Key: Legal requirements (LR). Contractual obligations (C). Business requirements/adopted best practices (BR/BP). Risk assessed (RA).

STATEMENT OF APPLICABILITY

Document Classification:	**Public**
Document Name:	**Statement of Applicability**
Document approved by	**CRO**

Date	**Version**	**Purpose of revision**
November 2024	9	Alignment to ISO 27001-2022 standard

The purpose of the Statement of Applicability is to detail which controls are relevant to managing EBA CLEARING's information security risk.

Control Name	**Control ID**	**Control Description**	**LR**	**CO**	**BR/BP**	**RA**	**Applicable** [Yes/No?]	**Implemented** [Yes/No?]
A.5 Organisational Controls								
Information Security Policies	**A5**						Yes	Yes
Policies for Information Security	A.5.1	*Control:* Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.			X	Yes	Yes	Yes
Information security roles & responsibilities	A.5.2	*Control* : Information security roles and responsibilities should be defined and allocated according to the organization needs.			X	Yes	Yes	Yes
Segregation of Duties	A.5.3	*Control:* Conflicting duties and conflicting areas of responsibility should be segregated.			X	Yes	Yes	Yes
Management Responsibilities	A.5.4	*Control:* Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization			X	Yes	Yes	Yes
Contact with Authorities	A5.5	*Control:* The organization should establish and maintain contact with relevant authorities.	X	X	X	Yes	Yes	Yes
Contact with special interest groups	A5.6	*Control:* The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	X	X	X	Yes	Yes	Yes
Threat Intel	A5.7	*Control:* Information relating to information security threats should be collected and analysed to produce threat intelligence.		X	X	Yes	Yes	Yes
Information security in project mgmt.	A5.8	*Control:* Information security should be integrated into project management.			X	Yes	Yes	Yes

Inventory of information & other associated assets	A5.9	*Control:* An inventory of information and other associated assets, including owners, should be developed and *maintained.*			X	Yes	Yes	Yes
Acceptable use of information & other associated assets (online collaboration & electronic messaging & Logging and Monitoring)	A5.10	*Control:* Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented		X	X	Yes	Yes	Yes
Return of Assets	A5.11	*Control:* Employees & external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.			X	Yes	Yes	Yes
Classification of Information	A5.12	*Control:* Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.			X	Yes	Yes	Yes
Labelling of Information	A5.13	*Control:* An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.			X	Yes	Yes	Yes
Information Transfer	A5.14	*Control:* Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.		X	X	Yes	Yes	Yes
Access Control	A5.15	*Control:* Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements			X	Yes	Yes	Yes
Identity Management	A5.16	*Control:* Formal user registration and de-registration process shall be implemented to enable assignment of access rights.			X	Yes	Yes	Yes
Authentication Information	A5.17	*Control:* Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information			X	Yes	Yes	Yes
Access Rights	A5.18	*Control:* Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization’s topic-specific policy on and rules for access control.			X	Yes	Yes	Yes
Information security policy in supplier relationships	A5.19	*Control:* Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier’s products or services.		X	X	Yes	Yes	Yes
Addressing security within supplier agreements	A5.20	*Control:* Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.		X	X	Yes	Yes	Yes
Managing Information Security in ICT Supply Chain	A5.21	*Control:* Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.		X	X	Yes	Yes	Yes

Monitoring, Review & Change Management of Supplier Services	A5.22	*Control:* The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	X	X	X	Yes	Yes	Yes
Information security for use of Cloud services	A5.23	*Control:* Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements	X	X	X	Yes	Yes	Yes
Information security incident management planning & preparation	A5.24	*Control:* The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities			X	Yes	Yes	Yes
Assessment & decision on information security events	A5.25	*Control:* The organization should assess information security events and decide if they are to be categorized as information security incidents			X	Yes	Yes	Yes
Response to information security incidents	A5.26	*Control:* Information security incidents should be responded to in accordance with the documented procedures			X	Yes	Yes	Yes
Learning from information security incidents	A5.27	*Control:* Knowledge gained from information security incidents should be used to strengthen and improve the information security controls			X	Yes	Yes	Yes
Collection of Evidence	A5.28	*Control:* The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.			X	Yes	Yes	Yes
Information Security during disruption	A5.29	*Control:* The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.			X	Yes	Yes	Yes
ICT Readiness for Business Continuity	A5.30	*Control:* ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.			X	Yes	Yes	Yes
Legal, statutory, regulatory, & contractual requirements	A5.31	*Control:* Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	X	X	X	Yes	Yes	Yes
Intellectual Property Rights	A5.32	*Control:* The organization should implement appropriate procedures to protect intellectual property rights.	X	X	X	Yes	Yes	Yes
Protection of records	A5.33	*Control:* Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorised release.			X	Yes	Yes	Yes
Privacy and protection of personally identifiable information (PII)	A5.34	*Control:* Privacy & protection of personally identifiable information shall be ensured as required in relevant legislation & regulation where applicable	X	X	X	Yes	Yes	Yes
Independent Review of Information Security	A5.35	*Control:* The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur		X	X	Yes	Yes	Yes

Compliance With Policies, Rules & Standards for Information Security	A5.36	*Control:* Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed			X	Yes	Yes	Yes
Documented Operating Procedures	A5.37	*Control:* Operating procedures shall be documented and made available to all users who need them			X	Yes	Yes	Yes
A.6 Peoples Controls								
Screening	A6.1	*Control:* Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	X	X	X	Yes	Yes	Yes
Terms and Conditions of Employment	A6.2	*Control:* The employment contractual agreements should state the personnel's and the organization's responsibilities for information security		X	X	Yes	Yes	Yes
Information Security Awareness, Education & Training	A6.3	*Control:* Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.		X	X	Yes	Yes	Yes
Disciplinary Process	A6.4	*Control:* A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.		X	X	Yes	Yes	Yes
Responsibilities After Termination or Change of Employment	A6.5	*Control:* Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.		X	X	Yes	Yes	Yes
Confidentiality or Non Disclosure Agreements	A6.6	*Control:* Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties		X	X	Yes	Yes	Yes
Remote Working	A6.7	*Control:* Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises			X	Yes	Yes	Yes
Information Security Event Reporting	A6.8	*Control:* The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner	X		X	Yes	Yes	Yes
A.7 Physical Controls								

Physical Security Perimeters	A7.1	*Control:* Security perimeters should be defined and used to protect areas that contain information and other associated assets.			X	Yes	Yes	Yes
Physical Entry	A7.2	*Control:* Secure areas should be protected by appropriate entry controls and access points.			X	Yes	Yes	Yes
Securing offices, rooms and facilities	A7.3	*Control:* Physical security for offices, rooms and facilities should be designed and implemented			X	Yes	Yes	Yes
Physical Security Monitoring	A7.4	*Control:* Premises should be continuously monitored for unauthorized physical access.		X	X	Yes	Yes	Yes
Protecting against External and Environmental Threats	A7.5	*Control:* Physical protection against natural disasters, malicious attack or accidents shall be designed and applied			X	Yes	Yes	Yes
Working in Secure Areas	A7.6	*Control:* Security measures for working in secure areas should be designed and implemented.			X	Yes	Yes	Yes
Clean Desk and Screen Policy	A7.7	*Control:* Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.			X	Yes	Yes	Yes
Equipment Siting and Protection	A7.8	*Control:* Equipment should be sited securely and protected.			X	Yes	Yes	Yes
Security of Assets Off Premises	A7.9	*Control:* Off-site assets should be protected.			X	Yes	Yes	Yes
Storage Media	A7.10	*Control:* Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.			X	Yes	Yes	Yes
Supporting Utilities	A7.11	*Control:* Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.			X	Yes	Yes	Yes
Cabling Security	A7.12	*Control:* Cables carrying power, data or supporting information services should be protected from interception, interference or damage.			X	Yes	Yes	Yes
Equipment Maintenance	A7.13	*Control:* Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.		X	X	Yes	Yes	Yes
Secure Disposal or Re-use of Equipment	A7.14	*Control:* Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.		X	X	Yes	Yes	Yes
A8 Technological Controls								
User EndPoint Devices (Mobiles)	A8.1	*Control:* Information stored on, processed by or accessible via user endpoint devices should be protected.			X	Yes	Yes	Yes
Privileged Access Rights	A8.2	*Control:* The allocation and use of privileged access rights should be restricted and managed.			X	Yes	Yes	Yes

Information Access Restriction	A8.3	*Control:* Access to information and application system functions should be restricted in accordance with the topic-specific policy on access control.			X	Yes	Yes	Yes
Access to Source Code	A8.4	*Control:* Read and write access to source code, development tools and software libraries should be appropriately managed.			X	Yes	Yes	Yes
Secure Authentication	A8.5	*Control:* Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.			X	Yes	Yes	Yes
Capacity Management	A8.6	*Control:* The use of resources should be monitored and adjusted in line with current and expected capacity requirements.			X	Yes	Yes	Yes
Protection Against Malware	A8.7	*Control:* Protection against malware should be implemented and supported by appropriate user awareness.			X	Yes	Yes	Yes
Management of Technical Vulnerabilities	A8.8	*Control:* Information about technical vulnerabilities of information systems in use should be obtained, the organization’s exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.			X	Yes	Yes	Yes
Configuration Management	A8.9	*Control:* Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.			X	Yes	Yes	Yes
Information Deletion	A8.10	*Control:* Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	X	X	X	Yes	Yes	Yes
Data Masking	A8.11	*Control* Data masking should be used in accordance with the organization’s topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	X	X	X	Yes	Yes	Yes
Data Leakage Prevention	A8.12	*Control:* Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	X		X	Yes	Yes	Yes
Information Backup	A8.13	*Control:* Back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.		X	X	Yes	Yes	Yes
Redundancy of information processing facilities (Availability Management)	A8.14	*Control:* Information processing facilities should be implemented with redundancy sufficient to meet availability.		X	X	Yes	Yes	Yes
Logging	A8.15	*Control:* Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.		X	X	Yes	Yes	Yes
Monitoring Activities	A8.16	*Control:* Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents			X	Yes	Yes	Yes

Clock Synchronisation	A8.17	*Control:* The clocks of information processing systems used by the organization should be synchronized to approved time sources.		X	X	Yes	Yes	Yes
Use of Privileged Utility Programs	A8.18	*Control:* The use of utility programs that might be capable of overriding system & application controls shall be restricted .			X	Yes	Yes	Yes
Installation of Software on Operational Systems	A8.19	*Control:* Procedures and measures shall be implemented to securely manage software installation on operational systems.			X	Yes	Yes	Yes
Network Security	A8.20	*Control:* Networks shall be managed and controlled to protect information in systems and applications.		X	X	Yes	Yes	Yes
Security of Network Services	A8.21	*Control:* Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored		X	X	Yes	Yes	Yes
Segregation of Networks	A8.22	*Control:* Groups of information services, users and information systems shall be segregated on networks.			X	Yes	Yes	Yes
Web Filtering	A8.23	*Control:* Access to external websites shall be managed to reduce exposure to malicious content.			X	Yes	Yes	Yes
Use of Cryptography	A8.24	*Control:* Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.			X	Yes	Yes	Yes
Secure Development Life cycle	A8.25	*Control:* Rules for the secure development of software and systems should be established and applied.			X	Yes	Yes	Yes
Application Security Requirements	A8.26	*Control:* Information security requirements should be identified, specified and approved when developing or acquiring applications.			X	Yes	Yes	Yes
Secure system architecture and engineering Principles	A8.27	*Control:* Principles for engineering secure systems should be established, documented, maintained and applied.			X	Yes	Yes	Yes
Secure Coding Policy	A8.28	*Control:* Secure coding principles shall be applied to software development.			X	Yes	Yes	Yes
Security Testing Processes	A8.29	*Control:* Security testing processes should be defined and implemented in the development life cycle.			X	Yes	Yes	Yes
Outsourced Development	A8.30	The organization should direct, monitor and review the activities related to outsourced system development.					No	No
Separation of development, test and production environments	A8.31	Development, testing and production environments should be separated and secured.			X	Yes	Yes	Yes
Change management	A8.32	Changes to information processing facilities and information systems should be subject to change management procedures.			X	Yes	Yes	Yes
Test Information	A8.33	Test information should be appropriately selected, protected and managed.			X	Yes	Yes	Yes
Protection of information systems during audit testing	A8.34	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.			X	Yes	Yes	Yes