

ISO/IEC 27001:2013 Annex A controls			Current controls
Clause	Sec	Control Objective/Control	
5 Security Policies	5.1	Management direction for information security	
	5.1.1	Policies for information	•
	5.1.2	Review of the policies for information security	•
6 Organisation of information security	6.1	Internal organisation	
	6.1.1	Information security roles and responsibilities	•
	6.1.2	Segregation of duties	•
	6.1.3	Contact with authorities	•
	6.1.4	Contact with special interest groups	•
	6.1.5	Information security in project management	•
	6.2	Mobile devices and teleworking	
	6.2.1	Mobile device policy	•
6.2.2	Teleworking	•	
7 Human resource security	7.1	Prior to employment	
	7.1.1	Screening	•
	7.1.2	Terms and conditions of employment	•
	7.2	During employment	
	7.2.1	Management responsibilities	•
	7.2.2	Information security awareness, education and training	•
	7.2.3	Disciplinary process	•
	7.3	Termination and change of employment	
7.3.1	Termination or change of employment responsibilities	•	
8 Asset management	8.1	Responsibility for assets	
	8.1.1	Inventory of assets	•
	8.1.2	Ownership of assets	•
	8.1.3	Acceptable use of assets	•
	8.1.4	Return of assets	•
	8.2	Information classification	
	8.2.1	Classification of information	•
	8.2.2	Labeling of information	•
	8.2.3	Handling of assets	•
	8.3	Media handling	
	8.3.1	Management of removable media	•
	8.3.2	Disposal of media	•
8.3.3	Physical media transfer	•	
9 Access control	9.1	Business requirements of access control	
	9.1.1	Access control policy	•
	9.1.2	Access to networks and network services	•
	9.2	User access management	
	9.2.1	User registration and de-registration	•
	9.2.2	User access provisioning	•
	9.2.3	Management of privileged access rights	•
	9.2.4	Management of secret authentication information of users	•
	9.2.5	Review of user access rights	•
	9.2.6	Removal or adjustment of access rights	•
	9.3	User responsibilities	
9.3.1	Use of secret authentication information	•	

	9.4	System and application access control	
	9.4.1	Information access restriction	•
	9.4.2	Secure log-on procedures	•
	9.4.3	Password management system	•
	9.4.4	Use of privileged utility programs	•
	9.4.5	Access control to program source code	•
10 Cryptography	10.1	Cryptographic controls	
	10.1.1	Policy on the use of cryptographic controls	•
	10.1.2	Key management	•
11 Physical and environmental security	11.1	Secure areas	
	11.1.1	Physical security perimeter	•
	11.1.2	Physical entry controls	•
	11.1.3	Securing office, room and facilities	•
	11.1.4	Protecting against external and environmental threats	•
	11.1.5	Working in secure areas	•
	11.1.6	Delivery and loading areas	•
	11.2	Equipment	
	11.2.1	Equipment siting and protection	•
	11.2.2	Supporting utilities	•
	11.2.3	Cabling security	•
	11.2.4	Equipment maintenance	•
	11.2.5	Removal of assets	•
	11.2.6	Security of equipment and assets off-premises	•
	11.2.7	Secure disposal or re-use of equipment	•
11.2.8	Unattended user equipment	•	
11.2.9	Clear desk and clear screen policy	•	
12 Operations security	12.1	Operational procedures and responsibilities	
	12.1.1	Documented operating procedures	•
	12.1.2	Change management	•
	12.1.3	Capacity management	•
	12.1.4	Separation of development, testing and operational environments	•
	12.2	Protection from malware	
	12.2.1	Controls against malware	•
	12.3	Backup	
	12.3.1	Information backup	•
	12.4	Logging and monitoring	
	12.4.1	Event logging	•
	12.4.2	Protection of log information	•
	12.4.3	Administrator and operator logs	•
	12.4.4	Clock synchronisation	•
	12.5	Control of operational software	
	12.5.1	Installation of software on operational systems	•
	12.6	Technical vulnerability management	
	12.6.1	Management of technical vulnerabilities	•
	12.6.2	Restrictions on software installation	•
	12.7	Information systems audit considerations	
12.7.1	Information systems audit controls	•	
13 Communications security	13.1	Network security management	
	13.1.1	Network controls	•
	13.1.2	Security of network services	•
	13.1.3	Segregation in networks	•
	13.2	Information transfer	
	13.2.1	Information transfer policies and procedures	•
	13.2.2	Agreements on information transfer	•
	13.2.3	Electronic messaging	•
13.2.4	Confidentiality or non-disclosure agreements	•	

14 System acquisition, development and maintenance	14.1	Security requirements of information systems	
	14.1.1	Information security requirements analysis and specification	•
	14.1.2	Securing applications services on public networks	•
	14.1.3	Protecting application services transactions	•
	14.2	Security in development and support processes	
	14.2.1	Secure development policy	•
	14.2.2	System change control procedures	•
	14.2.3	Technical review of applications after operating platform changes	•
	14.2.4	Restrictions on changes to software packages	•
	14.2.5	Secure system engineering principles	•
	14.2.6	Secure development environment	•
	14.2.7	Outsourced development	•
	14.2.8	System security testing	•
	14.2.9	System acceptance testing	•
14.3	Test data		
14.3.1	Protection of test data	•	
15 Supplier relationships	15.1	Information security in supplier relationships	
	15.1.1	Information security policy for supplier relationships	•
	15.1.2	Addressing security within supplier agreements	•
	15.1.3	Information and communication technology supply chain	•
	15.2	Supplier service delivery management	
	15.2.1	Monitoring and review of supplier services	•
15.2.2	Managing changes to supplier services	•	
16 Information security incident management	16.1	Management of information security incidents and improvements	
	16.1.1	Responsibilities and procedures	•
	16.1.2	Reporting information security events	•
	16.1.3	Reporting information security weaknesses	•
	16.1.4	Assessment of and decision on information security events	•
	16.1.5	Response to information security incidents	•
	16.1.6	Learning from information security incidents	•
	16.1.7	Collection of evidence	•
17 Information security aspects of business continuity management	17.1	Information security continuity	
	17.1.1	Planning information security continuity	•
	17.1.2	Implementing information security continuity	•
	17.1.3	Verify, review and evaluate information security continuity	•
	17.2	Redundancies	
17.2.1	Availability of information processing facilities	•	
18 Compliance	18.1	Compliance with legal and contractual requirements	
	18.1.1	Identification of applicable legislation and contractual requirements	•
	18.1.2	Intellectual property rights	•
	18.1.3	Protection of records	•
	18.1.4	Privacy and protection of personally identifiable information	•
	18.1.5	Regulation of cryptographic controls	•
	18.2	Information security reviews	
	18.2.1	Independent review of information security	•
	18.2.2	Compliance with security policies and standards	•
	18.2.3	Technical compliance review	•