CORAL project

Methodology for the Conformity Self-Assessment and Basic Assurance

Target Audience & Domains of Technical Requirements

A CORAL project deliverable

cases.lu
Cyberworld Awareness and
Security Enhancement Services
LUXEMBOURG

Co-financed by the Connecting Europe
Facility of the European Union

Table of Contents

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 scopes would later be considered as reference points in setting up the questionnaires for the self-assessment, 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
Products	Internet of Things (IoT)
	Artificial Intelligence
	5G Component products (Software, Hardware)
	Manufacturing of industrial products with low complexity and basic assurance level .
Services	Cloud services
	Supply chain services
	IT services
Processes	Manufacturing 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.

Co-financed by the Connecting Europe Facility of the European Union

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 testing)	Security testing with automatic tools
	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 Security Requirements	Password length
	Password complexity
	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 authentication
	Session tokens are in the browser using secure methods
	Security of session token generation
	The "Httponly" flag is set for cookie-based session tokens
	Prevent reuse of session token
Access control security requirements	Principe of least privilege is implemented
	Principe of deny by default is implemented
Input Validation requirements	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
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
Data Protection Verification Requirements	Implement Anti-caching
	PII and sensitive data are not stored in the browser
	Clear authenticated data from browser
	Users can delete or export their PI
	Data privacy policy
Communications Verification Requirements	Secured TLS is implemented
	Secure TLS protocols and arlgorithms are implemented
	Unsecure SSL and TLS protocols are disabled
Deployed Application Integrity Controls	Updates are done securely
	Integrity protection
	Subdomain takeover
File and Resources Verification Requirements	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)
	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 Requirements	Disable debug mode
	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.
Password requirements	Users are required to change default password during initial configuration.
	Password strength control.
	Secure storage of services and user passwords.
Data security & privacy 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 parameters)
Risk & Vulnerability management	Implement a vulnerability assessment
	Implement a risk assessment.
	Vulnerability reporting process.
	Continuous risk assessment procedure.
	Process for security notification to customers.
	Assess potential forms of attacks against the AI system.
	Evaluation of the possible attack surface.
	Implement processes to maintain security

	levels of components over time.
	Ensure used component comply with third parties’ security requirements.
Security update management	Security update requirements
	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).
Password management	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.
	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.
Security of stored and processed data	Encrypt local storage of sensitive data.
	Restrict access to data to only authenticated users and services.
System hardening	Minimize exposed attack surfaces.
	Ensure software integrity.
	Configuration should be tested and hardened.
	Input data validation
	Close Unnecessary Ports and Disable Unnecessary Services.
	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 security resilience	System should have some level of resilience to outage.
	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	Encrypt Configuration (Command & Control) Communications By Default.
	Secure communications to and from IoT 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).
Vulnerability management	Report discovery and remediation of software vulnerabilities.
	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**
Organisation Of Information Security	Information Security Management System
	Segregation Of Duties
	Contact With Authorities And Interest Groups
	Information Security In Project Management
Information Security Policies	Global Information Security Policy
	Security Policies And Procedures
	Exceptions
Risk Management	Risk Management Policy
	Risk Assessment Implementation
	Risk Treatment Implementation
Human Resources	Human Resource Policies
	Verification Of Qualification And Trustworthiness
	Employee Terms And Conditions
	Security Awareness And Training
	Termination Or Change In Employment
	Confidentiality Agreements
Asset Management	Asset Inventory
	Acceptable Use And Safe Handling Of Assets Policy
	Commissioning And Decommissioning Of Hardware
	Acceptable Use, Safe Handling And Return Of Assets
	Asset Classification And Labelling
Physical Security	Physical Security Perimeters
	Physical Site Access Control
	Working In Non-Public Areas
	Equipment Protection
	Protection Against External And Environmental Threats
Operational Security	Capacity Management – Planning
	Capacity Management – Monitoring
	Capacity Management – Controlling Of Resources
	Protection Against Malware – Policies
	Protection Against Malware – Implementation
	Data Backup And Recovery – Policies
	Data Backup And Recovery – Monitoring

	Data Backup And Recovery – Regular Testing
	Data Backup And Recovery – Storage
	Logging And Monitoring – Policies
	Logging And Monitoring – Derived Data Management
	Logging And Monitoring – Identification Of Events
	Logging And Monitoring – Access, Storage And Deletion
	Logging And Monitoring – Attribution
	Logging And Monitoring – Configuration
	Logging And Monitoring – Availability
	Managing Vulnerabilities, Malfunctions And Errors – Policies
	Managing Vulnerabilities, Malfunctions And Errors – Online Registers
	Managing Vulnerabilities, Malfunctions And Errors – Vulnerability Identification
	Managing Vulnerabilities, Malfunctions And Errors – Measurements, Analyses And Assessments Of Procedures
	Managing Vulnerabilities, Malfunctions And Errors – System Hardening
	Separation Of Datasets In The Cloud Infrastructure
Identity, Authentication, And Access Control Management	Policies For Access Control To Information
	Management Of User Accounts
	Locking, Unlocking And Revocation Of User Accounts
	Management Of Access Rights
	Regular Review Of Access Rights
	Privileged Access Rights
	Authentication Mechanisms
	Protection And Strength Of Credentials
	General Access Restrictions
Cryptography And Key Management	Policies For The Use Of Encryption Mechanisms And Key Management
	Encryption Of Data In Transit
	Encryption Of Data At Rest
	Secure Key Management
Communication Security	Technical Safeguards
	Security Requirements To Connect Within The Csp's Network
	Monitoring Of Connections Within The Csp's Network
	Cross-Network Access
	Networks For Administration
	Traffic Segregation In Shared Network Environments
	Network Topology Documentation
	Data Transmission Policies

Co-financed by the Connecting Europe
Facility of the European Union

Portability And Interoperability	Documentation And Security Of Input And Output Interfaces
	Contractual Agreements For The Provision Of Data
	Secure Deletion Of Data
Change And Configuration Management	Policies For Changes To Information Systems
	Risk Assessment, Categorisation And Prioritisation Of Changes
	Testing Changes
	Approvals For Provision In The Production Environment
	Performing And Logging Changes
Development Of Information Systems	Policies For The Development And Procurement Of Information Systems
	Development Supply Chain Security
	Secure Development Environment
	Separation Of Environments
	Development Of Security Features
	Identification Of Vulnerabilities Of The Cloud Service
	Outsourcing Of The Development
Procurement Management	Policies And Procedures For Controlling And Monitoring Third Parties
	Pmsk Assessment Of Suppliers
	Directory Of Suppliers
	Monitoring Of Compliance With Requirements
	Exit Strategy
Incident Management	Policy For Security Incident Management
	Processing Of Security Incidents
	Documentation And Reporting Of Security Incidents
	User’s Duty To Report Security Incidents
	Involvement Of Cloud Customers In The Event Of Incidents
	Evaluation And Learning Process
	Incident Evidence Preservation
Business Continuity	Business Continuity Policies And Top Management Responsibility
	Business Impact Analysis Procedures
	Business Continuity And Contingency Planning
	Business Continuity Tests And Exercises
Compliance	Identification Of Applicable Compliance Requirements
	Policy For Planning And Conducting Audits
	Internal Audits Of The Internal Control System
	Information On Internal Control System Assessment
User Documentation	Guidelines And Recommendations For Cloud Customers
	Online Register Of Known Vulnerabilities

	Locations Of Data Processing And Storage
	Justification Of The Targeted Assurance Level
	Guidelines And Recommendations For Composition
	Contribution To The Fulfilment Of Requirements For Composition
Dealing With Investigation Requests From Government Agencies	Legal Assessment Of Investigative Inquiries
	Iinforming Cloud Customers About Investigation Requests
	Conditions For Access To Or Disclosure Of Data In Investigation Requests
Product Safety And Security (Pss)	Error Handling And Logging Mechanisms
	Session Management
	Software Defined Networking
	Images For Virtual Machines And Containers
	Locations Of Data Processing And Storage

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.