

ent as of: 2023-04-04		ractual obligations, BR/BP: business requirements/adopted best p							
ewed and Approved by Aha! Man	agement: 20	23-04-04	Applicable	lucularis autori					
	ISO/IEC	27001:2013 Annex A Controls	Applicable Y/N	Implemented Full,partial,None,N/A	Justification for exclusion	LR J	lustification CO	for Inclusion BR/BP	n R
ise	Sec 5.1	Control Objective/Control  Management direction for Information Security							
5 Security Policies	5.1.1	Policies for Information Security	Yes	Full		Х	Х	Х	
	5.1.2	Review of the policies for Information Security	Yes	Full		Х	Х	Х	
	6.1.1	Internal organization Information Security roles and responsibilities	Yes	Full			Х	Х	
	6.1.2 6.1.3	Segregation of duties Contact with authorities	Yes Yes	Full Full		Х	X X	X	
Organization of Information Security	6.1.4	Contact with special interest groups	Yes	Full		^	Х	Х	
Security	6.1.5 6.2	Information Security in project management  Mobile devices and teleworking	Yes	Full			Х	Х	
	6.2.1	Mobile device policy	Yes	Full		Х	Х	Х	
	6.2.2	Teleworking	Yes	Full			Х	Х	
	7.1 7.1.1	Prior to employment Screening	Yes	Full			Х	Х	
	7.1.2	Terms and conditions of employment	Yes	Full			X	X	
7 Human resource security	7.2 7.2.1	During employment  Management responsibilities	Yes	Full			X	х	
,	7.2.2	Information Security awareness, education and training	Yes	Full		Х	Х	Х	
	7.2.3 7.3	Disciplinary process  Termination and change of employment	Yes	Full			Х	Х	
	7.3.1	Termination or change of employment responsibilities	Yes	Full			Х	Х	
	8.1	Responsibility for assets							
	8.1.1 8.1.2	Inventory of assets Ownership of assets	Yes Yes	Full Full			X	X	
	8.1.3	Acceptable use of assets	Yes	Full			Х	Х	
	8.1.4 8.2	Return of assets Information classification	Yes	Full			Х	Х	
8 Asset management	8.2.1 8.2.2	Classification of information	Yes Yes	Full Full		Х	X X	X X	
	8.2.2	Labeling of information Handling of assets	Yes	Full		Х	X	X	
	8.3 8.3.1	Media handling  Management of removable media	Yes	Full			X	Х	
	8.3.2	Disposal of media	Yes	Full		Х	Х	Х	
	8.3.3	Physical media transfer	Yes	Full			Х	Х	
	9.1	Business requirements of access control							
	9.1.1 9.1.2	Access control policy Access to networks and network services	Yes Yes	Full Full		X	X	X	
	9.2 9.2.1	User access management User registration and de-registration	Yes	Full			Х	Х	
	9.2.2	User access provisioning	Yes	Full			Х	Х	
	9.2.3	Management of privileged access rights	Yes	Full		Х	Х	Х	
9 Access control	9.2.4	Management of secret authentication information of users	Yes	Full			х	х	
	9.2.5 9.2.6	Review of user access rights  Removal or adjustment of access rights	Yes Yes	Full Full			X	X	
	9.3	User responsibilities							
	9.3.1 9.4	Use of secret authentication information  System and application access control	Yes	Full			Х	Х	
	9.4.1 9.4.2	Information access restriction Secure log-on procedures	Yes Yes	Full Full		Х	X	X	
	9.4.3	Password management system	Yes	Full			Х	Х	
	3.4.3						Х	Х	
	9.4.4	Use of privileged utility programs  Access control to program source code	Yes Yes	Full Full			X	X	_
	9.4.4 9.4.5	Access control to program source code					Х	X	
10 Cryptography	9.4.4	Access control to program source code  Cryptographic controls				Х	X	X	
10 Cryptography	9.4.4 9.4.5	Access control to program source code	Yes	Full		х			
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls	Yes	Full Full		Х	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management	Yes	Full Full	Aha! does not maintain any	Х	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management	Yes	Full Full	physical corporate office location or facility.	Х	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas	Yes Yes Yes	Full Full	physical corporate office location or facility. Aha! does not maintain any	Х	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas	Yes Yes Yes	Full Full	physical corporate office location or facility.	X	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter	Yes Yes Yes Yes No	Full Full Full N/A	physical corporate office location or facility. Aha! does not maintain any physical corporate office location or facility. Aha! does not maintain any	X	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter	Yes Yes Yes Yes No	Full Full Full N/A	physical corporate office location or facility. Aha! does not maintain any physical corporate office location or facility. Ahal does not maintain any physical corporate office location or facility.	X	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1 11.1.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter  Physical entry controls	Yes Yes Yes No	Full Full Full N/A	physical corporate office location or facility. Ahal does not maintain any physical corporate office location or facility. Ahal does not maintain any physical corporate office location or facility. Ahal does not maintain any	X	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1 11.1.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter  Physical entry controls	Yes Yes Yes No	Full Full Full N/A	physical corporate office location or facility. Ahal does not maintain any physical corporate office location or facility. Ahal does not maintain any physical corporate office location or facility. Ahal does not maintain any physical corporate office location or facility.	x	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1 11.1.1 11.1.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities	Yes Yes Yes No No	Full Full Full N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any	X	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1 11.1.1 11.1.1	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities	Yes Yes Yes No No	Full Full Full N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.	X	х	Х	
10 Cryptography	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1 11.1.1 11.1.1 11.1.2	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats	Yes Yes Yes No No No No	Full Full N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any	х	х	Х	
	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5	Access control to program source code  Cryptographic controls Policy on the use of cryptographic controls Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats  Working in secure areas  Delivery and loading areas	Yes Yes Yes No No No No	Full Full N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.	х	х	Х	
	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1.1 11.1.2 11.1.3 11.1.4	Access control to program source code  Cryptographic controls Policy on the use of cryptographic controls Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats  Working in secure areas	Yes Yes Yes Yes No No No No No	Full Full N/A N/A N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.	X	х	Х	
Physical and environmental	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5	Access control to program source code  Cryptographic controls Policy on the use of cryptographic controls Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats  Working in secure areas  Delivery and loading areas Equipment	Yes Yes Yes Yes No No No No No No	Full Full Full N/A N/A N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office	X	х	Х	
Physical and environmental	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5	Access control to program source code  Cryptographic controls Policy on the use of cryptographic controls Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats  Working in secure areas  Delivery and loading areas	Yes Yes Yes Yes No No No No No	Full Full N/A N/A N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.	X	х	Х	
Physical and environmental	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5 11.1.6 11.2	Access control to program source code  Cryptographic controls  Policy on the use of cryptographic controls  Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats  Working in secure areas  Delivery and loading areas  Equipment  Equipment siting and protection	Yes Yes Yes Yes No	Full Full N/A N/A N/A N/A N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.	x	х	Х	
Physical and environmental	9.4.4 9.4.5 10.1 10.1.1 10.1.2 11.1.1 11.1.2 11.1.3 11.1.4 11.1.5	Access control to program source code  Cryptographic controls Policy on the use of cryptographic controls Key management  Secure areas  Physical security perimeter  Physical entry controls  Securing office, room and facilities  Protecting against external end environmental threats  Working in secure areas  Delivery and loading areas Equipment	Yes Yes Yes Yes No No No No No No	Full Full Full N/A N/A N/A N/A N/A	physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.  Ahal does not maintain any physical corporate office location or facility.	X	х	Х	

1					Aha! does not maintain any					
	11.2.4	Equipment maintenance	No	N/A	physical corporate office location or facility.					
	11.2.4	Equipment maintenance	INU	N/A	Aha! does not maintain any					
					physical corporate office					
	11.2.5	Removal of assets	No	N/A	location or facility.					
	11.2.6	Security of equipment and assets off-premises	Yes	Full		X	X	X	Х	
	11.2.7 11.2.8	Secure disposal or re-use of equipment Unattended user equipment	Yes Yes	Full Full		Х	X	X	Х	
ļ	11.2.9	Clear desk and clear screen policy	Yes	Full			X	X	X	
ļ	12.1	Operational procedures and responsibilities	V	F 11						
ļ	12.1.1 12.1.2	Documented operating procedures  Change management	Yes Yes	Full Full			Х	X	Х	
ļ	12.1.3	Capacity management	Yes	Full				Х		
	12.1.4	Separation of development, testing and operational environments	Yes	Full			Х	Х		
	12.2	Protection from malware		- "						
	12.2.1	Controls against malware  Backup	Yes	Full			Х	Х	Х	
ļ	12.3.1	Information backup	Yes	Full		Х	Х	Х		
ļ	12.4	Logging and monitoring								
12 Operations security	12.4.1	Event logging	Yes	Full			X	X	Х	
ļ	12.4.2	Protection of log information Administrator and operator logs	Yes Yes	Full Full			Х	X	Х	
	12.4.4	Clock synchronization	Yes	Full				X	_^	
	12.5	Control of operational software								
	12.5.1	Installation of software on operational systems	Yes	Full				Х		
	12.6 12.6.1	Technical vulnerability management  Management of technical vulnerabilities	Yes	Full		Х	X	х		
	12.6.2	Restrictions on software installation	Yes	Full		^	_^	X	1	
	12.7	Information systems audit considerations								
	12.7.1	Information systems audit controls	Yes	Full			Х	Х	Х	
	13.1	Network security management				Х	X	Х	Х	
ļ	13.1.1	Network controls	Yes	Full		X	X	X	X	
l	13.1.2	Security of network services	Yes	Full		Х	Х	Х	Х	
ļ	13.1.3	Segregation in networks	Yes	Full				Х	Х	
l	13.2 13.2.1	Information transfer Information transfer policies and procedures	Yes	Full		Х	X	Х		
ļ	23.2.1					^	_^	_^		
				1	Aha! does not transfer					
13 Communications security				1	information to external					
,					parties for their own use.					
					Supplier relationship					
	13.2.2	Agreements on information transfer	No	N/A	agreements cover information security and privacy.					
ļ	15.2.2	Agreements on information cransica	140	N/A	security and privacy.					
ļ			l							
	13.2.4	Electronic messaging Confidentiality or non-disclosure agreements	Yes Yes	Full Full		х	X	X	х	
	15.2.4	confidentiality of non-disclosure agreements	ies	T dil			^		^	
14 System acquisition,	14.1	Security requirements of information systems								
	14.1.1 14.1.2	Information Security requirements analysis and specification	Yes Yes	Full Full		Х	X	X	X	
	14.1.3	Securing applications services on public networks Protecting application services transactions	Yes	Full		x	X	X	X	
	14.2	Security in development and support processes								
	14.2.1	Secure development policy	Yes	Full			Х	Х	Х	
	14.2.2	System change control procedures Technical review of applications after operating platform changes	Yes Yes	Full Full			X	X	Х	
	14.2.4	Restrictions on changes to software packages	Yes					^		
				IFUII			Х	Х	1 X	
	14.2.5	Secure system engineering principles	Yes	Full Full		Х	X X	X	Х	
						х			X	
development and maintenance	14.2.5 14.2.6	Secure system engineering principles Secure development environment	Yes Yes	Full Full	Aha! does not outsource	х	Х	Х	X	
development and maintenance	14.2.5 14.2.6 14.2.7	Secure system engineering principles Secure development environment Outsourced development	Yes Yes No	Full Full N/A	Aha! does not outsource software development.	х	X	X		
development and maintenance	14.2.5 14.2.6	Secure system engineering principles Secure development environment	Yes Yes	Full Full		Х	Х	Х	X	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8	Secure system engineering principles Secure development environment Outsourced development System security testing	Yes Yes No Yes	Full Full N/A Full		Х	X	X		
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9	Secure system engineering principles Secure development environment  Outsourced development System security testing System acceptance testing	Yes Yes No Yes	Full Full N/A Full	software development.  No customer data from	Х	X	X		
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9	Secure system engineering principles Secure development environment  Outsourced development System security testing System acceptance testing	Yes Yes No Yes	Full Full N/A Full	software development.  No customer data from production systems is used for	Х	X	X		
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9	Secure system engineering principles Secure development environment  Outsourced development System security testing System acceptance testing	Yes Yes No Yes	Full Full N/A Full	software development.  No customer data from	Х	X	X		
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3	Secure system engineering principles Secure development environment  Outsourced development System security testing System acceptance testing Test data  Protection of test data	Yes Yes No Yes Yes	Full Full N/A Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	х	X X X	X		
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships	Yes Yes No Yes Yes Yes	Full N/A Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT		X X X	X X X	х	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships	Yes Yes No Yes Yes Yes Yes	Full N/A Full Full Partial Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	х	X X X	X X X		
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships	Yes Yes No Yes Yes Yes	Full N/A Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT		X X X	X X X	х	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.2 15.1.3 15.2	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information and communication technology supply chain Supplier service delivery management	Yes Yes No Yes Yes Yes Yes Yes Yes Yes Yes	Full Full Partial  Full Full Full Full Full Full Full F	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X	X X X X	X	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.3 15.2.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security policy for supplier relationships Information Security policy for supplier relationships Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services	Yes Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes	Full  Partial  Pull  Partial  Full  Full  Full  Full  Full  Full  Full  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X	X X X X X	X X X X X X	х	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.2 15.1.3 15.2	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information and communication technology supply chain Supplier service delivery management	Yes Yes No Yes Yes Yes Yes Yes Yes Yes Yes	Full Full Partial  Full Full Full Full Full Full Full F	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X	X X X X	X	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 15.1 15.1.1 15.1.2 15.1.3 15.2 15.2.1 15.2.2	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data Test data Information Security in supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services	Yes Yes No Yes Yes Yes Yes Yes Yes Yes Yes Yes	Full  Partial  Pull  Partial  Full  Full  Full  Full  Full  Full  Full  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X	X X X X X X	X	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.2 15.2.1 15.2.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security within supplier relationships Information Security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements	Yes	Full Full Partial  Full Full Full Full Full Full Full F	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X	X X X X X X X	x x	
development and maintenance	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3 15.1.1 15.1.1 15.1.2 15.1.2 15.2.1 15.2.1 15.2.1 16.1 16.1.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Addressing security within supplier areationships Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security incidents and improvements Responsibilities and procedures	Yes	Full  Partial  Prull  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X	X X X X X X X X X X X X X	X	
development and maintenance  15 Supplier relationships  16 Information Security incident	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.2 15.2.1 15.2.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security within supplier relationships Information Security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements	Yes	Full Full Partial  Full Full Full Full Full Full Full F	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X	X X X X X X X	x x	
development and maintenance  15 Supplier relationships  16 Information Security incident	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.1 15.2.2 16.1 16.1.1 16.1.2 16.1.3	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security in supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Management of Information Security incidents and improvements Responsibilities and procedures Reporting Information Security vecations Reporting Information Security weaknesses Resporsing Information Security weeknesses Respossment of and decision on Information Security events	Yes  No  No  Yes  Yes  Yes  Yes  Yes  Yes  Yes  Ye	Full  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	x x	
development and maintenance  15 Supplier relationships  16 Information Security incident	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 15.1 15.1.1 15.1.2 15.1.3 15.2 16.1 16.1.1 16.1.2 16.1.1 16.1.1	Secure system engineering principles Secure development environment Outsourced development System security testing System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information Security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security incidents and improvements Responsibilities and procedures Reporting Information Security weekts Reporting Information Security weekts Reporting Information Security weekts Responses to Information Security weents Responses to Information Security incidents	Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	x x	
development and maintenance  15 Supplier relationships  16 Information Security incident	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.2 15.1.2 16.1.1 16.1.1 16.1.2 16.1.4 16.1.5	Secure yestem engineering principles Secure development environment Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Addressing security within supplier arelationships Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security weaknesses Assessment of and decision on Information Security events Response to Information Security events Response to Information Security events Response to Information Security incidents	Yes No No Yes	Full  Partial  Partial  Full  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	x x x x	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X	
development and maintenance  15 Supplier relationships  16 Information Security incident	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 15.1 15.1.1 15.1.2 15.1.3 15.2 16.1 16.1.1 16.1.2 16.1.1 16.1.1	Secure system engineering principles Secure development environment Outsourced development System security testing System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information Security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security incidents and improvements Responsibilities and procedures Reporting Information Security weekts Reporting Information Security weekts Reporting Information Security weekts Responses to Information Security weents Responses to Information Security incidents	Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	x x	
development and maintenance  15 Supplier relationships  16 Information Security incident	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.1 15.1.2 16.1.1 16.1.2 16.1.3 16.1.3 16.1.4 16.1.5 16.1.7	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security incidents and improvements Responsibilities and procedures Reporting information Security wents Reporting information Security weaknesses Assessment of and decision on Information Security tweathers Response to Information Security incidents Learning from Information Security Incidents	Yes  No  No  Yes  Yes  Yes  Yes  Yes  Yes  Yes  Ye	Full  Partial  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	X X X	
15 Supplier relationships  16 Information Security incident management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.2 15.1.2 15.1.2 15.2 16.1 16.1.3 16.1.4 16.1.6 16.1.6 16.1.7	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements Responsibilities and procedures Reporting information Security events Reporting information Security weaknesses Assessment of and decision on Information Security events Response to Information Security incidents Learning from Information Security incidents Collection of evidence	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	x x x x	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	X X X	
development and maintenance  15 Supplier relationships  16 Information Security incident management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.2 15.1.2 16.1.1 16.1.2 16.1.1 16.1.5 16.1.7 17.1 17.1.1	Secure yestem engineering principles Secure development environment Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Addressing security within supplier relationships Addressing security within supplier agreements Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security vincidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security events Response to information Security incidents Learning from Information Security incidents Collection of evidence Information Security incidents Collection of security continuity Planning Information Security continuity Implementing Information Security continuity	Yes No No Yes	Full  Full  Partial  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	X	
development and maintenance  15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3.1 15.1.1 15.1.1 15.1.2 15.1.1 15.1.2 15.2.1 15.2.1 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.6 16.1.6 17.1 17.1.1 17.1.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security weaknesses Assessment of and decision on Information Security events Response to Information Security incidents Learning from Information Security incidents Collection of evidence Information Security continuity Planning Information Security continuity Implementing Information Security continuity Verify, review and evaluate Information Security continuity	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	X X X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.2 15.1.2 16.1.1 16.1.2 16.1.1 16.1.5 16.1.7 17.1 17.1.1	Secure yestem engineering principles Secure development environment Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Addressing security within supplier relationships Addressing security within supplier agreements Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security vincidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security events Response to information Security incidents Learning from Information Security incidents Collection of evidence Information Security incidents Collection of security continuity Planning Information Security continuity Implementing Information Security continuity	Yes No No Yes	Full  Full  Partial  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.2 15.1.2 16.1.1 16.1.3 16.1.4 16.1.5 16.1.6 17.1 17.1.1 17.1.2 17.1.2 17.1.2 17.1.2 17.1.3	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Information Security policy for supplier actionships Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security events Response to Information Security incidents Learning from Information Security continuity Inplementing Information Security continuity Implementing Information Security continuity Redundancies Availability of information processing facilities	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	X X X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.1 15.1.2 15.1.3 15.2 16.1.1 16.1.2 16.1.1 16.1.5 16.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.2.1	Secure yestem engineering principles  Secure development environment  Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services  Managing changes to supplier services  Management of information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security events Response to Information Security weaknesses Assessment of and decision on Information Security events Response to Information Security incidents Calerning from Information Security incidents Collection of evidence Information Security continuity Planning Information Security continuity Verify, review and evaluate Information Security continuity Compliance with legal and contractual requirements	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X	
15 Supplier relationships  16 Information Security incident management  7 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.7 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.2.1 15.2.2 15.2.1 16.1.1 16.1.2 16.1.3 16.1.3 16.1.4 16.1.5 16.1.6 16.1.7 17.1.1 17.1.1 17.1.1 17.1.2 17.1.1 17.1.1 17.1.2 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 18.1	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security weaknesses Assessment of and decision on Information Security events Response to Information Security incidents Learning from Information Security incidents Collection of evidence Information Security continuity Planning Information Security continuity Planning Information Security continuity Verif, review and evaluate Information Security continuity Redundancies Availability of information processing facilities Compliance with legal and contractual requirements Identification of applicable legislation and contractual requirements	Yes  No No Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes	Full  Full  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	x x x x x x x x x x x x x x x x x x x	x	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.1 15.1.2 15.1.3 15.2 16.1.1 16.1.2 16.1.1 16.1.5 16.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.2.1	Secure yestem engineering principles  Secure development environment  Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services  Managing changes to supplier services  Management of information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security events Response to Information Security weaknesses Assessment of and decision on Information Security events Response to Information Security incidents Calerning from Information Security incidents Collection of evidence Information Security continuity Planning Information Security continuity Verify, review and evaluate Information Security continuity Compliance with legal and contractual requirements	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.2 15.1.2 15.1.3 15.2.1 16.1.1 16.1.5 16.1.6 16.1.7 17.1 17.1.2 17.1.1 17.1.2 17.1.2 17.2.1 18.1.1 18.1.1 18.1.1 18.1.2 18.1.3	Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing Test data  Protection of test data Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Information Security managements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of Information Security incidents and improvements Responsibilities and procedures Reporting Information Security events Reporting Information Security events Reporting Information Security events Learning from Information Security incidents Learning from Information Security continuity Implementing Information Security continuity Implementing Information Security continuity Redundancies Availability of information processing facilities Compliance with legal and contractual requirements Intellectual property rights Protection of records	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.1 15.1.2 15.1.2 16.1.1 16.1.2 16.1.1 16.1.2 16.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 18.1.1 18.1.1 18.1.1 18.1.1 18.1.1 18.1.1	Secure system engineering principles  Secure development environment  Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security within supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services  Managing changes to supplier services  Management of information Security incidents and improvements Responsibilities and procedures Reporting information Security events Reporting information Security events Resporting information Security weaknesses Assessment of and decision on information security events Learning from information Security incidents Collection of evidence  Information Security continuity Implementing information Security continuity Verify, review and evaluate Information Security continuity Implementing Information processing facilities  Compliance with legal and contractual requirements Intellectual property rights Protection of records Privacy and protection of personally identifiable information	Yes  No No Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes	Full  Partial  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.7 14.2.9 14.3 14.3.1 15.1.1 15.1.1 15.1.1 15.1.2 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5 16.1.7 17.1.1 17.1.1 17.1.1 17.1.1 17.1.2 17.1.3 17.2 17.1.3 18.1.1 18.1.1 18.1.2 18.1.1 18.1.1 18.1.1 18.1.5	Secure yestem engineering principles Secured development environment Outsourced development System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Information Security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services Managing changes to supplier services Management of information Security incidents and improvements Responsibilities and procedures Reporting information Security events Response to Information Security weaknesses Assessment of and decision on Information Security events Response to Information Security incidents Learning from Information Security incidents Learning from Information Security incidents Collection of evidence Information Security continuity Planning Information Security continuity Verify, review and evaluate Information Security continuity Verify, review and evaluate Information Security continuity Redundancies Availability of information processing facilities Compliance with legal and contractual requirements Intellectual property rights Protection of records Privacy and protection of personally identifiable information Regulation of cryptographic controls Information Security reviews	Yes  No No Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes	Full  Full  Partial  Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	
15 Supplier relationships  16 Information Security incident management  17 Information Security aspects of business continuity management	14.2.5 14.2.6 14.2.7 14.2.8 14.2.9 14.3 14.3.1 15.1 15.1.1 15.1.1 15.1.2 15.1.2 16.1.1 16.1.2 16.1.1 16.1.2 16.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 17.1.1 18.1.1 18.1.1 18.1.1 18.1.1 18.1.1 18.1.1	Secure system engineering principles  Secure development environment  Outsourced development System security testing System security testing System acceptance testing Test data  Information Security in supplier relationships Information Security policy for supplier relationships Information Security within supplier relationships Addressing security within supplier agreements Information and communication technology supply chain Supplier service delivery management Monitoring and review of supplier services  Managing changes to supplier services  Management of information Security incidents and improvements Responsibilities and procedures Reporting information Security events Reporting information Security events Resporting information Security weaknesses Assessment of and decision on information security events Learning from information Security incidents Collection of evidence  Information Security continuity Implementing information Security continuity Verify, review and evaluate Information Security continuity Implementing Information processing facilities  Compliance with legal and contractual requirements Intellectual property rights Protection of records Privacy and protection of personally identifiable information	Yes No No Yes	Full Full Full Full Full Full Full Full	software development.  No customer data from production systems is used for testing. The test data does NOT	X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	X X X X X X X X X X X X X X X X X X X	