British Assessment Bureau

Certification is conditional on maintaining the required performance standards throughout the certified period of registration
The British Assessment Bureau, 30 Tower View, Kings Hill, Kent, ME19 4UY

The management system of Certificate Number **231351**

Calastone Ltd

20 Birchin Lane, London, EC3V 9DU

has been assessed and certified as meeting the requirements of

ISO 27001:2013

for the following activities

Provision of trading support solutions encompassing Money Market Services, DMI Fund Services, Order Routing & Settlements, Transfers, Dividends and Reporting to clients worldwide.

This is in accordance with the Statement of Applicability **V1.5 dated 24/04/2023** .

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

UKAS MANAGEMENT SYSTEMS
8289

Valid from
Initial Certification: 07 August 2020
Latest Issue: 24 July 2023
Expiry Date: 31 October 2025
subject to annual assessments

Authorised by

Mike Tims
Chief Executive Officer

www.british-assessment.co.uk

Certificate issued by Amtivo Group Limited, trading as British Assessment Bureau

The validity and status of this certificate can be verified by using the UKAS CertCheck website at certcheck.ukas.com

Calastone ISO27001 - Statement of Applicability (SoA)

Version 1.5 (24/04/2023)

Section	Controls	Applicability	Implemented	Why Implemeneted	Document / Policy
Information Security Policies - A5	5.1 Information Security Policy	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A5 - Information Security Policies
	5.1.1 Policies for information security	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A5 - Information Security Policies
	5.1.2 Review of the policies for information security.	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A5 - Information Security Policies
Organization of Information security Policy - A6	6.1 Internal Organization	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.1.1 Information security roles and responsibilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.1.2 Segregation of duties	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.1.3 Contact with authorities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.1.4 Contact with special interest groups	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.1.5 Information security in project management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.2 Mobile devices and teleworking	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.2.1 Mobile device policy	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
	6.2.2 Teleworking	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A6 - Organization of Information security Policy
Human Resource Security Policy - A7	7.1 Prior to employment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.1.1 Screening	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.1.2 Terms and conditions of employment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.2 During employment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.2.1 Management responsibilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.2.2 Information security awareness, education and training	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.2.3 Disciplinary process	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.3 Termination and change of employment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
	7.3.1 Termination or change of employment responsibilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A7 - Human Resource Security Policy
Asset Management Policy - A8	8.1 Responsibility for assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.1.1 Inventory of assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.1.2 Ownership of assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.1.3 Acceptable use of assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.1.4 Return of assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.2 Information classification	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.2.1 Classification of information	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.2.2 Labelling of information	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.2.3 Handling of assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.3 Media handling	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.3.1 Management of removable media	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.3.2 Disposal of media	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
	8.3.3 Physical media transfer	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A8 - Asset Management Policy
Access Control Policy - A9	9.1 Business requirements of access control	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.1.1 Access control policy	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.1.2 Access to networks and network services	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2 User access management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2.1 User registration and de-registration	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2.2 User access provisioning	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2.3 Management of privileged access rights	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2.4 Management of secret authentication information of users	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2.5 Review of user access rights	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.2.6 Removal or adjustment of access rights	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.3 User responsibilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.3.1 Use of secret authentication	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.4 System and application access control	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.4.1 Information access restriction	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.4.2 Secure log-on procedures	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.4.3 Password management system	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.4.4 Use of privileged utility programs	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
	9.4.5 Access control to program source code	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A9 - Access Control Policy
Cryptography Policy - A10	10.1 Cryptographic controls	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A10 - Cryptography Policy
	10.1.1 Policy on the use of cryptographic controls	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A10 - Cryptography Policy
	10.1.2 Key management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A10 - Cryptography Policy
Physical and environmental security - A11	11.1 Secure areas	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.1.1 Physical security perimeter	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.1.2 Physical entry controls	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.1.3 Securing offices, rooms and facilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.1.4 Protecting against external and environmental threats	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.1.5 Working in secure areas	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.1.6 Delivery and loading areas	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2 Equipment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.1 Equipment siting and protection	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.2 Supporting utilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.3 Cabling security	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.4 Equipment maintenance	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.5 Removal of assets	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.6 Security of equipment and assets off-premises	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.7 Secure disposal or reuse of equipment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.8 Unattended user equipment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
	11.2.9 Clear desk and clear screen policy	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A11 - Physical and environmental security
Operations Security Policy - A12	12.1 Operational procedures and responsibilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.1.1 Documented operating procedures	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.1.2 Change management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.1.3 Capacity management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.1.4 Separation of development, testing and operational environments	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.2 Protection from malware	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.2.1 Controls against malware	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.3 Backup	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.3.1 Information backup	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.4 Logging and monitoring	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.4.1 Event logging	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.4.2 Protection of log information	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.4.3 Administrator and operator logs	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.4.4 Clock synchronisation	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.5 Control of operational software	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.5.1 Installation of software on operational systems	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.6 Technical Vulnerability Management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.6.1 Management of technical vulnerabilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy

	12.6.2 Restrictions on software installation	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.7 Information systems audit considerations	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
	12.7.1 Information systems audit controls	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A12 - Operations Security Policy
Communications Security Policy - A13	13.1 Network security management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.1.1 Network controls	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.1.2 Security of network services	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.1.3 Segregation in networks	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.2 Information transfer	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.2.1 Information transfer policies and procedures	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.2.2 Agreements on information transfer	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.2.3 Electronic messaging	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
	13.2.4 Confidentiality or nondisclosure agreements	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A13 - Communications Security Policy
System acquisition, development and maintenance Policy - A14	14.1 Security requirements of information systems	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.1.1 Information security requirements analysis and specification	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.1.2 Securing application services on public networks	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.1.3 Protecting application services transactions	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2 Security in development and support processes	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.1 Secure development policy	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.2 System change control procedures	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.3 Technical review of applications after operating platform changes	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.4 Restrictions on changes to software packages	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.5 Secure system engineering principles	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.6 Secure development environment	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.7 Outsourced development	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.8 System security testing	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.2.9 System acceptance testing	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.3 Test data	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
	14.3.1 Protection of test data	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A14 - System acquisition, development and maintenance Policy
Supplier relationships Policy - A15	15.1 Information security in supplier relationships	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
	15.1.1 Information security policy for supplier relationships	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
	15.1.2 Addressing security within supplier agreements	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
	15.1.3 Information and communication technology supply chain	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
	15.2 Supplier service delivery management	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
	15.2.1 Monitoring and review of supplier services	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
	15.2.2 Managing changes to supplier services	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A15 - Supplier relationships Policy
Information security incident management Policy - A16	16.1 Management of information security incidents and improvements	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.1 Responsibilities and procedures	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.2 Reporting information security events	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.3 Reporting information security weaknesses	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.4 Assessment of and decision on information security events	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.5 Response to information security incidents	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.6 Learning from information security incidents	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
	16.1.7 Collection of evidence	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A16 - Information security incident management Policy
Information security aspects of business continuity management	17.1 Information security continuity	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A17 - information security aspects of business continuity management Policy
	17.1.1 Planning information security continuity	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A17 - information security aspects of business continuity management Policy
	17.1.2 Implementing information security continuity	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A17 - information security aspects of business continuity management Policy
	17.1.3 Verify, review and evaluate information security continuity	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A17 - information security aspects of business continuity management Policy
	17.2 Redundancies	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A17 - information security aspects of business continuity management Policy
	17.2.1 Availability of information processing facilities	In Scope	Fully Implemented	Information Security Best Practice / Contractual Requirement (Client)	A17 - information security aspects of business continuity management Policy
Compliance Policy - A18	18.1 Compliance with legal and contractual requirements	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.1.1 Identification of applicable legislation and contractual requirements	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.1.2 Intellectual property rights	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.1.3 Protection of records	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.1.4 Privacy and protection of personally identifiable information	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.1.5 Regulation of cryptographic controls	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.2 Information security reviews	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.2.1 Independent review of information security	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.2.2 Compliance with security policies and standards	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy
	18.2.3 Technical compliance review	In Scope	Fully Implemented	Information Security Best Practice / Legal Requirement / Contractual Requirement (Client)	A18 - Compliance Policy