STATEMENT OF APPLICABILITY

Version:	1.3
Date of version:	08/03/2023
Created by:	CISO
Approved by:	CEO
Confidentiality level:	TLP Green

Change history

Date	Version	Created by	Description of change
01/03/22	1.0	CISO	First version
17/03/22	1.1.	CISO	Update layout
19/05/22	1.2.	CISO	Update controls
08/03/23	1.3.	CISO	Update TLP Orange to TLP Green

Table of contents

1. Purpose, scope and users

The purpose of this document is to define which controls are appropriate to be implemented in Compli, the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of Compli who have a role in the ISMS as well as relevant interested parties such as customers or partners.

2. Reference documents

- ISO/IEC 27001 standard, clause 6.1.3 d)
- Information Security Policy
- Risk Assessment and Risk Treatment Methodology

3. Definitions of justification

BR: Business requirement

LR: Legal requirement

RR: Risk requirement (add risk ID)

CR: Contractual requirement

4. Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.5	Information security policies				
A.5.1	Management direction for information security				
A.5.1.1	Policies for information security	Yes	BR	To set the rules of information security for all parties involved	All policies referred to as part of our ISMS
A.5.1.2	Review of the policies for information security	Yes	BR	Keeping the ISMS up to date	Each policy has a designated owner who has to review the document at planned intervals
A.6	Organization of information security				
A.6.1	Internal organization				
A.6.1.1	Information security roles and responsibilities	Yes	BR	To define clear responsibilities for all people involved	Responsibilities for information security are listed in various ISMS documents.
A.6.1.2	Segregation of duties	Yes	BR	Safeguard the confidentiality and integrity of our data.	Definition of roles & authorities as well as specific access rights to information systems.
A.6.1.3	Contact with authorities	Yes	BR	To have a single point of contact.	CEO is the contact person for all authorities.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.6.1.4	Contact with special interest groups	Yes	BR	To keep up to date with relevant information security techniques, risks & vulnerabilities	CISO is responsible for monitoring the list names of interest groups and security forums
A.6.1.5	Information security in project management	Yes	BR	Proactive approach to define the potential information security risks.	Project lead is required to include applicable information security rules in every project
A.6.2	Mobile devices and teleworking				
A.6.2.1	Mobile device policy	Yes	BR	Ensure that employees understand the risks related to Mobile devices	Applicable use of devices is defined in the IT Security Policy
A.6.2.2	Teleworking	Yes	BR – LR	Ensure that employees understand the risks related to working from home	Teleworking rules are part of the IT Security Policy
A.7	Human resource security				
A.7.1	Prior to employment				
A.7.1.1	Screening	Yes	BR	Safeguarding the identity and competences of potential employees	HR and hiring manager check each candidate by checking the CV, contacting former employers, internet search, interview

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.7.1.2	Terms and conditions of employment	Yes	BR - LR	Ensuring that our employees understand their duties and responsibilities in regard to information security	All employees/ contractors sign a (labor) contract which includes a Confidentiality Statement.
A.7.2	During employment				
A.7.2.1	Management responsibilities	Yes	BR	Ensuring the implementation of our policies	Management actively requires that all ISMS rules be implemented by all employees, suppliers and outsourcing partners
A.7.2.2	Information security awareness, education and training	Yes	BR	Ensuring proper awareness remains high	Information Security Policy, Training and Awareness Plan
A.7.2.3	Disciplinary process	Yes	BR - LR	Ensuring correct actions are taken when employees breach policies	Labor rules
A.7.3	Termination and change of employment				

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.7.3.1	Termination or change of employment responsibilities	Yes	BR - LR	Ensuring confidentiality is safeguarded when employees leave the company	All agreements with suppliers and partners contain clauses that remain valid after the termination of employment, as well as the Confidentiality Statements signed by employees.
A.8	Asset management				
A.8.1	Responsibility for assets				
A.8.1.1	Inventory of assets	Yes	BR	Manage the Compli information assets	Assets are logged in the asset inventory
A.8.1.2	Ownership of assets	Yes	BR	Clearly define responsibilities	Each asset has a defined owner.
A.8.1.3	Acceptable use of assets	Yes	BR	Define the rules regarding the use of Compli information systems and hardware	IT Security Policy describing the acceptable use of Compli information systems and hardware
A.8.1.4	Return of assets	Yes	BR	Collecting Compli property at the end of a contract or end of life hardware	Part of the IT Security Policy. Infra support collects the assets at time of contract termination.
A.8.2	Information classification				
A.8.2.1	Classification of information	Yes	BR	Safeguarding the confidentiality and integrity of information	Information Classification Policy

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.8.2.2	Labeling of information	Yes	BR	Visualizing the classification level	Information Classification Policy
A.8.2.3	Handling of assets	Yes	BR	Ensuring the correct handling of information assets	Information Classification Policy
A.8.3	Media handling				
A.8.3.1	Management of removable media	Yes	BR	Ensuring the correct handling of information assets	Policy defined in the IT security policy
A.8.3.2	Disposal of media	Yes	BR	Wiping of data before disposal	Disposal and Destruction Policy
A.8.3.3	Physical media transfer	Yes	BR	Ensuring the correct handling of information assets	Policy defined in the IT security policy
A.9	Access control				
A.9.1	Business requirements of access control				
A.9.1.1	Access control policy	Yes	BR	Ensuring that only authorized people have access to information systems	Access Control Policy
A.9.1.2	Access to networks and network services	Yes	BR	Ensuring that only authorized people have access to information systems	Access Control Policy
A.9.2	User access management				

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.9.2.1	User registration and de-registration	Yes	BR	Ensuring the correct access is given and revoked when people join or leave	Access Control Policy
A.9.2.2	User access provisioning	Yes	BR	Defining the correct access linked to the role of the employee	Access Control Policy
A.9.2.3	Management of privileged access rights	Yes	BR	Ensuring only limited number of people have privileged access	Access Control Policy
A.9.2.4	Management of secret authentication information of users	Yes	BR	Users need to change the initial password at first login	Access Control Policy
A.9.2.5	Review of user access rights	Yes	BR	Ensuring the access rights of users are still valid	Access Control Policy
A.9.2.6	Removal or adjustment of access rights	Yes	BR	Ensuring the access rights of users are still valid	Access Control Policy
A.9.3	User responsibilities				
A.9.3.1	Use of secret authentication information	Yes	BR	Ensuring the users is aware of his duties concerning passwords	Defined in the IT Security Policy
A.9.4	System and application access control				
A.9.4.1	Information access restriction	Yes	BR	Ensuring the confidentiality of data	Access Control Policy, Information Classification Policy

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.9.4.2	Secure log-on procedures	Yes	BR	Ensuring the confidentiality and integrity of data	A secure log-on process exists for all computers on the network
A.9.4.3	Password management system	Yes	BR	Ensuring the use of complex passwords	Managed in the ICT policy Use of password managers
A.9.4.4	Use of privileged utility programs	Yes	BR	Ensuring limited access to utility programs	Only Limited number of persons have the right to use privileged utility programs
A.9.4.5	Access control to program source code	Yes	BR	Ensuring limited access to source code	The program source code is stored in Gitlab and only developers have access rights
A.10	Cryptography				
A.10.1	Cryptographic controls				
A.10.1.1	Policy on the use of cryptographic controls	Yes	BR	Safeguarding the confidentiality and integrity of the data in case of theft/hacks	Policy on the Use of Encryption
A.10.1.2	Key management	Yes	BR	Ensuring the availability of the restore keys	Policy on the Use of Encryption
A.11	Physical and environmental security				
A.11.1	Secure areas				
A.11.1.1	Physical security perimeter	Yes	BR - CR	Ensuring the protection of Compli assets and information	Outsourced to hosting partner

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.11.1.2	Physical entry controls	Yes	BR	Ensuring the protection of Compli assets and information	Outsourced to hosting partner
A.11.1.3	Securing offices, rooms and facilities	Yes	BR	Ensuring the protection of Compli assets and information	Outsourced to hosting partner
A.11.1.4	Protecting against external and environmental threats	Yes	BR	Ensuring the protection of Compli assets and information	Outsourced to hosting partner
A.11.1.5	Working in secure areas	Yes	BR	Limit access the Data rooms and ensure only authorized and trained personnel work in the rooms.	Outsourced to hosting partner
A.11.1.6	Delivery and loading areas	Yes	BR	Prevent unauthorized access through open area's.	Outsourced to hosting partner
A.11.2	Equipment				
A.11.2.1	Equipment siting and protection	Yes	BR	Safeguarding the IT infrastructure in the office location	Limited to Laptops, encrypted. Rules described in IT-Policy
A.11.2.2	Supporting utilities	Yes	BR	Ensuring the safe shut down of servers in case of power outage	Outsourced to hosting partner
A.11.2.3	Cabling security	Yes	BR	Preventing malicious attacks on our infrastructure	Outsourced to hosting partner

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.11.2.4	Equipment maintenance	Yes	BR	Preventing downtime of the information system	Outsourced to hosting partner
A.11.2.5	Removal of assets	Yes	BR	Ensuring employees are aware of the information security risks	IT Security Policy
A.11.2.6	Security of equipment and assets off-premises	Yes	BR	Ensuring employees are aware of the information security risks	IT Security Policy
A.11.2.7	Secure disposal or reuse of equipment	Yes	BR	Ensuring secure disposal of obsolete equipment	Disposal and Destruction Policy
A.11.2.8	Unattended user equipment	Yes	BR	Ensuring employees safeguard unattended equipment	IT Security Policy
A.11.2.9	Clear desk and clear screen policy	Yes	BR	Safeguarding the confidentiality, integrity and availability of information	IT Security Policy Automatic screen lock deployed
A.12	Operations security				
A.12.1	Operational procedures and responsibilities				
A.12.1.1	Documented operating procedures	Yes	BR	Ensuring employees have instructions needed to perform their work	Instructions, policies available on Onedrive

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.12.1.2	Change management	Yes	BR	Ensuring that changes don't adversely influence the information security	Change Management Policy
A.12.1.3	Capacity management	Yes	BR	Ensuring the uptime of the systems	Outsourced to hosting partner
A.12.1.4	Separation of development, testing and operational environments	Yes	BR	Ensuring the integrity of the applications and data	Development and testing are separated.
A.12.2	Protection from malware				
A.12.2.1	Controls against malware	Yes	BR	Protection systems and data from malware.	Malware software implemented on all end point devices
A.12.3	Backup				
A.12.3.1	Information backup	Yes	BR	Ensuring the availability of the data	Backup Policy
A.12.4	Logging and monitoring				
A.12.4.1	Event logging	Yes	BR	Detection of malicious activities or potential security threats	Logs are generated in the Compli platform
A.12.4.2	Protection of log information	Yes	BR	Detection of malicious activities or potential security threats	Logs are only visible by a selected number of authorized persons.
A.12.4.3	Administrator and operator logs	Yes	BR	Detection of malicious activities or potential security threats	Logs are only visible by a selected number of authorized persons.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.12.4.4	Clock synchronization	Yes	BR	Ensuring correct time stamping	System clocks on all computers are synchronized on windows NTP
A.12.5	Control of operational software				
A.12.5.1	Installation of software on operational systems	Yes	BR	Ensuring that no unauthorized software is installed on systems and laptops	Managed by the development partner
A.12.6	Technical vulnerability management				
A.12.6.1	Management of technical vulnerabilities	Yes	BR	Ensuring the latest versions of applications and operating systems are installed.	Outsourced to hosting partner Automatic windows updates on personal laptops by asset owner.
A.12.6.2	Restrictions on software installation	Yes	BR	Ensuring that no unauthorized software is installed on systems and laptops	IT Security Policy
A.12.7	Information systems audit considerations				
A.12.7.1	Information systems audit controls	Yes	BR	Ensuring the availability of the systems during audits	Each audit is planned and coordinated with management; audits are performed only on read-only access rights
A.13	Communications security				
A.13.1	Network security management				

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.13.1.1	Network controls	Yes	BR	Securing our networks	
A.13.1.2	Security of network services	Yes	BR	Securing our networks	networks WPA2 protected.
A.13.1.3	Segregation in networks	Yes	BR	Securing our networks	Separation of guest network
A.13.2	Information transfer				
A.13.2.1	Information transfer policies and procedures	Yes	BR	Safeguarding the confidentiality and integrity of the data in transfer	Information classification policy
A.13.2.2	Agreements on information transfer	Yes	BR	Safeguarding the confidentiality and integrity of the data in transfer	Information classification policy Contracts with clients
A.13.2.3	Electronic messaging	Yes	BR	Safeguarding the confidentiality and integrity of the data in transfer	Information classification policy Contracts with clients
A.13.2.4	Confidentiality or nondisclosure agreements	Yes	BR	Ensuring mutual safeguards of knowledge and data sharing	NDA documents
A.14	System acquisition, development and maintenance				
A.14.1	Security requirements of information systems				

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.14.1.1	Information security requirements analysis and specification	Yes	BR	Ensuring that new information systems comply with our information security requirements	When acquiring new information systems or changing existing ones, CISO must document security requirements in the Compli requirements.
A.14.1.2	Securing application services on public networks	Yes	BR	Ensuring the integrity of the data on the website	HTTPS in place on the Compli website and platform.
A.14.1.3	Protecting application services transactions	Yes	BR	Ensuring the integrity of applications over the internet.	Secure User authentication in place for the Compli platform.
A.14.2	Security in development and support processes				
A.14.2.1	Secure development policy	Yes	BR	Ensure safe and qualitative software	Secure Development Policy
A.14.2.2	System change control procedures	Yes	BR	Ensure changes are handled correctly	Secure Development Policy
A.14.2.3	Technical review of applications after operating platform changes	Yes	BR	Ensure correctly functioning software after OS changes	Outsourced to development partner
A.14.2.4	Restrictions on changes to software packages	Yes	BR	Ensure that customization doesn't influence the level of information security	Change Management Policy

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.14.2.5	Secure system engineering principles	Yes	BR	Ensure that the design & development process is controlled	Secure Development Policy
A.14.2.6	Secure development environment	Yes	BR	Safeguard the development data and source code	Secure Development Policy
A.14.2.7	Outsourced development	Yes	BR	Ensuring safe external development	Secure Development policy
A.14.2.8	System security testing	Yes	BR	Ensure that software release comply with the security and quality objectives	Outsourced to development partner
A.14.2.9	System acceptance testing	Yes	BR	Ensure a controlled release of new software/systems	Secure Development Policy
A.14.3	Test data				
A.14.3.1	Protection of test data	Yes	BR	Ensure the test data is secure.	Secure Development Policy
A.15	Supplier relationships				
A.15.1	Information security in supplier relationships				
A.15.1.1	Information security policy for supplier relationships	Yes	BR	Ensure that suppliers adhere to the Compli Information security requirements	Supplier Security Policy

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.15.1.2	Addressing security within supplier agreements	Yes	BR	Ensure that suppliers adhere to the Compli Information security requirements	Supplier Security Policy Supplier agreements SLA's
A.15.1.3	Information and communication technology supply chain	Yes	BR	Ensure that suppliers adhere to the Compli Information security requirements	Supplier Security Policy
A.15.2	Supplier service delivery management				
A.15.2.1	Monitoring and review of supplier services	Yes	BR	Ensure that suppliers adhere to the Compli Information security requirements	Supplier Security Policy Supplier agreements SLA's
A.15.2.2	Managing changes to supplier services	Yes	BR	Ensure that suppliers adhere to the Compli Information security requirements	Supplier Security Policy Supplier agreements SLA's
A.16	Information security incident management				
A.16.1	Management of information security incidents and improvements				
A.16.1.1	Responsibilities and procedures	Yes	BR	Ensuring lessons learned from information security incidents	Incident Management Procedure

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.16.1.2	Reporting information security events	Yes	BR	Ensuring correct logging information security incidents	Incident Management Procedure Incident log
A.16.1.3	Reporting information security weaknesses	Yes	BR	Ensuring lessons learned from information security weaknesses	Incident Management Procedure Incident log
A.16.1.4	Assessment of and decision on information security events	Yes	BR	Ensuring the correct handling of security events	Incident Management Procedure Incident log
A.16.1.5	Response to information security incidents	Yes	BR	Ensuring the correct handling of security events	Incident Management Procedure Incident log
A.16.1.6	Learning from information security incidents	Yes	BR	Ensuring lessons learned from information security incidents	Incident Management Procedure Incident log
A.16.1.7	Collection of evidence	Yes	BR	Ensuring lessons learned from information security incidents	Incident Management Procedure Evidence stored in Microsoft Teams
A.17	Information security aspects of business continuity management				
A.17.1	Information security continuity				

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.17.1.1	Planning information security continuity	Yes	BR	Ensuring that the business and information security are safeguarded in case of a disaster	Disaster recovery plan
A.17.1.2	Implementing information security continuity	Yes	BR	Ensuring that the business and information security are safeguarded in case of a disaster	Disaster recovery plan
A.17.1.3	Verify, review and evaluate information security continuity	Yes	BR	Ensuring that the business and information security are safeguarded in case of a disaster	Disaster recovery plan Table top test of the DRP
A.17.2	Redundancies				
A.17.2.1	Availability of information processing facilities	Yes	BR	Ensuring redundancy in our IT infrastructure	Redundancy in place
A.18	Compliance				
A.18.1	Compliance with legal and contractual requirements				
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes	BR - LR	Ensuring Compli complies with statutory and contractual requirements	List of Legal, Regulatory, Contractual and Other Requirements
A.18.1.2	Intellectual property rights	Yes	BR - LR	Ensuring no pirate software is present on our systems	IT Security Policy

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	Justification for selection/ non-selection	Control objectives	Implementation method
A.18.1.3	Protection of records	Yes	BR	Safeguarding alle business critical data	Back up policy Access control policy
A.18.1.4	Privacy and protection of personally identifiable information	Yes	BR - LR	Safeguarding stored or processed personal data	Data processing register Processing agreements
A.18.1.5	Regulation of cryptographic controls	Yes	BR - LR	Ensuring that we comply with regulatory requirements on crypto	List of Legal, Regulatory, Contractual and Other Requirements, Policy on the Use of Encryption
A.18.2	Information security reviews				
A.18.2.1	Independent review of information security	Yes	BR	Ensuring that our ISMS is effective	Internal Audit Procedure, certification audit by third party CB
A.18.2.2	Compliance with security policies and standards	Yes	BR	Ensuring our ISMS policies remain up to date	All owners of information assets, as well as the management, regularly review the implementation of security controls
A.18.2.3	Technical compliance review	Yes	BR	Ensuring that the Compli information systems remain technically compliant.	CISO is responsible for checking the technical compliance of information systems with security requirements

5. Validity and document management

This document is valid as of 08.03.2023.

The owner of this document is the CISO, who must check and, if necessary, update the document at least once a year, and immediately after risk assessment review and updates to the Risk Assessment Table and Risk Treatment Table.