CORAL project

Methodology for the Conformity Self-Assessment and Basic Assurance

Target Audience & Domains of Technical Requirements

A CORAL project deliverable



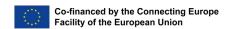
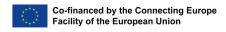


Table of Contents

1 Introduction	3
1.1 Objectives of this document	3
2 Identification of CSA basic target audience and Products/ Services	3
3 Definition of technical requirements	4
3.1 Technical requirements for ICT products	
3.1.1. Technical requirements for web applications product	
3.1.2. Technical requirements for AI products	8
3.1.3. Technical requirements for IOT products	10
3.2 Technical requirements for ICT services	
3.3 Technical requirements for ICT processes	19
4 Conclusion	





1 Introduction

1.1 Objectives of this document

This document focuses on the identification of CSA's basic target audience, the definition of low-complexity products, services, and the identification of technical scopes. These two tasks are defined in activity 2 of the CORAL project, which covers the "Methodology for the Conformity Self-Assessment and Basic Assurance". The objectives per task can be summarized to the following points:

- The task regarding the identification of the target audience and the
 definition of low-complexity products and services will be dedicated to the
 identification of the category of ICT services, ICT products, etc. that could
 be concerned by the certification being designed. It is important to note
 that the certification procedure would not be sector-specific, but as generic
 as possible.
- The identification of technical scopes will be dedicated to the identification
 of the main domains of technical inquiry needed to cover all the baseline of
 information security and cybersecurity. These scope would later be
 considered as reference points in setting up the questionnaires for the selfassessment, which is an important step in the certification procedure.

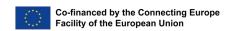
2 Identification of CSA basic target audience and Products/ Services

The CORAL project focuses on the need for a basic cybersecurity certification in the context of CSA, in an effort to make it more accessible to startups, small and medium enterprises (SMEs), etc.

Startups and SMEs often provide ICT services or propose ICT products or processes that could be considered as non-critical and low complicity, which perfectly align with the scope defined in the CORAL project. Furthermore, these companies have very limited information technology and cybersecurity resources, which prevent them from undertaking existing certifications.

The information security and cybersecurity maturity level of most startups and SMEs is on average low, and with a limited budget, they can badly afford the





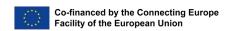
existing information security certifications. This let the products, processes, and services they offer insecure and vulnerable. Hence, the proposed CORAL certification framework would not only be very affordable but also provide to this category of companies a friendly entry-level certification that addresses all security baselines.

However, it is important to note that any other categories of companies providing ICT services or proposing ICT products and ICT processes that could be characterized as non-critical and low complexity, and aiming to achieve the basic assurance level can also request for the CORAL certification. Large enterprises often have a considerable number of products, services, and processes that possibly consume a lot of resources and budget for security certification. The CORAL certification procedure would be beneficial to large enterprises by reducing certification costs and the number of works on their resources. The certification framework proposed in the context of this project does not discriminate between startups, SMEs, and large enterprises.

The following categories of ICT products, services, and processes have been identified and defined as the scope to be considered for the definition of the technical requirements and the certification procedure. This scope could be amended in the future based on needs, requirements, and new Cybersecurity and IT risk management development at the European level or in the world.

	Categories
Internet of Things (IoT)	
Products Artificial Intelligence 5G Component products (Software, Hardware)	
	Cloud services
Services Supply chain services	
	IT services
Manufacturing processes	
Processes	Supply chain processes
	Application development processes





3 Definition of technical requirements

The defined technical requirements result from our findings during the study, review of existing standards, research, and literature on the best practices to secure ICT products, ICT services, and ICT processes. The technical requirements defined in the context of the CORAL project are limited to the objectives of the certification, that is basic assurance and low complexity products, services, and processes.

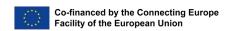
The technical requirements are defined for ICT products, ICT services, ICT processes. Especially for ICT products, due to the particularity of some type of technologies and products, specific requirements are defined by technology or type of products.

3.1 Technical requirements for ICT products

ICT products independent of the technology or sector should have the following requirements, which are defined based on the Common Criteria. These controls are considered as a security baseline for any ICT products independent of the type of technology or sector.

Domains	Controls
	Security architecture
Security architecture	Self protection
	Non-bypassable
Security by design: Basic Architecture design principles	Domain Separation
	Layering
	Encapsulation
	Redundancy of systems and processes
	Access management
	Attack surface minimization Basic systems and components hardening
	Centralized parameter validation
	Centralized general security services
	Preparing for error and exception





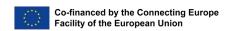
	handling
Testing (functional and security	Security testing with automatic tools
testing)	Functional testing
Vulnerability management strategy / plan	Vulnerability analysis and management

3.1.1. Technical requirements for web applications product

The technical requirements for web applications products are mostly based on the OWASP application security verification standard. OWASP security requirements were considered as a reference in designing these requirements because it is the market-leading resource for web application security evaluation. However, the controls are set for the evaluation of low-risk and low complexity products and to achieve the basic level of assurance.

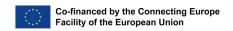
Domains	Controls
Authenticator requirements	Anti-automation is implemented (eg. CAPTCHA)
	Notify user following updates to authentication details
	Password length
	Password complexity
Password Security Requirements	Users can change their password
	Password change functionality requires the user's current and new password
Credential Storage requirements	Passwords are not stored in plain text
	Passwords are hashed and salted before been stored
Credential Recovery requirements	No Password hints
	The current password cannot be reveal
	Default accounts and credentials are changed or deactivated
Session management	New session token is generated on user





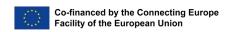
Principe of deny by default is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Ferror Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the beaution		authentication
The "Httponly" flag is set for cookie-based session tokens Prevent reuse of session token Principe of least privilege is implemented Principe of deny by default is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements No sensitive information is logged by the application Users credentials are not logged by the application Error Handling Input Walidation No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in		
hased session tokens Prevent reuse of session token Principe of least privilege is implemented Principe of deny by default is implemented Principe of deny by default is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements Log management No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browners.		Security of session token generation
Access control security requirements Principe of least privilege is implemented Principe of deny by default is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Protection against SSRF attacks Prevent executable file to be uploaded All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling Error Handling Principe of least privilege is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Measure against HTTP parameter pollution attacks Protection against SSRF attacks Protection against SSRF attacks Prevent executable file to be uploaded All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Users credentials are not logged by the application Principe of deny by default is implemented Input data sanitization Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against parameter pollution Measure against HTTP parameter pollution Measure against HTTP parameter pollution Measure against HTTP parameter pollution Input validation		
implemented Principe of deny by default is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Inputs validation Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Protection against SSRF attacks Prevent executable file to be uploaded All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.		Prevent reuse of session token
Principe of deny by default is implemented Anti-CSRF is implemented Directory browsing is disabled Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Ferror Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the beautiful principle of deny by default is implement and sensitive data are not stored in the beautiful principle of the department.	Access control security requirements	
Directory browsing is disabled Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.		
Input data sanitization Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browsers		Anti-CSRF is implemented
Inputs validation Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Protection against SSRF attacks Prevent executable file to be uploaded Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browners		Directory browsing is disabled
Input Validation requirements Measure against HTTP parameter pollution attacks Protection against parameter assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browners		Input data sanitization
Input Validation requirements Protection against parameter assignment attacks Protection against SSRF attacks Protection against SSRF attacks Prevent executable file to be uploaded All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.		Inputs validation
assignment attacks Protection against SSRF attacks Prevent executable file to be uploaded All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browners	Input Validation requirements	
Prevent executable file to be uploaded Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.		
Error handling and logging verification requirements All application components and systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser		Protection against SSRF attacks
requirements Systems fail securely No sensitive information is logged by the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.		Prevent executable file to be uploaded
the application Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.	Error handling and logging verification requirements	**
Users credentials are not logged by the application Error Handling No sensitive information is shared in error messages or logs Implement Anti-caching PII and sensitive data are not stored in the browser.	_	
error messages or logs Implement Anti-caching PII and sensitive data are not stored in	Log management	
PII and sensitive data are not stored in	Error Handling	
the browser		Implement Anti-caching
	Data Protection Verification Requirements	
		Clear authenticated data from browser
Users can delete or export their PI		Users can delete or export their PI
Data privacy policy		Data privacy policy
Communications Verification Secured TLS is implemented	Communications Verification	Secured TLS is implemented





Doguinamenta	Secure TLS protocols and arlgorithms are implemented
Requirements	Unsecure SSL and TLS protocols are disabled
	Updates are done securely
Deployed Application Integrity Controls	Integrity protection
	Subdomain takeover
	File size restriction is set
	Protection against path transversal
	Protection against local file inclusion
	Protection against RFI and SSRF
	Protection against Reflective File Download (RFD)
File and Resources Verification Requirements	Protection against OS command injection
	Upload file security
	Upload file security (Scan files for malware)
	Restrict file upload to specific
	Security of upload requests
	Whitelisting data or file upload sources
API and Web Service Verification Requirements	Administrator access requirements
	Protection of sensitive information / credentials
RESTful Web Service Verification Requirements	Validation of JSON schema
	Secure RESTful web services
Dependency	Secure dependencies update
	Disable unused features
	Ensure the integrity of exchanged data between systems
Unintended Security Disclosure	Disable debug mode
Requirements	Limit HTTP header information disclosure
	HTTP response contains a Content- Type header.





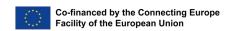
	API responses contain a Content- disposition
	Content Security policy is implemented
	API responses contain a X-Content type
	Strict-Transport Security
	A secure Referrer Policy is implemented
	Content security policy

3.1.2. Technical requirements for AI products

The technical requirements for Artificial intelligence (AI) products are based on the Assessment List for Trustworthy AI (ALTAI) and controls, which is intended for self-evaluation purposes. These requirements aim to ensure that users benefit from AI without being exposed to unnecessary risks by indicating a set of concrete steps for self-assessment.

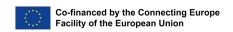
Domains	Controls
Fundamental rights	AI system should not negatively discriminate against people on any grounds.
	Process to test and remediate potentially discrimination against people.
	Process to test and remediate child rights and protection.
	Are end- users or subjects informed that they are interacting with an AI system?
	Did you put in place procedures to avoid that end-users over-rely on the AI system?
Access Management	Access control to data set and model is implemented.
	Principe of least privilege is implemented.
	Principe of deny by default is implemented.
	Users are required to change default





Password requirements Password strength control. Secure storage of services and user passwords. Implement data subject rights (request, deletion, etc) Respect the rights of the child Data privacy requirements in line with GDPR freedom of expression and information and/or freedom of assembly and association?		password during initial configuration.
Secure storage of services and user passwords. Implement data subject rights (request, deletion, etc) Respect the rights of the child Data privacy requirements in line with GDPR freedom of expression and information and/or freedom of assembly and association? Prevent data disclosure Protection against data poisoning Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model	Password requirements	
Implement data subject rights (request, deletion, etc) Respect the rights of the child Data privacy requirements in line with GDPR freedom of expression and information and/or freedom of assembly and association? Prevent data disclosure Protection against data poisoning Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model		Secure storage of services and user
Data privacy requirements in line with GDPR freedom of expression and information and/or freedom of assembly and association? Data security & privacy requirements Prevent data disclosure Protection against data poisoning Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model		Implement data subject rights (request,
GDPR freedom of expression and information and/or freedom of assembly and association? Data security & privacy requirements Prevent data disclosure Protection against data poisoning Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model		Respect the rights of the child
and/or freedom of assembly and association? Data security & privacy requirements Prevent data disclosure Protection against data poisoning Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model		1 1 1
Protection against data poisoning Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model		and/or freedom of assembly and
Data poisoning (i.e. manipulation of training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model	Data security & privacy requirements	Prevent data disclosure
training data); Model evasion (i.e. classifying the data according to the attacker's will); Model inversion (i.e. infer the model		Protection against data poisoning
according to the attacker's will); Model inversion (i.e. infer the model		
· · · · · · · · · · · · · · · · · · ·		according to the attacker's
		,
Implement a vulnerability assessment	Risk & Vulnerability management	Implement a vulnerability assessment
Implement a risk assessment.		Implement a risk assessment.
Vulnerability reporting process.		Vulnerability reporting process.
Continuous risk assessment procedure.		Continuous risk assessment procedure.
Process for security notification to customers.		
Risk & Vulnerability management Assess potential forms of attacks against the AI system.		1
Evaluation of the possible attack surface.		
Implement processes to maintain security levels of components over time.		security levels of components over
Ensure used component comply with third parties' security requirements.		
Security update requirements		Security update requirements





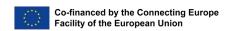
Security update management	Users update notification procedure.
General security requirements	Model inversion attack
	Evaluate all security dependencies.
	Define and test fail-safe fallback plans to address AI system errors.
	Model accuracy on the security of the AI solution.
	Implementation security monitoring and notification.
	Implement error or unplanned event handling.
	Consider security in the continual improvement of the AI model.
	Log management

3.1.3. Technical requirements for IOT products

These technical requirements are defined based on principles for securing the internet of things and frameworks defined by different structures and organizations across the world.

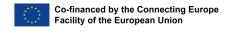
Domains	Controls
Security by Design Principles	A security threat and risk assessment implemented before product/service design.
	Remove OS command line access to privileged accounts.
	Essential kernel, services or functions are prevented from being called by unauthorized external product.
	Provide a manual with a key security user information.
Access Management	Use unique credentials for Each Device, to prevent unauthorized access.
	Users should be able to update their credentials.





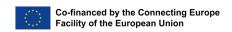
	Unique and tamper-resistant device identifier.
	Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).
	Ship with reasonably updated software.
	Null or blank passwords should be not be allow.
	New passwords containing the user account name should not be allow.
	Password entry follows industry standard practice.
	Defense against brute force repeated login attempts should be implemented.
	The product securely stores any passwords using an industry standard cryptographic algorithm.
Password management	Access control to restrict access to sensitive information should be implemented.
	The product only allows controlled user account access.
	The product supports having any or all of the factory default user login passwords required password change during installation or deployment.
	For product with a web interface, user passwords are not stored in plain text.
	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.
	Administration Interfaces are accessible only by authorized operators.
Software and System update Management	Automated software updates mechanism.
	Process for validating "updates" and





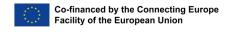
	updating devices.
	Users should have the ability to disable updating.
	Software update packages has it digital signature, signing certificate and signing certificate chain.
	User notification of software updates (Specially security updates) should be implemented.
	Encrypt local storage of sensitive data.
Security of stored and processed data	Restrict access to data to only authenticated users and services.
	Minimize exposed attack surfaces.
	Ensure software integrity.
	Configuration should be tested and hardened.
	Input data validation
Constant handoning	Close Unnecessary Ports and Disable Unnecessary Services.
System hardening	Use libraries that are actively maintained and supported.
	The product's processor system has an irrevocable hardware Secure Boot process by default.
	The OS is separated from the application(s) and is only accessible via defined secure interfaces.
	System should have some level of resilience to outage.
System security resilience	Continue to Function If the Cloud Back- End Fails.
Installation and Maintenance	Friendly installation and maintenance procedure.
	Installation and maintenance manuals
	are available.
Security & Cryptography best practices	are available. Encrypt Configuration (Command & Control) Communications By Default.





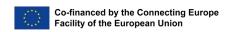
	Controllers.
	Cryptographically sign application image.
	Implement a secure method of key insertion that protects keys against copying.
	Enforce memory protection.
	Implement an Input validation for all type of data.
	Ensure that any devices with duplicate serial numbers are not shipped.
Data Privacy	Product is shipped with a privacy policy that is easy to find & understand.
	Implement user data privacy rights.
	Collect just the PII need for the product to work.
	Personal Information is encrypted and only accessible after successful authentication.
	The product ensures that only authorized personnel have access to personal data of users.
	The product manufacturer or Service provider shall ensure that a data retention policy is in place and documented for users.
	There is a method for the product owner to be informed about what Personal Information is collected.
	There is a method for each user to check/verify what Personal Information is collected.
	Data collection is done only in accordance with the authorization of the user.
	Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any





	impact to product features or functionality.
	Comply with applicable regulations, including but not limited to the Children's Online Privacy Protection Act (COPPA).
	Report discovery and remediation of software vulnerabilities.
Vulnerability management	Vulnerability reporting process.
	Process for security notification to user.
Support	Provide contact information and procedure to contact the support service.
Compliance	Compliance to any regulatory requirements in the sector of operation (Eg. ISO 30111)
Configuration management	Prevent an authorized and unauthenticated software, configurations and files.
	If a factory reset is made, the device should warn that secure operation may be compromised until updated.
Communication Security	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password.
	For any Wi-Fi connection, WPA-2 AES or a similar strength encryption has been used.
	Where WPA-2 WPS is used it has a unique and random key per device.
	All network communications keys are stored securely, in accordance with industry standards.
	Where a TCP protocol is used, it is protected by a TLS connection with no known vulnerabilities.
	Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off.





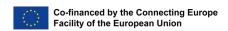
	All product related web servers have their webserver HTTP trace and trace methods disabled.
	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities.
	Relevant security advisories monitoring is implemented.
	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers.
	Communication with any remote systems is done via a secure remote connection.

3.2 Technical requirements for ICT services

The requirements defined for evaluating the security of ICT services are based on the ISO standard and the controls from the center for internet security (CIS controls). The requirements are set to be very practical and limited to the scope and objectives for the CORAL certification.

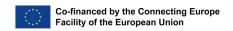
Domains	Controls
	Policies for information security.
	Information security roles and responsibilities.
	Contact with the authorities.
Information security policies	Training and awareness.
	Human resource security requirements.
	regulatory requirements.
	Implementation of security procedures
Inventory and controls of Assets	Asset inventory.
	Ensure only authorized software asset is supported.
	Utilize automated software inventory





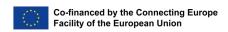
	tools.
	allowlist authorized software.
	allowlist authorized libraries.
	allowlist authorized scripts.
	Establish and maintain a data management process.
	Establish and maintain a data inventory.
	Configure data access control Lists.
	Enforce data retention policy.
	Securely dispose of data.
D . D	Encrypt data on end-user devices.
Data Protection	Establish and maintain a data Classification Scheme.
	Document data flows.
	Encrypt data on removable media.
	Encrypt sensitive data in transit.
	Encrypt sensitive data at rest.
	Deploy a data loss prevention solution.
	Log sensitive data access.
Secure Configuration of Assets	Establish and maintain a secure configuration process.
	Establish and maintain a secure configuration process for network infrastructure.
	Configure automatic session locking on enterprise assets.
	Implement and manage a firewall on servers.
	Implement and manage a firewall on end-user devices.
	Securely manage enterprise assets and software.
	Manage default accounts on enterprise assets and Software.
	Uninstall or disable unnecessary





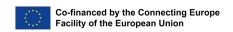
	services on enterprise assets and software.
	Configure trusted DNS servers on enterprise assets.
	Enforce automatic device lockout on portable end-user devices.
	Enforce remote wipe capability on portable end-user devices.
	Separate enterprise workspaces on mobile end-user devices.
	Establish an access granting process.
	Require a secret authentication information to access the enterprise assets.
	Establish an access revoking process.
Access Control Management	Require MFA for externally exposed Applications.
	Require MFA for remote network access.
	Require MFA for administrative access.
	Establish and maintain an inventory of authentication and authorization systems.
	Centralize access control.
	Define and maintain role-based access control.
	Establish and maintain an inventory of accounts.
	Disable dormant accounts.
Account Management	Restrict administrator privileges to dedicated administrator accounts.
	Establish and maintain an inventory of service accounts.
	Centralize account management.
Continuous vulnerability Management	Establish and maintain a vulnerability management process.
	Establish and maintain a remediation





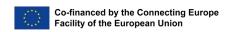
	process.
	Perform automated operating system patch management.
	Perform automated application patch management.
	Perform automated vulnerability scans of internal enterprise assets.
	Perform automated vulnerability scans of externally-exposed enterprise assets.
	Remediate detected vulnerabilities.
	Establish and maintain an audit log management process.
Audit log management	Collect and retain audit logs.
	Ensure adequate audit log storage.
	Conduct audit log reviews.
Malware Defenses	Deploy and maintain anti-malware software.
	Configure automatic anti-malware signature updates.
	Disable auto-run and auto-play for removable media.
	Configure automatic anti-malware scanning of removable media.
	Centrally manage anti-malware software.
Data Recovery	Establish and maintain a data recovery process .
	Perform automated backups.
	Protect recovery data.
	Establish and maintain an isolated instance of recovery data .
	Test data recovery.
Network Infrastructure management	Ensure network infrastructure is up-to-date.
	Establish and maintain a secure network architecture.
	Securely manage network





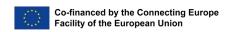
	infrastructure.
	Establish and maintain architecture diagram(s).
	Centralize network authentication, authorization, and auditing (AAA).
	Use of secure network management and communication protocols .
	Ensure remote devices utilize a VPN and are connecting to an enterprise's AAA infrastructure.
	Centralize security event alerting.
	Deploy a host-based intrusion detection solution.
Network Monitoring and defense	Deploy a network intrusion detection solution.
	Perform traffic filtering between network segments.
	Manage access control for remote assets.
	Collect network traffic flow logs.
Security Awareness and Skills Training	Establish and maintain a security awareness program.
	Train workforce members to recognize social engineering attacks.
	Train workforce members on authentication best practices.
	Train workforce on data handling best practices.
	Train workforce members on causes of unintentional data exposure.
	Train workforce members on recognizing and reporting security incidents.
	Train workforce on how to identify and report if their enterprise assets are missing security updates.
	Train workforce on the dangers of connecting to and transmitting





	enterprise data over insecure networks.
	Establish and maintain a secure application development process.
	Establish and maintain a process to accept and address software vulnerabilities.
	Perform root cause analysis on security vulnerabilities.
	Establish and manage an inventory of third-party software components.
Application Security	Use up-to-date and trusted third-party software components.
	Use standard hardening configuration templates for application infrastructure.
	Separate production and non-production systems.
	Train developers in application security concepts and secure coding.
	Apply secure design principles in application architectures.
	Designate personnel to manage incident handling.
Incident Response Management	Establish and maintain contact information for reporting security incidents.
	Establish and maintain an enterprise process for reporting incidents.
	Establish and maintain an incident response process.
	Assign key roles and responsibilities.
	Define mechanisms for communicating during incident response.
	Define security clauses.
Contract security requirements	Service level agreements clauses.
	Responsibilities from each parties.
Contract privacy requirements	Define data privacy clauses (Data





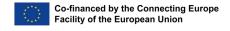
	transfer , Geographic location of data, etc.)
	Controller and processor responsibilities.
	Controls any third parties accessing data.

3.3 Technical requirements for ICT processes

The technical requirements ICT processes are defined based on the ISO/IEC 27036 series which covers Information security for supplier relationships and ISO/IEC 21827:2008.

Domains	Controls
Agreement Process	Supply Process
Organizational project-enabling process	Life cycle model management process
	Infrastructure Management process
	Project Portfolio Management Process
	Human Resource Management Process
	Quality Management Process
Project Process	Project Planning Process
	Project Assessment and Control Process
	Decision Management Process
	Risk Management Process
	Configuration Management Process
Technical Process	Stakeholder Requirements Definition Process
	Requirements Analysis Process
	Architectural Design Process
	Implementation Process
	Integration Process
	Verification Process
	Operation Process
	Maintenance Process





	Disposal Process
Compliance requirements	Compliance with legal and contractual requirements
	Identification of applicable legislation and contractual requirements
	Intellectual property rights
Supply relationship Process	Supplier selection process
	Supplier relationship agreement process
	Supplier relationship management process
	Supplier relationship termination process

4 Conclusion

This document's aim is to present the target audience, products, services, and processes suitable for the CORAL certification framework. The technical requirements and controls necessary to evaluate the security and conformity of ICT products, ICT services, and ICT processes were also presented.

These requirements would further be used as a reference to setting up the questions for the conformity self-assessment and the evaluation of the assurance level.

However, the project team is aware that neither the target audience nor the technical requirements are fixed. These can change and evolve during the project and the lifetime of the certification framework based on threats landscape and vulnerabilities. Furthermore, the CORAL certification framework is based on the framework proposed by the ENISA, hence any change in the scope of products, services, processes, and assurance evaluation criteria in the Cybersecurity Act would affect it.



