	Recording of PII Disclosures	Yes		X	
A.6 Accuracy and Quality	6	Accuracy and quality	Yes		X	
	6.1	Recording of PII Disclosures	Yes		X	
A.7 Openness, Transparency, and Notice	7.1	Disclosure of subcontracted PII Processing	Yes		X	
A.8 Individual Participation and access	8	Individual participation and access	No			
A.9 Accountability	9.1	Notification of Data Breach involving PII	Yes		X	
	9.2	Retention period for administrative security policies and guidelines	Yes		X	
	9.3	PII Return, transfer and disposal	Yes		X	
A.10 Information Security	10.1	Confidentiality or non-disclosure agreements	Yes		X	
	10.2	Restriction on creation of hardcopy material	Yes		X	
	10.3	Control of logging of data restoration	No			
	10.4	Protecting data on storage media leaving the premises	Yes		X	
	10.5	Use of unencrypted portable media and devices	Yes		X	
	10.6	Encryption of PII transmitted over public data transmission networks	Yes		X	
	10.7	Secure disposal of hardcopy materials	Yes		X	
	10.8	Unique use of user IDS	Yes		X	
	10.9	Records of authorized users	Yes		X	

	10.10	User ID management	Yes		X	
	10.11	Contract Measures	Yes		X	
	10.12	Sub-contracted PII Processing	Yes		X	
	10.13	Access to data on pre-used data storage space	Yes		X	
A.11 Privacy Compliance	11.1	Geographical location of PII	Yes		X	
	11.2	Intended destination of PII	Yes		X	