CC&G INFORMATION SECURITY CONTROLS

ISO/IEC 27001:2013 Statement of Applicability

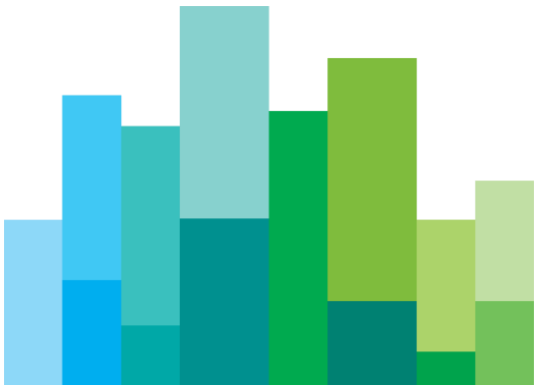
April 2021

CC&G
A EURONEXT COMPANY

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 3
2. ISO/IEC 27001:2013 STATEMENT OF APPLICABILITY 5

1. EXECUTIVE SUMMARY

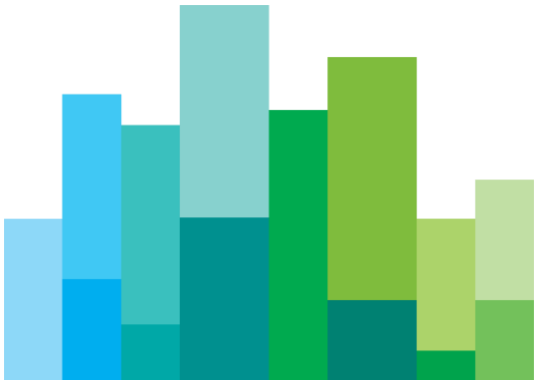


CC&G operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope: The Information Security Management System for regulated processes supporting CC&G's institutional activities, with a specific focus on CCP and Risk Management services.

This document details the Information Security controls that are applicable / not applicable to CC&G, as per Annex A of ISO/IEC 27001:2013. The document is called Statement of Applicability (SoA).

The SoA is reported in **Section** Error! Reference source not found..

2. ISO/IEC 27001:2013 STATEMENT OF APPLICABILITY



Please refer to Annex A of ISO/IEC 27001:2013 for the description of controls and to ISO/IEC 27002:2013 for the application of controls.

#	Controls listed in ISO 27001:2013 Annex A	Applicability
A.5 Information security policies		
A.5.1.1	Policies for information security	Applicable
A.5.1.2	Review of the policies for information security	Applicable
A.6 Organization of information security		
A.6.1.1	Information security roles and responsibilities	Applicable
A.6.1.2	Segregation of duties	Applicable
A.6.1.3	Contact with authorities	Applicable
A.6.1.4	Contact with special interest groups	Applicable
A.6.1.5	Information security in project management	Applicable
A.6.2.1	Mobile device policy	Applicable
A.6.2.2	Teleworking	Applicable
A.7 Human resource security		
A.7.1.1	Screening	Applicable
A.7.1.2	Terms and conditions of employment	Applicable
A.7.2.1	Management responsibilities	Applicable
A.7.2.2	Information security awareness, education and training	Applicable
A.7.2.3	Disciplinary process	Applicable
A.7.3.1	Termination or change of employment responsibilities	Applicable
A.8 Asset management		
A.8.1.1	Inventory of assets	Applicable
A.8.1.2	Ownership of assets	Applicable
A.8.1.3	Acceptable use of assets	Applicable
A.8.1.4	Return of assets	Applicable
A.8.2.1	Classification of information	Applicable
A.8.2.2	Labelling of information	Applicable
A.8.2.3	Handling of assets	Applicable
A.8.3.1	Management of removable media	Applicable
A.8.3.2	Disposal of media	Applicable
A.8.3.3	Physical media transfer	Applicable
A.9 Access control		
A.9.1.1	Access control policy	Applicable
A.9.1.2	Access to networks and network services	Applicable

#	Controls listed in ISO 27001:2013 Annex A	Applicability
A.9.2.1	User registration and de-registration	Applicable
A.9.2.2	User access provisioning	Applicable
A.9.2.3	Management of privileged access rights	Applicable
A.9.2.4	Management of secret authentication information of users	Applicable
A.9.2.5	Review of user access rights	Applicable
A.9.2.6	Removal or adjustment of access rights	Applicable
A.9.3.1	Use of secret authentication information	Applicable
A.9.4.1	Information access restriction	Applicable
A.9.4.2	Secure log-on procedures	Applicable
A.9.4.3	Password management system	Applicable
A.9.4.4	Use of privileged utility programs	Applicable
A.9.4.5	Access control to program source code	Applicable
A.10 Cryptography		
A.10.1.1	Policy on the use of cryptographic controls	Applicable
A.10.1.2	Key management	Applicable
A.11 Physical and environmental security		
A.11.1.1	Physical security perimeter	Applicable
A.11.1.2	Physical entry controls	Applicable
A.11.1.3	Securing offices, rooms and facilities	Applicable
A.11.1.4	Protecting against external and environmental threats	Applicable
A.11.1.5	Working in secure areas	Applicable
A.11.1.6	Delivery and loading areas	Applicable
A.11.2.1	Equipment siting and protection	Applicable
A.11.2.2	Supporting utilities	Applicable
A.11.2.3	Cabling security	Applicable
A.11.2.4	Equipment maintenance	Applicable
A.11.2.5	Removal of assets	Applicable
A.11.2.6	Security of equipment and assets off-premises	Applicable
A.11.2.7	Secure disposal or re-use of equipment	Applicable
A.11.2.8	Unattended user equipment	Applicable
A.11.2.9	Clear desk and clear screen policy	Applicable
A.12 Operations security		
A.12.1.1	Documented operating procedures	Applicable
A.12.1.2	Change management	Applicable

#	Controls listed in ISO 27001:2013 Annex A	Applicability
A.12.1.3	Capacity management	Applicable
A.12.1.4	Separation of development, testing and operational environments	Applicable
A.12.2.1	Controls against malware	Applicable
A.12.3.1	Information backup	Applicable
A.12.4.1	Event logging	Applicable
A.12.4.2	Protection of log information	Applicable
A.12.4.3	Administrator and operator logs	Applicable
A.12.4.4	Clock synchronisation	Applicable
A.12.5.1	Installation of software on operational systems	Applicable
A.12.6.1	Management of technical vulnerabilities	Applicable
A.12.6.2	Restrictions on software installation	Applicable
A.12.7.1	Information systems audit controls	Applicable
A.13 Communications security		
A.13.1.1	Network controls	Applicable
A.13.1.2	Security of network services	Applicable
A.13.1.3	Segregation in networks	Applicable
A.13.2.1	Information transfer policies and procedures	Applicable
A.13.2.2	Agreements on information transfer	Applicable
A.13.2.3	Electronic messaging	Applicable
A.13.2.4	Confidentiality or non-disclosure agreements	Applicable
A.14 System acquisition, development and maintenance		
A.14.1.1	Information Security requirements analysis and specification	Applicable
A.14.1.2	Securing application services on public networks	Applicable
A.14.1.3	Protecting application services transactions	Applicable
A.14.2.1	Secure development policy	Applicable
A.14.2.2	System change control procedures	Applicable
A.14.2.3	Technical review of applications after operating platform changes	Applicable
A.14.2.4	Restrictions on changes to software packages	Applicable
A.14.2.5	Secure system engineering principles	Applicable
A.14.2.6	Secure development environment	Applicable
A.14.2.7	Outsourced development	Not applicable
A.14.2.8	System security testing	Applicable
A.14.2.9	System acceptance testing	Applicable
A.14.3.1	Protection of test data	Applicable

#	Controls listed in ISO 27001:2013 Annex A	Applicability
A.15 Supplier relationships		
A.15.1.1	Information security policy for supplier relationships	Applicable
A.15.1.2	Addressing security within supplier agreements	Applicable
A.15.1.3	Information and communication technology supply chain	Applicable
A.15.2.1	Monitoring and review of supplier services	Applicable
A.15.2.2	Managing changes to supplier services	Applicable
A.16 Information security incident management		
A.16.1.1	Responsibilities and procedures	Applicable
A.16.1.2	Reporting information security events	Applicable
A.16.1.3	Reporting information security weaknesses	Applicable
A.16.1.4	Assessment of and decision on information security events	Applicable
A.16.1.5	Response to information security incidents	Applicable
A.16.1.6	Learning from information security incidents	Applicable
A.16.1.7	Collection of evidence	Applicable
A.17 Information security aspects of business continuity management		
A.17.1.1	Planning information security continuity	Applicable
A.17.1.2	Implementing information security continuity	Applicable
A.17.1.3	Verify, review and evaluate information security continuity	Applicable
A.17.2.1	Availability of information processing facilities	Applicable
A.18 Compliance		
A.18.1.1	Identification of applicable legislation and contractual requirements	Applicable
A.18.1.2	Intellectual property rights	Applicable
A.18.1.3	Protection of records	Applicable
A.18.1.4	Privacy and protection of personally identifiable information	Applicable
A.18.1.5	Regulation of cryptographic controls	Applicable
A.18.2.1	Independent review of information security	Applicable
A.18.2.2	Compliance with security policies and standards	Applicable
A.18.2.3	Technical compliance review	Applicable

Disclaimer

This publication is for information purposes only and is not a recommendation to engage in investment activities. This publication is provided "as is" without representation or warranty of any kind. Whilst all reasonable care has been taken to ensure the accuracy of the content, CC&G does not guarantee its accuracy or completeness. CC&G will not be held liable for any loss or damages of any nature ensuing from using, trusting or acting on information provided. No information set out or referred to in this publication shall form the basis of any contract. The creation of rights and obligations in respect of services provided by CC&G shall depend solely on the applicable rules and /or contractual provisions of CC&G. All proprietary rights and interest in or connected with this publication shall vest in CC&G. No part of it may be redistributed or reproduced in any form without the prior written permission of CC&G. CC&G disclaims any duty to update this information. Unauthorised use of the trademarks and intellectual properties owned by the Company or other Companies belonging to Euronext Group is strictly prohibited and may violate trademark, copyright or other applicable laws.

CC&G

A EURONEXT COMPANY

www.ccg.it