Statement of Applicability

Current as of: 01-11-2018

Legend (for Selected Controls and Reasons for controls selection)

LR: **legal requirements**,CO: **contractual obligations**,BR/BP: **business requirements/adopted best practices**,RRA: **results of risk assessment**

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection			
					LR	CO	BR/BP	RRA
Clause	Sec	Control Objective/Control						
5 Security Policies	5.1	Management direction for information security						
	5.1.1	Policies for information	Performed				x	
	5.1.2	Review of the policies for information security	Performed				x	
6 Organisation of information security	6.1	Internal organisation						
	6.1.1	Information security roles and responsibilities	Performed				x	
	6.1.2	Segregation of duties	Performed					x
	6.1.3	Contact with authorities	Performed		x			x
	6.1.4	Contact with special interest groups	Performed					x
	6.1.5	Information security in project management	Performed					x
	6.2	Mobile devices and teleworking						
	6.2.1	Mobile device policy	Performed					x
	6.2.2	Teleworking	Performed					x
7 Human resource security	7.1	Prior to employment						
	7.1.1	Screening	Performed					x
	7.1.2	Terms and conditions of employment	Performed					x
	7.2	During employment						
	7.2.1	Management responsibilities	Performed					x
	7.2.2	Information security awareness, education and training	Performed					x
	7.2.3	Disciplinary process	Performed					x
	7.3	Termination and change of employment						
	7.3.1	Termination or change of employment responsibilities	Performed					x
8 Asset management	8.1	Responsibility for assets						
	8.1.1	Inventory of assets	Performed					x
	8.1.2	Ownership of assets	Performed					x
	8.1.3	Acceptable use of assets	Performed					x
	8.1.4	Return of assets	Performed					x
	8.2	Information classification						
	8.2.1	Classification of information	Performed					x
	8.2.2	Labeling of information	Performed					x
	8.2.3	Handling of assets	Performed					x
	8.3	Media handling						
	8.3.1	Management of removable media	Performed					x
	8.3.2	Disposal of media	Performed					x
	8.3.3	Physical media transfer	Performed					x
9 Access control	9.1	Business requirements of access control						
	9.1.1	Access control policy	Performed					x
	9.1.2	Access to networks and network services	Performed					x
	9.2	User access management						
	9.2.1	User registration and de-registration	Performed					x
	9.2.2	User access provisioning	Performed					x
	9.2.3	Management of privileged access rights	Performed					x
	9.2.4	Management of secret authentication information of users	Performed					x
	9.2.5	Review of user access rights	Performed					x
	9.2.6	Removal or adjustment of access rights	Performed					x
	9.3	User responsibilities						
	9.3.1	Use of secret authentication information	Performed					x
	9.4	System and application access control						
	9.4.1	Information access restriction	Performed					x
	9.4.2	Secure log-on procedures	Performed					x
	9.4.3	Password management system	Performed					x
	9.4.4	Use of privileged utility programs	Performed					x
	9.4.5	Access control to program source code	Performed			x		x
10 Cryptography	10.1	Cryptographic controls						
	10.1.1	Policy on the use of cryptographic controls	Performed					x
	10.1.2	Key management	Performed					x
11 Physical and environmental security	11.1	Secure areas						
	11.1.1	Physical security perimeter	Performed					x
	11.1.2	Physical entry controls	Performed					x
	11.1.3	Securing office, room and facilities	Performed					x
	11.1.4	Protecting against external end environmental threats	Performed					x
	11.1.5	Working in secure areas	Performed					x
	11.1.6	Delivery and loading areas		Not applicable				
	11.2	Equipment						
	11.2.1	Equipment siting and protection	Performed					x
	11.2.2	Supporting utilities	Performed					x
	11.2.3	Cabling security	Performed					x
	11.2.4	Equipment maintenance	Performed					x
	11.2.5	Removal of assets	Performed					x
	11.2.6	Security of equipment and assets off-premises	Performed					x
	11.2.7	Secure disposal or re-use of equipment	Performed					x
	11.2.8	Unattended user equipment	Performed					x
	11.2.9	Clear desk and clear screen policy	Performed					x

12 Operations security	12.1	Operational procedures and responsibilities						
	12.1.1	Documented operating procedures	Performed					x
	12.1.2	Change management	Performed					x
	12.1.3	Capacity management	Performed					x
	12.1.4	Separation of development, testing and operational environments	Performed					x
	12.2	Protection from malware						
	12.2.1	Controls against malware	Performed					x
	12.3	Backup						
	12.3.1	Information backup	Performed				x	x
	12.4	Logging and monitoring						
	12.4.1	Event logging	Performed					x
	12.4.2	Protection of log information	Performed					x
	12.4.3	Administrator and operator logs	Performed					x
	12.4.4	Clock synchronisaton	Performed				x	
	12.5	Control of operational software						
	12.5.1	Installation of software on operational systems	Performed					x
	12.6	Technical vulnerability management						
	12.6.1	Management of technical vulnerabilities	Performed				x	x
	12.6.2	Restrictions on software installation	Performed					x
	12.7	Information systems audit considerations						
	12.7.1	Information systems audit controls	Performed					x
13 Communications security	13.1	Network security management						
	13.1.1	Network controls	Performed					x
	13.1.2	Security of network services	Performed					x
	13.1.3	Segregation in networks	Performed					x
	13.2	Information transfer						
	13.2.1	Information transfer policies and procedures	Performed					x
	13.2.2	Agreements on information transfer	Performed			x		x
	13.2.3	Electronic messaging	Performed					x
	13.2.4	Confidentiality or non-disclosure agreements	Performed			x		x
14 System acquisition, development and maintenance	14.1	Security requirements of information systems						
	14.1.1	Information security requirements analysis and specification	Performed					x
	14.1.2	Securing applications services on public networks	Performed					x
	14.1.3	Protecting application services transactions	Performed					x
	14.2	Security in development and support processes						
	14.2.1	Secure development policy	Performed					x
	14.2.2	System change control procedures	Performed					x
	14.2.3	Technical review of applications after operating platform changes	Performed					x
	14.2.4	Restrictions on changes to software packages	Performed					x
	14.2.5	Secure system engineering principles	Performed					x
	14.2.6	Secure development environment	Performed					x
	14.2.7	Outsourced development		Not applicable				
	14.2.8	System security testing	Performed					x
	14.2.9	System acceptance testing	Performed					x
	14.3	Test data						
	14.3.1	Protection of test data	Performed					x
15 Supplier relationships	15.1	Information security in supplier relationships						
	15.1.1	Information security policy for supplier relationships	Performed			x		x
	15.1.2	Addressing security within supplier agreements	Performed			x		x
	15.1.3	Information and communication technology supply chain	Performed			x		x
	15.2	Supplier service delivery management						
	15.2.1	Monitoring and review of supplier services	Performed			x		x
	15.2.2	Managing changes to supplier services	Performed			x		x
16 Information security incident management	16.1	Management of information security incidents and improvements						
	16.1.1	Responsibilities and procedures	Performed			x		x
	16.1.2	Reporting information security events	Performed					x
	16.1.3	Reporting information security weaknesses	Performed					x
	16.1.4	Assessment of and decision on information security events	Performed					x
	16.1.5	Response to information security incidents	Performed					x
	16.1.6	Learning from information security incidents	Performed					x
	16.1.7	Collection of evidence	Performed					x
17 Information security aspects of business continuity management	17.1	Information security continuity						
	17.1.1	Planning information security continuity	Performed					x
	17.1.2	Implementing information security continuity	Performed					x
	17.1.3	Verify, review and evaluate information security continuity	Performed					x
	17.2	Redundancies						
	17.2.1	Availability of information processing facilities	Performed					x
18 Compliance	18.1	Compliance with legal and contractual requirements						
	18.1.1	Identification of applicable legislation and contractual requirements	Performed		x	x		x
	18.1.2	Intellectual property rights	Performed		x			x
	18.1.3	Protection of records	Performed					x
	18.1.4	Privacy and protection of personally identifiable information	Performed					x
	18.1.5	Regulation of cryptographic controls	Performed			x		x
	18.2	Information security reviews						
	18.2.1	Independent review of information security	Performed			x		
	18.2.2	Compliance with security policies and standards	Performed			x		
	18.2.3	Technical compliance review	Performed			x		