State-of-the-Art: Cybersecurity standards and guidelines for low-complexity, low-risk products, services, and processes v1.0

A CORAL project deliverable

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

Document working group

Name	Affiliation	Role
Dominique Kogue	SMILE GIE	Reviewer
Fabien Mathey	SMILE GIE	Reviewer
Natalia Cassagnes	ANEC GIE	Contributor
Rim Doukha	ANEC GIE	Contributor
Shyam Wagle	ANEC GIE	Contributor
Jean Lancrenon	ANEC GIE	Leading contributor

Document history

Version	Date	Changes from previous
0.1	29/10/2021	Creation of document. Validation of general direction and table formats for inputs during the project meeting on 28/10/2021.
0.2	25/11/2021	Addition of more standards cards, introductory text.
1.0	14/01/2022	Chapter of references added. More standards cards added. Conclusion added. Structuring finalized. A couple of processes were found. Artificial Intelligence added. Summary explanation of the topics categorization added. Standards projects of interest added.

European Union funding

The CORAL project - of which this deliverable is a part - is Action no. 2020-LU-IA-0209, benefitting from European Union funding under the 2020 CEF Telecom Call[1].

The contents of this publication are the sole responsibility of the ANEC GIE and do not necessarily reflect the opinion of the European Union.

[1] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

Acronyms

Acronym	Full meaning
AES	Advanced Encryption Standard
AI	Artificial Intelligence
ANEC GIE	*Groupement d'Intérêt Economique Agence pour la Normalisation et l'Economie de la Connaissance*
ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information*
BITAG	Broadband Internet Technical Advisory Group
BSI	*Bundesamt für Sicherheit in der Informationstechnik*
CASES	Cyberworld Awareness and Security Enhancement Services
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CoAP	Constrained Application Protocol
CORAL	cybersecurity Certification based On Risk evALuation and treatment
CSA	Cybersecurity Act
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DDoS	Distributed Denial-of-Service
DNSSEC	Domain Name System Security Extensions
DTLS	Datagram TLS
EAL	Evaluation Assurance Level
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
ETSI ISG	ETSI Industry Specification Group
EUCC	Common Criteria based European cybersecurity certification scheme
EUCS	European Union Cybersecurity Certification Scheme for Cloud Services
FIPS	Federal Information Processing Standard
GSM	Global System for Mobile
GSMA	GSM Association
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICSA	International Computer Security Association
IEC	International Electrotechnical Commission
ILNAS	*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISG SAI	ETSI ISG Securing Artificial Intelligence
ISO	International Organization for Standardization
IT	Information Technology

ITU-T	International Telecommunications Union Telecommunication Standardization Sector
OEM	Original Equipment Manufacturer
OS	Operating System
OWASP	Open Web Application Security Project
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RBAC	Role-Based Access Control
RF	Radio Frequency
RoT	Root of Trust
SESIP	Security Evaluation Standard for IoT Platforms
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Universal Resource Locator
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

Contents

1. Introduction

The CORAL project

The *cybersecurity Certification based On Risk evALuation and treatment* (CORAL) research project (Action no. 2020-LU-IA-0209, benefitting from EU funding under the 2020 CEF Telecom Call[2]) aims to elaborate a toolkit and methodology to speed up the certification process in line with the Regulation (EU) 2019/881 (Cybersecurity Act - CSA)[3] in what concerns the self-certification and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with this act. In particular, this project will develop a light, efficient and straightforward evaluation method in line with the technical objectives of Article 51 of the CSA and based on risk assessments, to achieve a basic assurance level. This evaluation method will apply to SMEs that are in charge of ICT products, services or processes, acting in any sector. This method will also be used for conformity self-assessments, also possible with the entry into force of the CSA.

The project partners are:

- Cyberworld Awareness and Security Enhancement Services (CASES) / Security Made In Luxembourg *GIE*[4];
- The *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (ILNAS)[5] ; and
- The *Agence pour la normalisation et l'économie de la connaissance* (ANEC GIE)[6].

More information on the CORAL project and its partners can be found on the project website: https://coral-project.org/

Purpose and scope of this CORAL deliverable

The purpose of this deliverable is to compile a repository of categories of requirements or considerations from widely accepted published standards and guidelines to serve as a source of generic requirements and recommendations for basic levels of security in low-complexity and low-risk products, services and processes. It is a starting point for generating the afore-mentioned evaluation method. The leading CORAL partner in charge of this deliverable is the ANEC GIE.

Among the documents, methodologies, or projects surveyed, one finds for instance:

[2] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity
[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/eli/reg/2019/881/oj
[4] https://www.cases.lu/
[5] https://portail-qualite.public.lu/fr/acteurs/ilnas.html
[6] https://portail-qualite.public.lu/fr/acteurs/gie-anec.html

- International or European standards, such as those produced by ISO, IEC, ITU-T, CEN, CENELEC, and ETSI;
- Deliverables developed and managed by recognized fora and consortia, e.g. OWASP or GSMA;
- Deliverables developed by other well-known guideline-developing bodies, such as France's ANSSI or Germany's BSI.

The main characteristics of the scope of this document are 1) *applicability to products, services and processes*, 2) *genericity*, and 3) the *achievement of a basic level of security*.

Regarding the first, will be generally considered out of scope material that applies directly to the security of organizations themselves (e.g., ISO/IEC 27001). While it is indeed true that in some cases the security of an organization has an effect on the security of its delivered goods, it was largely observed for this state of the art that a) this is overwhelmingly the case for services (although it does happen for some products, e.g. in artificial intelligence) and b) in that case, the standards surveyed typically integrate organization-level guidance as an overall part of the service delivery already.

Regarding the second, while the aim is to remain as generic as possible, little of the existing material seems to fit this level of generality. Taking into account the overall exclusions adopted, a certain subcategorization of products and services appeared in the course of the drafting of this document:

- Products
    - Generic
    - Internet of Things
    - Web applications
    - Artificial Intelligence
- Services
    - Generic
    - Cloud
    - Telecommunications
- Processes

Little process-related material was found, so a subcategorization is not needed in this case. This categorization choice is largely driven by an ad-hoc evaluation of the perceived breadth of a class or domain (see the paragraph on Topic categorization for more details). In particular, topics deemed too narrow or specific are considered out of scope (e.g. requirements standards that apply only to smart meters, or to the service management of a specific virtual private network technology). Are also considered out of scope documentation that is not geared towards giving implementable requirements or guidelines or controls, such as penetration testing, or risk or vulnerability management specifications.

Finally, regarding the third characteristic, despite containing potentially important security requirements in their own right, certain vertical domains do not fit the profile of a "basic" level of security. Indeed, the target of this project is more precisely products, services or processes having low complexity and low risk with respect to the public. Thus, are generally out of scope documents pertaining to the security of

industrial automation and control systems, devices for healthcare, smart grid systems, the financial industry, critical infrastructures, etc.

Methodology followed

The starting point for the production of this document is the European Cyber Security Organisation's (ECSO) State of the Art Syllabus Overview of existing Cybersecurity standards and certification schemes v2, published in December 2017, see [1]. Additional searches were then made within ISO, IEC, ITU-T, CEN, CENELEC, ETSI, and other sources, on a more ad-hoc basis.

Topic categorization

The obtained topic categorization is largely due to the methodology followed. Some points that are worth noting are:

- First, for neither products, nor services, nor processes are there many completely generic frameworks to choose from, suggesting a gap that CORAL can fill;
- Secondly, the "products" category is very heavily dominated by Internet of Things (IoT) frameworks. This is not surprising, as the advent of the IoT – wherein nearly anything can be internetworked to share data and create new service and business opportunities – has created an entire ecosystem of extremely varied products that fit a need for baseline security, in particular in the case of the consumer market. Frameworks in this category tend to either cover the devices, or the devices and associated services, in which case these were placed in the "products" section. Very rarely will it be just associated services;
- Third, Artificial Intelligence (AI) is beginning to take flight in certain applications that fit the scope of this document (e.g. hotel recommendation systems). Accordingly, some considerations for baseline AI applications are considered here. The authors of this document categorized them more as products than services;
- Next, it is somewhat surprising that general low-risk, low-complexity software recommendations were not encountered. However, some guidelines exist in the particular case of web applications. Some may be applicable to the general case of software products;
- In the "services" category, the dominating topic is the provisioning of Cloud Computing services. This is in line with the fact that this market has grown considerably in recent years. Cloud services, depending on the application, will vary in complexity and risk;
- Finally, not many processes were found to fit the scope. This might be attributable to the fact that processes are more abstract in nature.

In any case, the categorization should not be viewed as a limitation. It is likely that the recommendations of a large sub-category of products, services, or processes can also serve as inspiration in a more generic case.

Important disclaimer

The present document makes no claims of originality. Indeed, most of the requirement categories are directly lifted from the surveyed documents, usually a table of contents or similar construct. The present document is also purely informative, and can in no way be used as a basis to comply to any of the described frameworks.

Structure

This document

Chapter 1. is this introduction. Next, Chapter 2. covers published standards or guidelines for products, regrouped by sub-class in the following order: Generic, Internet of Things, Web Applications, and Artificial Intelligence. Then, Chapter 3. covers published standards or guidelines for services, regrouped by sub-class in the following order: Generic, Cloud Computing, Internet of Things, and Telecommunications. Chapter 4. treats a few standards and guidelines for processes[7]. A few tables of ongoing international and European standardization projects, which may be relevant to the purpose of this document in the future, can be found in Chapter 5.. Finally, Chapter 6. concludes the document.

The description of the standards/guidelines themselves

Each published standard or guideline will be presented in the form of a table following the template in Table 1. The contents of each cell is described in the cell itself.

On one hand, presenting the information in this way has the following main advantage: cards are reasonably self-contained, in that categories of requirements are made immediately available. On the other hand, in some cases the document tends to introduce redundancy, particularly in cases where certain standards of interest have their categories of requirements presented/structured in nearly-identical ways (for instance, several standards presented repeat the structure of the ISO/IEC 27002:2013 standard). Our view is that cards being self-contained outweighs this disadvantage.

Name	
The official name of the resource, possibly including its version number. This might designate a document or a methodology, depending on the resource.	
Developing body	**Date of publication**
The name of the body (SDO, industrial forum, national entity, etc.) that develops and/or maintains the resource. There are sometimes multiple bodies outputting a joint publication.	*The date of publication of the resource in force.*
Type	**Applies to**
Requirements/guidelines/controls *OR* *Evaluation/ assessment/testing*	*An indication of whether the resource applies to products, services, or processes, and possibly an additional indication of a subcategory.*

[7] There are too few of these to create sub-classes.

Scope	
Either the official scope of the resource, or a description of it extracted from resource-related inputs.	
Relation to CSA	
An indication of whether the resource is cited in the context of the CSA. This is checked against the following available ENISA documentation: - *The "Cybersecurity Certification Market Study", from April 2021* [2]; - *The "Methodology for Sectoral Cybersecurity Assessments", from September 2021* [3]; - *The document on "Standardisation in Support of the Cybersecurity Certification", from December 2019* [4]; - *The document on "Advancing Software Security in the EU", from November 2019* [5]; - *The document on "Cybersecurity Certification EUCC", from May 2021* [6]; - *The "Public Consultation on the Draft Candidate EUCC Scheme", from May 2021* [7]; - *The document on "EUCS – Cloud Services Scheme", from December 2020* [8].	
Weblinks	**Accessibility**
Relevant weblinks, as much as possible directly to the resource itself.	*Whether the resource is available for free or not*
Specific relevance for CORAL	
A description of why the resource is deemed to have significance for the CORAL project's objectives, beyond the main characteristics already presented in the Introduction. In particular, whenever applicable, here is where a list of ***CATEGORIES OF*** *controls, requirements, recommendations, etc. found in the resource will be compiled. This list will in general* ***NOT*** *be the full list of actual requirements, to keep the present document reasonable in length. In some cases, e.g. when categories are not descriptive enough or when requirements lists are particularly short, the requirements themselves may actually be given.* *Most of the time, the categories listed are directly from the resource considered. However, it is convenient in certain cases for the authors of this document to come up with titles or summaries for requirements, in particular when these a) have no proposed title and b) are described in too much detail.* *The numbering used in presenting the lists of categories is usually that of the resource itself.* ***Other characteristics of interest to CORAL may also be listed here, on a case-by-case basis, for example, if a resource formulates questions, or if a resource already has some form of security level classification of requirements. Thus, in case a subset of control categories is considered relevant to the CORAL project's objectives for one such specific reason, those will be indicated in bold. However, this in no way means that control categories not in bold are automatically out of scope.*** *No attempt is made to either assess the level of security of a resource, or, when applicable, to compare the "basic" levels of security formulated across analyzed resources.*	

Table 1: Template for document/framework presentation

2. Products

Generic

The ISO/IEC 15408 series "Evaluation criteria for IT security" (Common Criteria)

Name	
ISO/IEC 15408 series of standards on Information technology — Security techniques — Evaluation criteria for IT security (also known as the "Common Criteria for Information Technology Evaluation" series)	
Developing body	**Date of publication**
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	*Part 1: 01/2014 (corrected version)* *Part 2: 05/2011 (corrected version)* *Part 3: 05/2011 (corrected version)*
Type	**Applies to**
Requirements/guidelines/controls	*Products: generic*
Scope	
"ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software." – Introduction, p. vi, of [9] *Part 1* [9] *is the general model.* *Part 2* [10] *list the security functional components.* *Part 3* [11] *list the security assurance components.* *At the time of writing of this deliverable, the identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organizations. See the weblinks below.* *Note also that at the time of writing of this deliverable, Parts 1, 2, and 3 are under revision, and in FDIS stage.*	
Relation to CSA	
This series of standards is the foundation of the first certification scheme – the EUCC scheme proposed as an update of the SOG-IS framework, see [6] - proposed by ENISA under the CSA framework, covering the "substantial" and "high" levels of assurance.	
Weblinks	**Accessibility**
ISO: https://www.iso.org/standard/50341.html (Part 1) *https://www.iso.org/standard/46414.html (Part 2)* *https://www.iso.org/standard/46413.html (Part 3)* *https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (search for "15408")* *CC portal: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf*	*Free*
Specific relevance for CORAL	
Part 1 [9] *is the general model of the standards series.*	

Parts 2 [10] and 3 [11] contain literal lists of security functional and assurance components, from which CORAL security questions can certainly be engineered. We detail these below, beginning with the assurance components, since these come equipped with a security level classification.

Part 3 lists Security Assurance Components. There are 8 classes subdivided into families, and each family is further subdivided into components. Two of these classes pertain to the verification of the correct usage of the standards' formal constructs in relation to the product in question. These are the class APE: Protection Profile evaluation and the class ASE: Security Target evaluation. Another of the classes pertains to conditions under which assurance of a product composed of other "sub-products" may be deduced from these other products' own assurance. This is the class ACO: Composition. The remaining six classes pertain to technical considerations.

The three classes APE, ASE and ACO are considered out of scope for low-level, low-risk security products, which ideally would not need protection profiles or security targets, and whose evaluation should be simple to do directly.

Furthermore, the candidate EUCC scheme already maps assurance level "substantial" to the 15408 series' Evaluation Assurance Level (EAL) 1, which is the lowest possible EAL. Therefore, logically, anything that could potentially correspond to a "low" level of assurance in this framework is necessarily weaker than EAL 1.

Consequently, assurance components from APE, ASE, or ACO are not included in the following list, and only those that appear in EAL 1 are in bold.

- ***11 Class ADV: Development***
  - *11.1 Security Architecture (ADV_ARC)*
    - *11.1.4 ADV_ARC.1 Security architecture description*
  - ***11.2 Functional specification (ADV_FSP)***
    - ***11.2.4 ADV_FSP.1 Basic functional specification***
    - *11.2.5 ADV_FSP.2 Security-enforcing functional specification*
    - *11.2.6 ADV_FSP.3 Functional specification with complete summary*
    - *11.2.7 ADV_FSP.4 Complete functional specification*
    - *11.2.8 ADV_FSP.5 Complete semi-formal functional specification with additional error information*
    - *11.2.9 ADV_FSP.6 Complete semi-formal functional specification with additional formal specification*
  - *11.3 Implementation representation (ADV_IMP)*
    - *11.3.4 ADV_IMP.1 Implementation representation of the TSF*
    - *11.3.5 ADV_IMP.2 Complete mapping of the implementation representation of the TSF*
  - *11.4 TSF internals (ADV_INT)*

- *11.4.4 ADV_INT.1 Well-structured subset of TSF internals*
- *11.4.5 ADV_INT.2 Well-structured internals*
- *11.4.6 ADV_INT.3 Minimally complex internals*

o *11.5 Security policy modelling (ADV_SPM)*

- *11.5.4 ADV_SPM.1 Formal TOE security policy model*

o *11.6 TOE design (ADV_TDS)*

- *11.6.4 ADV_TDS.1 Basic design*
- *11.6.5 ADV_TDS.2 Architectural design*
- *11.6.6 ADV_TDS.3 Basic modular design*
- *11.6.7 ADV_TDS.4 Semiformal modular design*
- *11.6.8 ADV_TDS.5 Complete semiformal modular design*
- *11.6.9 ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation*

- ***12 Class AGD: Guidance documents***
  - ***12.1 Operational user guidance (AGD_OPE)***
    - ***12.1.4 AGD_OPE.1 Operational user guidance***
  - ***12.2 Preparative procedures (AGD_PRE)***
    - ***12.2.4 AGD_PRE.1 Preparative procedures***
- ***13 Class ALC: Life-cycle support***
  - ***13.1 CM capabilities (ALC_CMC)***
    - ***13.1.4 ALC_CMC.1 Labelling of the TOE***
    - *13.1.5 ALC_CMC.2 Use of a CM system*
    - *13.1.6 ALC_CMC.3 Authorisation controls*
    - *13.1.7 ALC_CMC.4 Production support, acceptance procedures and automation*
    - *13.1.8 ALC_CMC.5 Advanced support*
  - ***13.2 CM scope (ALC_CMS)***
    - ***13.2.4 ALC_CMS.1 TOE CM coverage***
    - *13.2.5 ALC_CMS.2 Parts of the TOE CM coverage*
    - *13.2.6 ALC_CMS.3 Implementation representation CM coverage*
    - *13.2.7 ALC_CMS.4 Problem tracking CM coverage*
    - *13.2.8 ALC_CMS.5 Development tools CM coverage*
  - *13.3 Delivery (ALC_DEL)*
    - *13.3.4 ALC_DEL.1 Delivery procedures*
  - *13.4 Development security (ALC_DVS)*
    - *13.4.4 ALC_DVS.1 Identification of security measures*
    - *13.4.5 ALC_DVS.2 Sufficiency of security measures*
  - *13.5 Flaw remediation (ALC_FLR)*
    - *13.5.4 ALC_FLR.1 Basic flaw remediation*
    - *13.5.5 ALC_FLR.2 Flaw reporting procedures*
    - *13.5.6 ALC_FLR.3 Systematic flaw remediation*
  - *13.6 Life-cycle definition (ALC_LCD)*

- *13.6.4 ALC_LCD.1 Developer defined life-cycle model*
- *13.6.5 ALC_LCD.2 Measurable life-cycle model*

o *13.7 Tools and techniques (ALC_TAT)*

- *13.7.4 ALC_TAT.1 Well-defined development tools*
- *13.7.5 ALC_TAT.2 Compliance with implementation standards*
- *13.7.6 ALC_TAT.3 Compliance with implementation standards - all parts*

- ***14 Class ATE: Tests***

o *14.1 Coverage (ATE_COV)*

- *14.1.4 ATE_COV.1 Evidence of coverage*
- *14.1.5 ATE_COV.2 Analysis of coverage*
- *14.1.6 ATE_COV.3 Rigorous analysis of coverage*

o *14.2 Depth (ATE_DPT)*

- *14.2.4 ATE_DPT.1 Testing: basic design*
- *14.2.5 ATE_DPT.2 Testing: security enforcing modules*
- *14.2.6 ATE_DPT.3 Testing: modular design*
- *14.2.7 ATE_DPT.4 Testing: implementation representation*

o *14.3 Functional tests (ATE_FUN)*

- *14.3.4 ATE_FUN.1 Functional testing*
- *14.3.5 ATE_FUN.2 Ordered functional testing*

o ***14.4 Independent testing (ATE_IND)***

- ***14.4.4 ATE_IND.1 Independent testing - conformance***
- *14.4.5 ATE_IND.2 Independent testing - sample*
- *14.4.6 ATE_IND.3 Independent testing - complete*

- ***15 Class AVA: Vulnerability assessment***

o ***15.2 Vulnerability analysis (AVA_VAN)***

- ***15.2.3 AVA_VAN.1 Vulnerability survey***
- *15.2.4 AVA_VAN.2 Vulnerability analysis*
- *15.2.5 AVA_VAN.3 Focused vulnerability analysis*
- *15.2.6 AVA_VAN.4 Methodical vulnerability analysis*
- *15.2.7 AVA_VAN.5 Advanced methodical vulnerability analysis*

Part 2 list Security Functional Components. There are 11 classes subdivided into families, and each family is further subdivided into components. Here, no particular effort is placed into "pre-flagging" components for a "low" level, as this depends too much on the target product. Thus, all of the security functional components ought to be considered, on a product-by-product basis. Furthermore, the standards series does not provide any form of mapping between assurance components and functional components. (When defining a security target, one has to specify a security requirements rationale that traces chosen SFRs to security objectives, and also that explains why a particular set of SACs was chosen. But there are no particular requirements for this, see Clause A.9.3 of [9]*.)*

- *7 Class FAU: Security audit*

o *7.1 Security audit automatic response (FAU_ARP)*

- *14.11 Inter-TSF TSF data consistency (FPT_TDC)*
  - *14.11.5 FPT_TDC.1 Inter-TSF basic TSF data consistency*
- *14.12 Testing of external entities (FPT_TEE)*
  - *14.12.5 FPT_TEE.1 Testing of external entities*
- *14.13 Internal TOE TSF data replication consistency (FPT_TRC)*
  - *14.13.5 FPT_TRC.1 Internal TSF consistency.*
- *14.14 TSF self test (FPT_TST)*
  - *14.14.5 FPT_TST.1 TSF testing*

- *15 Class FRU: Resource utilisation*
  - *15.1 Fault tolerance (FRU_FLT)*
    - *15.1.6 FRU_FLT.1 Degraded fault tolerance*
    - *15.1.7 FRU_FLT.2 Limited fault tolerance*
  - *15.2 Priority of service (FRU_PRS)*
    - *15.2.5 FRU_PRS.1 Limited priority of service*
    - *15.2.6 FRU_PRS.2 Full priority of service*
  - *15.3 Resource allocation (FRU_RSA)*
    - *15.3.6 FRU_RSA.1 Maximum quotas*
    - *15.3.7 FRU_RSA.2 Minimum and maximum quotas*
- *16 Class FTA: TOE access*
  - *16.1 Limitation on scope of selectable attributes (FTA_LSA)*
    - *16.1.5 FTA_LSA.1 Limitation on scope of selectable attributes*
  - *16.2 Limitation on multiple concurrent sessions (FTA_MCS)*
    - *16.2.6 FTA_MCS.1 Basic limitation on multiple concurrent sessions*
    - *16.2.7 FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions*
  - *16.3 Session locking and termination (FTA_SSL)*
    - *16.3.10 FTA_SSL.1 TSF-initiated session locking*
    - *16.3.11 FTA_SSL.2 User-initiated locking*
    - *16.3.12 FTA_SSL.3 TSF-initiated termination*
    - *16.3.13 FTA_SSL.4 User-initiated termination*
  - *16.4 TOE access banners (FTA_TAB)*
    - *16.4.5 FTA_TAB.1 Default TOE access banners*
  - *16.5 TOE access history (FTA_TAH)*
    - *16.5.5 FTA_TAH.1 TOE access history*
  - *16.6 TOE session establishment (FTA_TSE)*
    - *16.6.5 FTA_TSE.1 TOE session establishment*
- *17 Class FTP: Trusted path/channels*
  - *17.1 Inter-TSF trusted channel (FTP_ITC)*
    - *17.1.5 FTP_ITC.1 Inter-TSF trusted channel*
  - *17.2 Trusted path (FTP_TRP)*
    - *17.2.5 FTP_TRP.1 Trusted path*

Note that a related standard on evaluation methodology following the 15408 framework also exists: ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation [12].

ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications

Name	
ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications	
Developing body	**Date of publication**
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	*10/2017*
Type	**Applies to**
Requirements/guidelines/controls	*Products: generic, systems, applications*
Scope	
"ISO/IEC TS 19249:2017 provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications together with guidance on how to use those principles effectively. *ISO/IEC TS 19249:2017 gives guidelines for the development of secure products, systems and applications including a more effective assessment with respect to the security properties they are supposed to implement.* *ISO/IEC TS 19249:2017 does not establish any requirements for the evaluation or the assessment process or implementation." – Scope of* [13]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.iso.org/standard/64140.html	*Not free*
Specific relevance for CORAL	
This is a set of principles to follow in order to architect and design secure products, systems or applications. For each principle, is stated: - *how it may be implemented,* - *how it contributes to security, and* - *how it may aid in assessing the product's security.* *Links to the ISO/IEC 15408 series of standards are also made.* *Since CORAL aims to create a set of security questions in a rather generic way, the list of design principles and the manner in which they may support security assessment can be useful. The architecting principles are:*	

- *domain separation,*
- *layering,*
- *encapsulation,*
- *redundancy, and*
- *virtualization.*

The design principles are:

- *least privilege,*
- *attack surface minimization,*
- *centralized parameter validation,*
- *centralized general security services, and*
- *preparing for error and exception handling.*

Internet of Things products

ETSI EN 303 645 V2.1.1 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

Name	
ETSI EN 303 645 V2.1.1 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements	
Developing body	**Date of publication**
ETSI TC CYBER (Cybersecurity)	*06/2020*
Type	**Applies to**
Requirements/guidelines/controls	*Products: Consumer IoT*
Scope	
"The present document specifies high-level security and data protection provisions for consumer IoT devices that are connected to network infrastructure (such as the Internet or home network) and their interactions with associated services. The associated services are out of scope. […] *Moreover, the present document addresses security considerations specific to constrained devices.* *[…]* *The present document provides basic guidance through examples and explanatory text for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions. […]* *Devices that are not consumer IoT devices, for example those that are primarily intended to be used in manufacturing, healthcare or other industrial applications, are not in scope of the present document.* *The present document has been developed primarily to help protect consumers, however, other users of consumer IoT equally benefit from the implementation of the provisions set out here.* *[…]" – Extract of scope of* [14]	
Relation to CSA	

The standard is viewed, in ENISA's publication [4], as a "basis for [...] cybersecurity evaluation" in the overall context of the CSA.

Weblinks	**Accessibility**
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf *https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf*	*Free*

Specific relevance for CORAL

The technical content of this EN is identical to the technical content of the ETSI TS 103 645 V2.1.2 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements [15], *per Annex C of* [15].

This document provides fundamental security requirements for IoT devices that are suitable for general consumers. Thus, one can expect there being generally a low level of risk and complexity in the devices covered. While the document is more geared towards device manufacturers, it can still use it as a checklist of requirements, and a good source of security questions.
Note that only devices are covered, as well as their interactions with services, but the associated services are out of scope.
The document organizes its requirements as provisions that are regrouped under Chapter 5 per subsection. The subsections covered are:

- *No universal default passwords;*
- *Implement a means to manage reports of vulnerabilities;*
- *Keep software updated;*
- *Securely store sensitive security parameters;*
- *Communicate securely;*
- *Minimize exposed attack surfaces;*
- *Ensure software integrity;*
- *Ensure that personal data is secure;*
- *Make systems resilient to outages;*
- *Examine system telemetry data;*
- *Make it easy for users to delete user data;*
- *Make installation and maintenance of devices easy;*
- *Validate input data.*

(Chapter 6 is dedicated to a few provisions on device user data protection.)

Note that related to this document is also the ETSI standard ETSI TS 103 701 V1.1.1 (2021-08) CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements [16], *which specifies test scenarios to use in assessing whether a device is conform to* [14]. *This document also structures its test scenarios following the subsections listed above.*

ICSA Internet of Things (IoT) Security Testing Framework v2.01

Name	
ICSA Internet of Things (IoT) Security Testing Framework v2.01	
Developing body	**Date of publication**
ICSA	*14/07/2021*
Type	**Applies to**
Evaluation/ assessment/testing	*Products: IoT*

Scope

The document presents a framework for developing security testing requirements for IoT products. A product in this case designates more than just the IoT device. Indeed, to quote the introduction of [17], "[…] IoT security controls need to go beyond those provided by the IoT device itself. For this reason, […] IoT security certification testing is aimed at both unique classes of IoT devices and their relevant component parts.
An IoT device's component parts potentially include the communication between it and other things as well as a potentially varied set of interfaces through which users and/or other "things" interact with it and/or its data."

Relation to CSA

No direct relation.

Weblinks	**Accessibility**
https://www.icsalabs.com/technology-program/iot-devices-sensors/iot-device-requirements-framework *https://www.icsalabs.com/sites/default/files/ICSALABS_IoT_reqts_framework_v2.01_210714.pdf*	*Free*

Specific relevance for CORAL

This document, is to be used as "a starting point when developing specific, testable requirement sets" for a given IoT product. It lists categories of "potential IoT product requirements". The document has the advantage of being very compact, which lends to flexibility and ease of use. Indeed, there are a total of 6 categories of requirements, with each containing between 3 and 9 generic requirements. The categories are listed below.

- *A. Cryptography;*
- *B. Communications;*
- *C. Authentication;*
- *D. Physical security;*
- *E. Platform security;*
- *F. Alerting/logging.*

BITAG Internet of Things (IoT) Security and Privacy Recommendations

Name
BITAG Internet of Things (IoT) Security and Privacy Recommendations

Developing body	Date of publication
BITAG	*11/2016*
Type	**Applies to**
Requirements/guidelines/controls	*Products: IoT*

Scope

The document gives a set of high-level recommendations as proposed fixes for the observed lack of security in the IoT device landscape. According to the executive summary of [18], it more particularly targets "consumer-oriented devices and their associated local and remote software systems, though some or all of" the "recommendations may be more broadly applicable. This report is concerned with scenarios where consumers are installing, configuring, and administering devices that they lease or own."

Relation to CSA

No direct relation.

Weblinks	Accessibility
https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php *https://www.bitag.org/index.php*	*Free*

Specific relevance for CORAL

As the report targets primarily consumer IoT, it is reasonable to assume that basic security is the objective.

The report lists its recommendations in categories. The recommendation categories are listed below. Some also have subcategories.

- *7.1 IoT Devices Should Use Best Current Software Practices*
  - *IoT Devices Should Ship with Reasonably Current Software*
  - *IoT Devices Should Have a Mechanism for Automated, Secure Software*
  - *Updates*
  - *IoT Devices Should Use Strong Authentication by Default*
  - *IoT Device Configurations Should Be Tested and Hardened*
- *7.2 IoT Devices Should Follow Security & Cryptography Best Practices*
  - *Encrypt Configuration (Command & Control) Communications By Default*
  - *Secure Communications To and From IoT Controllers*
  - *Encrypt Local Storage of Sensitive Data*
  - *Authenticate Communications, Software Changes, and Requests for Data*
  - *Use Unique Credentials for Each Device*
  - *Use Credentials That Can Be Updated*
  - *Close Unnecessary Ports and Disable Unnecessary Services*
  - *Use Libraries That Are Actively Maintained and Supported*
- *7.3 IoT Devices Should Be Restrictive Rather Than Permissive in Communicating*
- *7.4 IoT Devices Should Continue to Function if Internet Connectivity is Disrupted*

- *7.5 IoT Devices Should Continue to Function If the Cloud Back-End Fails*
- *7.6 IoT Devices Should Support Addressing and Naming Best Practices*
  - *IPv6*
  - *DNSSEC*
- *7.7 IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand*
- *7.8 Disclose Rights to Remotely Decrease IoT Device Functionality*
- *7.9 The IoT Device Industry Should Consider an Industry Cybersecurity Program*
- *7.10 The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues*
  - *privacy policy*
  - *reset mechanism*
  - *bug reporting system*
  - *secure software supply chain*
  - *support for an IoT device throughout the course of its lifespan*
  - *clear methods for consumers to determine who they can contact for support and methods to contact consumers*
  - *report discovery and remediation of software vulnerabilities*
  - *vulnerability reporting process*

GSMA IoT Security Guidelines for Endpoint Ecosystems v2.2

Name	
GSMA IoT Security Guidelines for Endpoint Ecosystems v2.2	
Developing body	**Date of publication**
GSMA	*29/02/2020*
Type	**Applies to**
Requirements/guidelines/controls	*Products: IoT*
Scope	
From the introduction of [19]: "This document is one part of a set of [...] security guideline documents that are intended to help the nascent "Internet of Things" (IoT) industry establish a common understanding of IoT security issues. The set of non-binding guideline documents promotes methodology for developing secure IoT Services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT Services." *The particular document at hand is targeted towards the elements of the "endpoint ecosystem", that is the devices themselves.*	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.gsma.com/ *https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/*	*Free*
Specific relevance for CORAL	

The recommendations are categorized as critical, high-priority, medium-priority, and low-priority. ***According to the framework, only the critical recommendations are to be implemented in all cases. Thus, these can be reasonably interpreted as providing a baseline model of security, and hence are in bold.*** *The other recommendations are also listed, as baseline security will inevitably vary according to the specific product ("endpoint") considered.*

- *8.2 Disable Debugging and Testing Technologies*
- *8.3 Tainted Memory via Peripheral-Based Attacks*
- *8.4 User Interface Security*
- *8.5 Third Party Code Auditing*
- *8.6 Utilize a Private APN*
- *8.7 Implement Environmental Lock-Out Thresholds*
- *8.8 Enforce Power Warning Thresholds*
- *8.9 Environments Without Back-End Connectivity*
- *8.10 Device Decommissioning and Sunsetting*
- *8.11 Unauthorized Metadata Harvesting*

- *9 Low Priority Recommendations*
  - *9.1 Intentional and Unintentional Denial of Service*
  - *9.2 Safety Critical Analysis*
  - *9.3 Defeating Shadowed Components and Untrusted Bridges*
  - *9.4 Defeating a Cold Boot Attack*
  - *9.5 Non-Obvious Security Risks (Seeing Through Walls)*
  - *9.6 Combating Focused Ion Beams and X-Rays*
  - *9.7 Consider Supply Chain Security*
  - *9.8 Lawful Interception*

Note that this guideline is part of an overall package of guidelines from GSMA, where another part covers IoT services. See the corresponding card for GSMA IoT Security Guidelines for IoT Service Ecosystems v2.2 in this document.

IoT Security Assurance framework v3.0

Name	
IoT Security Assurance framework v3.0	
Developing body	**Date of publication**
IoT Security Foundation	*11/2021*
Type	**Applies to**
Requirements/guidelines/controls	*Products: IoT* *Services: IoT*

Scope

"The scope of this document includes (but is not limited to):

- *Business processes*
- *The "Things" in IoT, i.e. network connected products and/or devices*
- *Aggregation points such as gateways and hubs that form part of the connectivity*
- *Networking including wired, and radio connections, cloud and server elements." – Scope, p. 5 of* [20]

While the framework can be used by many different IoT stakeholders, its main aim appears to be to

help build secure IoT devices and develop secure IoT apps and services. Thus, while a large part of the framework is devoted to devices, some are more geared towards IoT service management and business management.

Relation to CSA

No direct relation.

Weblinks	**Accessibility**
https://www.iotsecurityfoundation.org/ *https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf*	*Free*

Specific relevance for CORAL

This document specifies an assurance framework that holistically covers IoT device production and IoT service provisioning. Thus, while this card was placed in the "products" category, there are bit applicable to services.

The assurance framework is organized first in "Assurance applicability" clauses. Then, each clause is subdivided into requirements. Five classes of assurance are specified in increasing order of required security, from assurance level Class 0 "where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organisation" to assurance level Class 4 "[…] where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury". Class 1 corresponds to "where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organisation". (See Section 2.2 of [20].) ***Thus, for the purpose of this document, the authors of the present document believe that low-complexity and low-risk can be reasonably assigned to Class 0 or Class 1.***

In** [20]**, the requirements are directly described rather than being named. Thus, the authors of the present document have devised shorter summaries for each requirement, in order to flag those that are required for Class 0 ("Mandatory for all classes") or Class 1 ("Mandatory for Class 1 and above"). Accordingly, these are in bold.

- ***2.4.3 Assurance Applicability – Business Security Processes, Policies and Responsibilities***
  - ***2.4.3.1 Accountability assignment of product/service security***
  - ***2.4.3.2 Accountability assignment to compliance framework***
  - *2.4.3.3 Intentionally left blank to maintain requirement numbering -*
  - ***2.4.3.4 Follow standard cybersecurity recommendations***
  - ***2.4.3.5 Policy for interacting with security researcher(s)***
  - ***2.4.3.5.1 Public availability of this policy, contact information, and interaction timelines***
  - *2.4.3.6 Policy for addressing security risks as part of product/service development and support*
  - ***2.4.3.7 Process for vulnerability disclosure***

- o ***2.4.3.8 Process for executive briefing on vulnerabilities/security breaches***
- o ***2.4.3.9 Process for security notifications to customers***
- o ***2.4.3.9.1 Minimum support period for security updates***
- o ***2.4.3.10 A security threat and risk assessment implemented before product/service design***
- o ***2.4.3.11 Contact information/web page for vulnerability disclosure reporting***
- o ***2.4.3.12 Security email address/online page for vulnerability disclosure communications***
- o ***2.4.3.13 Process for conflict resolution for vulnerability disclosures***
- o ***2.4.3.14 Publish the organization's conflict resolution process for vulnerability disclosures***
- o ***2.4.3.16 Develop security advisory notification steps***
- o *2.4.3.17 Compliance of the security policy with ISO 30111 or a similar standard*
- o *2.4.3.18 Process to notify operators of connected components and system management of impending downtime for updates*
- o *2.4.3.19 Accountability assignment of product/service security for each domain involved in any system or device update process*
- o *2.4.3.20 Responsibility is allocated for control, logging and auditing of the update process*
- o ***2.4.3.21 Raise security issues***
- o *2.4.3.22 Process for validating "updates" and updating devices*
- o ***2.4.3.22.1 Users must have the ability to disable updating***
- o *2.4.3.23 Assessing the security update policy for devices with a constrained power source*
- o *2.4.3.24 Assessing responsibility for third party supplied components used in the product*
- o *2.4.3.25 Transparent and auditable policy for remote software upgrade to fix vulnerabilities*
- o ***2.4.3.26 Process for maintaining a central inventory of third-party components and services, and their suppliers, for each product***
- o ***2.4.3.27 Define the manner to establish and assess security requirements on third party components***
- o ***2.4.3.28 Awarding a higher score to the supplier implementing a secure design***
- o ***2.4.3.29 Retain an enduring competency to revisit and act upon such information during product upgrades or in the event of a potential vulnerability being identified***

- ***2.4.4 Assurance Applicability – Device Hardware & Physical Security***
  - o ***2.4.4.1 The product's processor system has an irrevocable hardware Secure Boot process***

- *2.4.4.2 The product's processor system has an irrevocable "Trusted Root Hardware Secure Boot"*
- *2.4.4.3 Secure boot*
- ***2.4.4.4 The Secure Boot process is enabled by default***
- ***2.4.4.5 Any debug interface communicates with authorized and authenticated entities***
- ***2.4.4.6 The hardware incorporates protection against tampering***
- *2.4.4.7 Reduce the attack surface by incorporating physical, electrical and logical protection against tampering*
- *2.4.4.8 The hardware incorporates physical, electrical & logical protection against reverse engineering*
- ***2.4.4.9 Securing all communications port(s)***
- *2.4.4.10 All the product's development test points are securely disabled or removed*
- *2.4.4.11 Tamper Evident measures have been used to identify any interference*
- *2.4.4.12 Intentionally left blank to maintain requirement numbering*
- ***2.4.4.13 Encrypting the separate non-volatile memory device***
- ***2.4.4.14 Cryptographic pairing of storage and processor when the product's credential/key storage is external to its processor***
- ***2.4.4.15 Resetting the device in the event of any unauthorized attempts***
- ***2.4.4.16 Where the product has a hardware source for generating true random numbers, it is used for all relevant cryptographic operations***
- *2.4.4.17 The product shall have a hardware source for generating true random numbers*
- *2.4.4.18 Control access to memory to reduce the risk of running malicious code*

- ***2.4.5 Assurance Applicability – Device Software***
  - ***2.4.5.1 Prevent unauthorized and unauthenticated software, configurations and files***
  - ***2.4.5.2 Software images must be digitally signed by an appropriate signing authority***
  - ***2.4.5.3 Software update package has its digital signature, signing certificate and signing certificate chain***
  - *2.4.5.4 software images shall be encrypted for a remote software upgrade*
  - *2.4.5.5 Access control to the product's virtual port(s) that are not required for normal operation, if any*
  - ***2.4.5.6 Watchdog timers must be enabled***
  - ***2.4.5.7 The product's software signing root of trust is stored in tamper-resistant memory***
  - *2.4.5.8 Only authorized entities can restore a software to an earlier secure version*

- ***2.4.5.9 There are measures to prevent the installation of non-production software onto production devices***
- ***2.4.5.10 Prevent accidental release of superfluous data by removing unnecessary debug information***
- *2.4.5.11 Switch off the debug functionality when the software is operated outside the trusted environment*
- *2.4.5.12 Protect the product's software from sensitive information leakage*
- *2.4.5.13 The product's software source code follows the basic good practice of a Language subset coding standard*
- *2.4.5.14 The product's software source code follows the basic good practice of static vulnerability analysis by the developer*
- ***2.4.5.15 The software must be architected to identify and ring fence sensitive software components***
- ***2.4.5.16 The source code of the software follows defined repeatable processes***
- *2.4.5.17 Toolchain used to compile the application is run with controlled and auditable access*
- *2.4.5.18 the integrity of toolchain used to create the software is validated regularly*
- ***2.4.5.19 Production software signing keys are under access control***
- ***2.4.5.20 The production software signing keys are stored and secured in a storage device compliant to FIPS-140-2/FIPS-140-3 level 2, or equivalent or higher standard***
- *2.4.5.21 Certificate pinning is used when the device communicates over TCP/IP or UDP/IP*
- ***2.4.5.22 A replacement strategy must be communicated to the user for a device with no possibility of a software update***
- *2.4.5.23 All inputs and outputs are checked for validity*
- *2.4.5.24 The software has been designed to meet the safety requirements identified in the risk assessment*
- ***2.4.5.25 Support for partially installing updates is provided for devices whose on-time is insufficient for the complete installation of a whole update***
- ***2.4.5.26 Support for partially downloading updates is provided for devices whose network access is limited or sporadic***
- ***2.4.5.27 Where real-time expectations of performance are present, update mechanisms must not interfere with meeting these expectations***
- ***2.4.5.28 Where a device doesn't support secure boot, the user data and credentials should be re-initialized***
- ***2.4.5.29 Only a local update by a physically present user is permitted when device cannot verify authenticity of updates***
- ***2.4.5.30 An update to a device must be authenticated before it is installed***

- *o 2.4.5.31 Withdrawn as duplicate requirement*
- ***o 2.4.5.32 There is secure provisioning of cryptographic keys for updates during manufacture in accordance with industry standards***
- *o 2.4.5.33 Memory locations used to store sensitive material are sanitized as soon as possible after they are no longer needed*
- *o 2.4.5.34 Any caches which potentially store sensitive material are cleared flushed after memory locations containing sensitive material have been sanitized*
- ***o 2.4.5. An end-of-life policy shall be published which explicitly states the minimum length of time for which a device will receive software***
- ***o 2.4.5.36 Updates should be provided for a period appropriate to the device***
- *o 2.4.5.37 The device manufacturer should ensure that shared libraries that deliver network and security functionalities have been evaluated*
- *o 2.4.5.38 Maintenance changes should trigger full security regression testing*
- *o 2.4.5.39 IoT devices must allow software updates to maintain security over the product lifetime*
- ***o 2.4.5.40 Hard-coded critical/ security parameters in device software source code shall not be used; if needed these should be injected in a secure process***
- *o* ***2.4.5.41 The device should check if security updates are available, either autonomously or as part of the support service***

- ***2.4.6 Assurance Applicability – Device Operating System***
  - *o 2.4.6.1 The OS is implemented with relevant security updates prior to release*
  - *o 2.4.6.2 Intentionally left blank to maintain requirement numbering*
  - ***o 2.4.6.3 All unnecessary accounts or logins have been disabled or eliminated from the software at the end of the software development process***
  - ***o 2.4.6.4 Files, directories and persistent data are set to minimum access privileges required to correctly function***
  - ***o 2.4.6.5 Security parameters and passwords should not be hard-coded into source code or stored in a local file***
  - ***o 2.4.6.6 All OS non-essential services have been removed from the product's software, image or file systems***
  - ***o 2.4.6.7 All OS command line access to the most privileged accounts has been removed from the OS***
  - ***o 2.4.6.8 Essential kernel, services or functions are prevented from being called by unauthorized external product***
  - ***o 2.4.6.9 All software is operated at the least privilege level possible and only has access to the resources needed***
  - ***o 2.4.6.10 All the applicable security features supported by the OS are enabled***
  - ***o 2.4.6.11 The OS is separated from the application(s) and is only accessible via***

defined secure interfaces

- *2.4.6.12 The OS implements a separation architecture to separate trusted from untrusted applications*
- *2.4.6.13 The product's OS kernel is designed such that each component runs with the least security privilege required and the minimum functionality needed*
- ***2.4.6.14 Cryptographic algorithms, primitives, libraries and protocols should be updateable to address any vulnerabilities***
- ***2.4.6.15 As per 2.4.10.5, the user interface is protected by an automatic session idle logout timeout function***

- ***2.4.7 Assurance Applicability – Device Wired and Wireless Interfaces***
  - ***2.4.7.1 The product prevents unauthorized connections to it or other devices the product is connected to***
  - ***2.4.7.2 The network component and firewall configuration has been reviewed and documented for the required/defined secure behavior***
  - ***2.4.7.3 Forwarding functions should be blocked to prevent bridging of security domains***
  - ***2.4.7.4 Devices support only the versions of application layer protocols that have been reviewed***
  - ***2.4.7.5 the device should alert the user/administrator if an unauthorized change is detected***
  - ***2.4.7.6 All the product's unused ports are closed and only the necessary ones are active***
  - ***2.4.7.7 Password is unique to each device***
  - ***2.4.7.8 Where using initial pairing process, a Strong Authentication shall be used***
  - ***2.4.7.9 Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password***
  - ***2.4.7.10 For any Wi-Fi connection, WPA-2 AES or a similar strength encryption has been used***
  - ***2.4.7.11 Where WPA-2 WPS is used it has a unique and random key per device***
  - ***2.4.7.12 All network communications keys are stored securely, in accordance with industry standards***
  - ***2.4.7.13 Where a TCP protocol is used, it is protected by a TLS connection with no known vulnerabilities***
  - ***2.4.7.14 Where a UDP protocol is used, such as CoAP, it is protected by a DTLS connection with no known vulnerabilities.***
  - ***2.4.7.15 All cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A or OWASP***
  - ***2.4.7.16 All use of cryptography by the product shall be listed and validated against the import/export requirements***

- *o 2.4.7.17 Where there is a loss of communications or availability it shall not compromise the local integrity of the device*
- *o 2.4.7.18 Enable only the services necessary for the product's operation*
- *o 2.4.7.19 Communications protocols should be latest versions*
- *o 2.4.7.20 Post product launch, communications protocols should be reviewed throughout the product life cycle against publicly known vulnerabilities*
- *o 2.4.7.21 If a factory reset is made, the device should warn that secure operation may be compromised until updated*
- *o 2.4.7.22 Where RF communications are enabled, antenna power is configured to limit ability of mapping assets*
- *o 2.4.7.23 Protocol anonymity features are enabled in protocols (e.g., Bluetooth) to limit location tracking capabilities*
- *o 2.4.7.24 Devices should remain operating and locally functional in the case of a loss of network connection*
- *o 2.4.7.25 Following restoration of power or network connection, devices should be able to return to a network in a sensible state and in an orderly fashion*

- *2.4.8 Assurance Applicability – Authentication and Authorization*
  - *o 2.4.8.1 The product contains a unique and tamper-resistant device identifier*
  - *o 2.4.8.2 Where the product has a secure source of time there is a method of validating its integrity*
  - *o 2.4.8.3 The factory issued or reset password is randomly unique for every device in the product family*
  - *o 2.4.8.4 The product does not accept the use of null or blank passwords*
  - *o 2.4.8.5 The product will not allow new passwords containing the user account name*
  - *o 2.4.8.6 Password entry follows industry standard practice*
  - *o 2.4.8.7 The product has defense against brute force repeated login attempts*
  - *o 2.4.8.8 The product securely stores any passwords using an industry standard cryptographic algorithm*
  - *o 2.4.8.9 The product supports access control to restrict access to sensitive information*
  - *o 2.4.8.10 The access control privileges are defined, justified and documented*
  - *o 2.4.8.11 The product only allows controlled user account access*
  - *o 2.4.8.12 The product allows the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned*
  - *o 2.4.8.13 The product supports having any or all of the factory default user login passwords altered when installed or commissioned*
  - *o 2.4.8.14 If the product has a password recovery or reset mechanism, an assessment has been made*

- ***o 2.4.8.15 Where passwords are entered on a user interface, the actual pass phrase is obscured by default***
- ***o 2.4.8.16 The product allows an authorised and complete factory reset of all of the device's authorisation information***
- ***o 2.4.8.17 Where the product has the ability to remotely recover from attack, it should rely on a known good state, to enable safe recovery of the device***
- ***o 2.4.8.18 Devices are provided with a RoT-backed unique authenticable logical identity***

- ***2.4.9 Assurance Applicability – Encryption and Key Management for Hardware***
  - *o 2.4.9.1 Intentionally left blank to maintain requirement numbering*
  - *o 2.4.9.2 If present, a true random number generator source has been validated for true randomness*
  - *o 2.4.9.3 There is a process for secure provisioning of security parameters and keys*
  - ***o 2.4.9.4 There is a secure method of key insertion that protects keys against copying***
  - ***o 2.4.9.5 All the product related cryptographic functions have no publicly known unmitigated weaknesses in the algorithms or implementation***
  - ***o 2.4.9.6 All the product related cryptographic functions are sufficiently secure for the lifecycle of the product***
  - ***o 2.4.9.7 The product stores all sensitive unencrypted parameters in a secure, tamper-resistant location.***
  - ***o 2.4.9.8 The cryptographic key chain used for signing production software is different from that used for any other process***
  - *o 2.4.9.9 In device manufacture, all asymmetric encryption private keys that are unique to each device are secured*
  - *o 2.4.9.10 All key lengths are sufficient for the level of assurance required*
  - ***o 2.4.9.11 In systems with many layered sub devices, key management should follow best practice***
- ***2.4.10 Assurance Applicability – Web User Interface***
  - ***o 2.4.10.1 Where the product or service provides a web-based user interface, Authentication is secured using current best practice cryptography***
  - ***o 2.4.10.2 Where the product or service provides a web browser-based interface, access to any restricted/administrator area or functionality shall require authentication***
  - ***o 2.4.10.3 Where the product or service provides a web-based management interface, Authentication is secured using current best practice cryptography***
  - ***o 2.4.10.4 The initial password for a web user interface is unique for every device in the product family***
  - ***o 2.4.10.5 The web user interface is protected by an automatic session idle logout timeout function***

- *2.4.10.6 User passwords are not stored in plain text*
- *2.4.10.6.1 Strong passwords are required, and a random salt value is incorporated with the password*
- *2.4.10.7 Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords*
- *2.4.10.8 The web user interface shall follow good practice guidelines.*
- *2.4.10.9 A vulnerability assessment has been performed before deployment and is repeated periodically throughout the lifecycle of the service or product*
- *2.4.10.10 All data being transferred over interfaces should be validated where appropriate*
- *2.4.10.11 Sanitize input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script*
- *2.4.10.12 All inputs and outputs are validated using for example an allow list containing authorized origins of data and valid attributes*
- *2.4.10.13 Administration Interfaces are accessible only by authorized operators*
- *2.4.10.14 Reduce the lifetime of sessions to mitigate the risk of session hijacking and replay attacks*
- *2.4.10.15 All inputs and outputs are checked for validity*
- *2.4.10.16 Web Interfaces should be developed using best practice secure coding techniques and server frameworks*
- *2.4.10.17 Password entry follows industry standard practice*
- *2.4.10.18 Web interface should provide a simple method to initiate any security update to the end device*
- *2.4.10.19 Personal data communicated between the web interface and the device shall be encrypted*

- *2.4.11 Assurance Applicability – Mobile Application*
  - *2.4.11.1 The initial password or factory reset password is unique to each device in the product family*
  - *2.4.11.2 Password entry follows industry standard practice*
  - *2.4.11.3 The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access*
  - *2.4.11.4 Communication with the remote server (s) is via a secure connection*
  - *2.4.11.5 The product securely stores any passwords using an industry standard cryptographic algorithm*
  - *2.4.11.6 Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords*
  - *2.4.11.7 All data being transferred over interfaces should be validated where appropriate*

- *o 2.4.11.8 Enforce Strong Authentication over administration interfaces*
- *o 2.4.11.9 All application inputs and outputs are validated using for example a allowed list containing authorized origins of data and valid attributes of such data*
- *o 2.4.11.10 Mobile Apps should be developed using best practice secure coding techniques and server frameworks*
- *o 2.4.11.11 App interface should provide a simple method (one to two clicks) to initiate any security update to the end device*
- *o 2.4.11.12 Access to device functionality should only be permitted after successful Authentication*
- *o 2.4.11.13 Personal data communicated between the mobile app and the device shall be encrypted*

- *2.4.12 Assurance Applicability – Data Protection and Privacy*
  - *o 2.4.12.1 The product/service stores the minimum amount of Personal Information from users required for the operation of the service*
  - *o 2.4.12.2 The product/service ensures that all Personal Information is encrypted and only accessible after successful authentication*
  - *o 2.4.12.3 The product/service ensures that only authorized personnel have access to personal data of users*
  - *o 2.4.12.4 The product/service ensures that Personal Information is anonymized whenever possible*
  - *o 2.4.12.5 The Product Manufacturer or Service Provider shall ensure that a data retention policy is in place and documented for users*
  - *o 2.4.12.6 There is a method or methods for the product owner to be informed about what Personal Information is collected*
  - *o 2.4.12.7 There is a method or methods for each user to check/verify what Personal Information is collected*
  - *o 2.4.12.8 The product/service can be made compliant with the local and/or regional Personal Information protection legislation*
  - *o 2.4.12.9 The supplier or manufacturer of any device shall provide documented information to end users*
  - *o 2.4.12.10 The supplier of any devices shall provide clear information about the security process of the device(s)*
  - *o 2.4.12.11 The supplier of any devices and/or services shall provide the necessary information to maintain the end user's privacy and security when decommissioning a device*
  - *o 2.4.12.12 The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities*
  - *o 2.4.12.13 Security of devices and services should be designed with usability in mind*
  - *o 2.4.12.14 The product or service only records audio/visual/or any other data in*

accordance with the authorization of the user

- ***2.4.12.15 The supplier or manufacturer performs a privacy impact assessment (PIA) to identify Personally Identifiable Information (PII)***

- ***2.4.13 Assurance Applicability – Cloud and Network Elements***
  - *2.4.13.1 All the product related cloud and network elements have the latest operating system(s) security updates*
  - ***2.4.13.2 Any product related web servers have their webserver identification options (e.g. Apache or Linux) switched off***
  - ***2.4.13.3 All product related web servers have their webserver HTTP trace and trace methods disabled***
  - ***2.4.13.4 All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities***
  - ***2.4.13.5 The Product Manufacturer or Service Provider has a process to monitor the relevant security advisories***
  - ***2.4.13.6 The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers***
  - ***2.4.13.7 The product related web servers have repeated renegotiation of TLS connections disabled***
  - ***2.4.13.8 The related servers have unused IP ports disabled***
  - ***2.4.13.9 The server(s) only establishes a connection if the client certificate and its chain of trust are valid***
  - ***2.4.13.10 Where a product related to a webserver encrypts communications using TLS, certificate pinning is implemented***
  - ***2.4.13.11 All the related servers and network elements prevent the use of null or blank passwords***
  - *2.4.13.12 Intentionally left blank to maintain requirement numbering*
  - *2.4.13.13 Intentionally left blank to maintain requirement numbering*
  - ***2.4.13.14 All the related servers and network elements enforce passwords that follows industry good practice***
  - ***2.4.13.15 Brute force attacks are impeded by introducing escalating delays following failed login attempts***
  - ***2.4.13.16 All the related servers and network elements store any passwords using a cryptographic implementation***
  - ***2.4.13.17 All the related servers and network elements support access control measures to restrict access to sensitive information***
  - ***2.4.13.18 All the related servers and network elements prevent anonymous/guest access except for read only access to public information***
  - ***2.4.13.19 If run as a cloud service, the service meets industry standard cloud security principles. Advisory for all classes System Software***

- *2.4.13.20 The services infrastructure shall incorporate protection against DDOS attacks*
- ***2.4.13.21 the services infrastructure shall incorporate redundancy to ensure service continuity and availability***
- ***2.4.13.22 Input data validation should be maintained in accordance with industry best practice methods***
- ***2.4.13.23 The cloud service TCP based communications are encrypted and authenticated using the latest TLS standard***
- ***2.4.13.24 If run as a cloud service, UDP-based communications are encrypted using the latest Datagram Transport Layer Security (DTLS)***
- ***2.4.13.25 The registries of a cloud service are configured to restrict access to only authorized administrators***
- *2.4.13.26 Product-related cloud services bind API keys to specific IoT applications and are not installed on non-authorized devices*
- ***2.4.13.27 Product-related cloud services API keys are not hard-coded into devices or applications. Mandatory for all classes System Software***
- ***2.4.13.28 If run as a cloud service, privileged roles are defined and implemented for any gateway/service that can configure devices***
- ***2.4.13.29 Product-related cloud service databases are encrypted during storage.***
- ***2.4.13.30 Product-related cloud service databases restrict read/write access to only authorized individuals, devices and services***
- ***2.4.13.31 Defense-in-depth cloud services***
- ***2.4.13.32 When implemented as a cloud service, all remote access to cloud services is via secure means***
- *2.4.13.33 Product-related cloud services monitor for compliance with connection policies and report out-of-compliance connection attempts*
- ***2.4.13.34 IoT edge devices should connect to cloud services using secure hardware and services***
- *2.4.13.35 Any personal data communicated between the mobile app and the device shall be encrypted*
- *2.4.13.36 Subject to user permission, telemetry data from the device should be analyzed for anomalous behavior to detect malfunctioning or malicious activity*

- ***2.4.14 Assurance Applicability – Secure Supply Chain and Production***
  - *2.4.14.1 Ensure the entire production test and calibration software is removed or secured before the product is dispatched from the factory*
  - ***2.4.14.2 Software source code and final production software images are stored encrypted in off-site locations or by a 3rd party Escrow service***
  - ***2.4.14.3 In manufacture, all the devices are logged by the product vendor, utilizing unique tamper resistant identifiers***

- ***2.4.14.4 Ensure that any devices with duplicate serial numbers are not shipped***
- ***2.4.14.5 The entire production test and any related calibration is executed with the processor system operating in its secured boot***
- ***2.4.14.6 A securely controlled area and process shall be used for device provisioning where the production facility is untrusted***
- ***2.4.14.7 A cryptographic protected ownership proof shall be transferred along the supply chain***
- ***2.4.14.8 An auditable manifest of all libraries used within the product is maintained to inform vulnerability management***
- *2.4.14.9 All encryption keys that are unique to each device are securely generated or programmed into each device in accordance with FIPS 140-2*
- *2.4.14.10 An authorized actor in physical possession of a device can discover and authenticate its ROT-backed logical identity*
- ***2.4.14.11 Devices are shipped with readily-accessible physical identifiers derived from their ROT-backed IDs***
- *2.4.14.12 IoT devices' RoT-backed logical identity is used to identify them in logs of their physical chain of custody*
- *2.4.14.13 Products ship with information about their operations and normal behavior*
- *2.4.14.14 Procedures for proper disposal of scrap product exist at manufacturing facilities, and compliance is monitored*
- *2.4.14.15 Production assets are encrypted during transport to the intended production facility, area or system, or delivered via private channel*
- *2.4.14.16 Device firmware images and configuration data are secured against unauthorized modification*
- *2.4.14.17 Steps have been taken to prevent inauthentic devices from being programmed with confidential firmware images and configuration data*
- *2.4.14.18 Steps have been taken to prevent inauthentic devices from being signed into certificate chains of trust or otherwise on boarded*
- *2.4.14.19 Device certificate signing keys and other on boarding credentials are secured against unauthorized access*
- ***2.4.14.20 Ensure secure alternative access to resource production if needed***
- *2.4.14.21 Operators keep their software up to date and monitor them for signs of compromise*
- *2.4.14.22 The OEM retains authorization of secure production control methods*
- *2.4.14.23 The supplier shall provide information about how the device(s) removal, disposal or replacement shall be carried out in a secure manner*
- ***2.4.14.24 An end-of-life disposal process shall be provided to ensure the confidentiality***
- *2.4.14.25 Software bill of materials (SBOM) shall be available and notified (URL) to*

customers with product documentation

- ***2.4.15 Assurance Applicability – Configuration***
  - ***2.4.15.1 The configuration of the device and any related web services is secure and tamper***
  - ***2.4.15.2 Updates to configuration should be provisioned securely***
  - ***2.4.15.3 The manufacturer should provide users with guidance***
- ***2.4.16 Assurance Applicability – Device Ownership Transfer***
  - ***2.4.16.1 The supplier shall provide necessary information to maintain the end user's privacy and security when transferring device ownership to different owner***
  - ***2.4.16.2 Where a device User wishes to end the service, the supplier shall provide necessary information to maintain the end user's privacy and security***
  - ***2.4.16.3 The Service Provider should not have the ability to do a reverse lookup of device ownership from the device identity***
  - ***2.4.16.4 If ownership change is required/allowed, the device must have an irrevocable method of decommissioning and recommissioning***
  - *2.4.16.5 The device registration with the Service Provider shall use a secure connection*
  - ***2.4.16.6 The device manufacturer ensures that the exposed identity of the device cannot be linked by unauthorized actors to the end user***
  - ***2.4.16.7 Confidential user data on a device should be reliably erasable when transferring a device to a new end user***

Online Trust Alliance IoT Trust Framework

Name	
IoT Security & Privacy Trust Framework v2.5	
Developing body	**Date of publication**
Online trust alliance	*14/10/2017*
Type	**Applies to**
Requirements/guidelines/controls	*Products: IoT* *Services: IoT*
Scope	
"The IoT Trust Framework includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which need to be provided prior to product purchase, policies regarding data collection, usage and sharing, as well as the terms and conditions of security patching post-warranty. […] *Core to addressing the inherent security risks and privacy issues is the application of the principles to the entire device solution or ecosystem. These include the device or sensor, the supporting*	

applications, and the backend / cloud services." – P. 1 of [21].

Thus, the document covers both IoT devices and the associated services.

Relation to CSA

No direct relation.

Weblinks	**Accessibility**
https://www.internetsociety.org/wp-content/uploads/2018/05/iot_trust_framework2.5a_EN.pdf	*Free*

Specific relevance for CORAL

This document contains a set of principles to help secure IoT devices and data. Its audience includes developers and acquirers, and is destined to serve in IoT certification programs.
The Framework presented in the document is broken down into 4 main areas:

- *Security Principles*
- *User Access & Credentials*
- *Privacy, Disclosures & Transparency*
- *Notifications & Related Best Practices*

For each area, a set of requirements is presented. A two-level classification is given in the document: each requirement is either mandatory ("Must") or recommended ("Should"). ***Therefore, the requirements in bold represent those that are mandatory, as these logically form the security baseline. Some requirements have descriptions that are too lengthy for the present document; in that case, the authors of this deliverable have shortened the description.***

- *Security – Device, Apps and Cloud Services*
  - ***1. Disclose whether the device is capable of receiving security related updates.***
  - ***2. All personally identifiable data in transit and in storage must be encrypted.***
  - ***3. All IoT support websites must fully encrypt the user session from the device to the backend services.***
  - ***4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations.***
  - ***5. Establish coordinated vulnerability disclosure.***
  - ***6. Ensure a mechanism is in place for automated safe and secure methods.***
  - ***7. Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification.***
  - ***8. Security update process must disclose if they are Automated (vs automatic).***
  - ***9. Ensure all IoT devices and associated software have been subjected to rigorous, standardized software development lifecycle testing.***
  - ***10. Conduct security and compliance risk assessments for all service and cloud providers.***
  - *11. Develop and maintain a "bill of materials" including software, firmware, hardware and third-party software libraries.*
  - ***12. Design devices to minimum requirements necessary for operation.***
- *User Access & Credentials*

- ***13. Include strong authentication by default.***
- ***14. Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential reset.***
- ***15. Take steps to protect against 'brute force' and/or other abusive login attempts.***
- ***16. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).***
- ***17. Authentication credentials shall be salted, hashed and/or encrypted.***

- *Privacy, Disclosures & Transparency*
  - ***18. Ensure privacy, security, and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download, or enrollment.***
  - ***19. Disclose the duration and end-of-life security and patch support.***
  - ***20. Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used.***
  - ***21. Disclose what and how features will fail to function if connectivity or backend services become disabled or stopped.***
  - ***22. Disclose the data retention policy and storage duration of personally identifiable information.***
  - ***23. IoT devices must provide notice and/or request user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.***
  - ***24. Disclose if and how IoT device/product/service ownership and the data may be transferred.***
  - ***25. Personal data protection.***
  - ***26. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default."***
  - ***27. Commit to not sell or transfer any identifiable consumer data.***
  - ***28. Provide the ability for a consumer to return a product after reviewing the privacy practices.***
  - ***29. 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.***
  - ***30. Comply with applicable regulations, including but not limited to the Children's Online Privacy Protection Act (COPPA) and international privacy, security and data transfer regulatory requirements.***
  - ***31. Publicly post the history of material privacy notice changes for a minimum of two years.***
  - *32. Provide the ability for the user or proxy to delete, or make anonymous, personal or sensitive data stored on company servers upon discontinuing use, loss or sale of device.*
  - *33. Provide the ability to reset a device and application to factory settings, including the ability to erase user data in the event of transfer, rental, loss or sale.*
- *Notifications & Related Best Practices*

- ***34. End-user communications must adopt authentication protocols to help prevent spearphishing and spoofing.***
- *35. For email communications, within 180 days of publishing a DMARC policy, implement a reject or quarantine policy, which helps ISPs and receiving networks to reject email which fails email authentication verification checks.*
- *36. IoT vendors using email communication should adopt transport-level confidentiality, including generally accepted security.*
- *37. Implement measures to help prevent or make evident any physical tampering of devices.*
- *38. Consider how to accommodate accessibility requirements for users who may be vision, hearing and or mobility impaired to maximize access for users of all physical capabilities.*
- ***39. Develop communications processes to maximize user awareness of any potential security or privacy issues, end-of life notifications and possible product recalls.***
- ***40. Enact a breach and cyber response and consumer notification plan to be re-evaluated, tested and updated at least annually and/or after significant internal system, technical and/or operational changes.***

Strategic Principles for Securing the Internet of Things (IoT)

Name	
Strategic Principles for Securing the Internet of Things (IoT)	
Developing body	**Date of publication**
U.S. Department of Homeland Security	*15/11/2016*
Type	**Applies to**
Requirements/guidelines/controls	*Products: IoT* *Services: IoT*
Scope	
"IoT security [...] has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate." – Extract from the Introduction and overview of [22]. *These principles are designed for: IoT developers for both devices and services, IoT manufacturers, IoT service providers, and industrial and business-level consumers.*	
Relation to CSA	
No direct relation.	
Weblink(s)	**Accessibility**
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf	*Free*
Specific relevance for CORAL	

Six principles are put forward to improve security of IoT across the full range of design, manufacturing, and deployment activities. The principles are each subdivided into sub-sets of suggested practices. These principles and suggested practices are listed below. The suggested practices are directly described in [22]. *Thus, the authors of this document have shortened these descriptions, where applicable.*

- *Incorporate Security at the Design Phase*
  - *Enable security by default through unique, hard to crack default user names and passwords.*
  - *Build the device using the most recent operating system that is technically viable and*
  - *economically feasible.*
  - *Use hardware that incorporates security features to strengthen the protection and*
  - *integrity of the device.*
  - *Design with system and operational disruption in mind.*
- *Advance Security Updates and Vulnerability Management*
  - *Consider ways in which to secure the device over network connections or through automated means.*
  - *Consider coordinating software updates among third-party vendors.*
  - *Develop automated mechanisms for addressing vulnerabilities.*
  - *Develop a policy regarding the coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities.*
  - *Develop an end-of-life strategy for IoT products.*
- *Build on Proven Security Practices*
  - *Start with basic software security and cybersecurity practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.*
  - *Practice defense in depth.*
  - *Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.*
- *Prioritize Security Measures According to Potential Impact*
  - *Know a device's intended use and environment, where possible.*
  - *Perform a "red-teaming" exercise, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers.*
  - *Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks.*
- *Promote Transparency across IoT*
  - *Conduct end-to-end risk assessments that account for both internal and third party vendor risks, where possible.*
  - *Consider creating a publicly disclosed mechanism for using vulnerability reports.*
  - *Consider developing and employing a software bill of materials that can be used as a means of building shared trust among vendors and manufacturers.*

- *Connect Carefully and Deliberately*
  - *Advise IoT consumers on the intended purpose of any network connections.*
  - *Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity.*

Web Applications

OWASP Application Security Verification Standard 4.0.2

Name	
OWASP Application Security Verification Standard 4.0.2	
Developing body	**Date of publication**
OWASP	*10/2020*
Type	**Applies to**
Requirements/guidelines/controls	*Products: Web applications*

Scope

"The ASVS is a community-driven effort to establish a framework of security requirements and controls that focus on defining the functional and non-functional security controls required when designing, developing and testing modern web applications and web services." – Preface, p. 8 of [23]

"Goals of ASVS:

- *to help organizations develop and maintain secure applications.*
- *to allow security service vendors, security tools vendors, and consumers to align their requirements and offerings." – p. 10 of* [23]

"ASVS defines three security verification levels, with each level increasing in depth:

- *ASVS Level 1 is for low assurance levels, and is completely penetration testable.*
- *ASVS Level 2 is for applications that contain sensitive data, which requires protection and is the recommended level for most apps.*
- *ASVS Level 3 is for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.*

Each ASVS level contains a list of security requirements. Each of these requirements can also be mapped to security-specific features and capabilities that must be built into software by developers." – p. 10 of [23]

Relation to CSA

This guideline is taken as an example source of good software security practice in ENISA's publication [5]*. The publication summarizes software security considerations in preparation for implementation of the CSA.*

Weblink(s)	**Accessibility**
https://owasp.org/www-project-application-security-verification-standard/ *https://raw.githubusercontent.com/OWASP/ASVS/v4.0.2/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.2-en.pdf*	*Free*

Specific relevance for CORAL

The primary usage of this document is as a security assessment methodology. ASVS level 1 is for a low assurance level. The stated definition of this level is as follows:
"An application achieves ASVS Level 1 if it adequately defends against application security vulnerabilities that are easy to discover, and included in the OWASP Top 10 and other similar checklists. […] Level 1 controls can be checked either automatically by tools or simply manually without access to source code. […] Threats to the application will most likely be from attackers who are using simple and low effort techniques to identify easy-to-find and easy-to-exploit vulnerabilities. This is in contrast to a determined attacker who will spend focused energy to specifically target the application." – p. 11 of [23]
Therefore, the requirements listed in this level may be useful for deriving good low-level security questions related to web applications. The chapters and sections containing requirements for ASVS Level 1 are indicated in bold:

- *V1: Architecture, Design and Threat Modeling Requirements*
  - *V1.1 Secure Software Development Lifecycle Requirements*
  - *V1.2 Authentication Architectural Requirements*
  - *V1.3 Session Management Architectural Requirements*
  - *V1.4 Access Control Architectural Requirements*
  - *V1.5 Input and Output Architectural Requirements*
  - *V1.6 Cryptographic Architectural Requirements*
  - *V1.7 Errors, Logging and Auditing Architectural Requirements*
  - *V1.8 Data Protection and Privacy Architectural Requirements*
  - *V1.9 Communications Architectural Requirements*
  - *V1.10 Malicious Software Architectural Requirements*
  - *V1.11 Business Logic Architectural Requirements*
  - *V1.12 Secure File Upload Architectural Requirements*
  - *V1.13 API Architectural Requirements*
  - *V1.14 Configuration Architectural Requirements*
- ***V2: Authentication Verification Requirements***
  - ***V2.1 Password Security Requirements***
  - ***V2.2 General Authenticator Requirements***
  - ***V2.3 Authenticator Lifecycle Requirements***
  - *V2.4 Credential Storage Requirements*
  - ***V2.5 Credential Recovery Requirements***
  - *V2.6 Look-up Secret Verifier Requirements*
  - ***V2.7 Out of Band Verifier Requirements***
  - ***V2.8 Single or Multi-factor One Time Verifier Requirements***
  - *V2.9 Cryptographic Software and Devices Verifier Requirements*
  - *V2.10 Service Authentication Requirements*
- ***V3: Session Management Verification Requirements***

- ***o V3.1 Fundamental Session Management Requirements***
- ***o V3.2 Session Binding Requirements***
- ***o V3.3 Session Logout and Timeout Requirements***
- ***o V3.4 Cookie-based Session Management***
- *o V3.5 Token-based Session Management*
- *o V3.6 Re-authentication from a Federation or Assertion*
- ***o V3.7 Defenses Against Session Management Exploits***

- ***V4: Access Control Verification Requirements***
  - ***o V4.1 General Access Control Design***
  - ***o V4.2 Operation Level Access Control***
  - *o* ***V4.3 Other Access Control Considerations***
- ***V5: Validation, Sanitization and Encoding Verification Requirements***
  - ***o V5.1 Input Validation Requirements***
  - ***o V5.2 Sanitization and Sandboxing Requirements***
  - ***o V5.3 Output Encoding and Injection Prevention Requirements***
  - *o V5.4 Memory, String, and Unmanaged Code Requirements*
  - ***o V5.5 Deserialization Prevention Requirements***
- ***V6: Stored Cryptography Verification Requirements***
  - *o V6.1 Data Classification*
  - ***o V6.2 Algorithms***
  - *o V6.3 Random Values*
  - *o V6.4 Secret Management*
- ***V7: Error Handling and Logging Verification Requirements***
  - ***o V7.1 Log Content Requirements***
  - *o V7.2 Log Processing Requirements*
  - *o V7.3 Log Protection Requirements*
  - ***o V7.4 Error Handling***
- ***V8: Data Protection Verification Requirements***
  - *o V8.1 General Data Protection*
  - ***o V8.2 Client-side Data Protection***
  - *o* ***V8.3 Sensitive Private Data***
- ***V9: Communications Verification Requirements***
  - ***o V9.1 Client Communications Security Requirements***
  - *o V9.2 Server Communications Security Requirements*
- ***V10: Malicious Code Verification Requirements***
  - *o V10.1 Code Integrity Controls*
  - *o V10.2 Malicious Code Search*
  - ***o V10.3 Deployed Application Integrity Controls***
- ***V11: Business Logic Verification Requirements***
  - *o* ***V11.1 Business Logic Security Requirements***
- ***V12: File and Resources Verification Requirements***

- ***V12.1 File Upload Requirements***
- *V12.2 File Integrity Requirements*
- ***V12.3 File Execution Requirements***
- ***V12.4 File Storage Requirements***
- ***V12.5 File Download Requirements***
- ***V12.6 SSRF Protection Requirements***

- ***V13: API and Web Service Verification Requirements***
  - ***V13.1 Generic Web Service Security Verification Requirements***
  - ***V13.2 RESTful Web Service Verification Requirements***
  - ***V13.3 SOAP Web Service Verification Requirements***
  - *V13.4 GraphQL and other Web Service Data Layer Security Requirements*
- ***V14: Configuration Verification Requirements***
  - *V14.1 Build*
  - ***V14.2 Dependency***
  - ***V14.3 Unintended Security Disclosure Requirements***
  - ***V14.4 HTTP Security Headers Requirements***
  - ***V14.5 Validate HTTP Request Header Requirements***

Note that, oddly enough, there is no apparent direct relation between the ASVS and the OWASP Web Security Testing Guide (see the corresponding card in this document).

OWASP Web Security Testing Guide v4.2

Name	
OWASP Web Security Testing Guide v4.2	
Developing body	**Date of publication**
OWASP	*03/12/2020*
Type	**Applies to**
Evaluation/assessment/testing	*Products: Web applications*
Scope	
The OWASP Web Security Testing Guide (WSTG) is a guideline for testing security functionalities of web applications. To quote the Introduction on p. 11 of [23]: "The aim of the project is to help people understand the what, why, when, where, and how of testing web applications. The project has delivered a complete testing framework [...]. Readers can use this framework as a template to build their own testing programs or to qualify other people's processes. The Testing Guide describes in detail both the general testing framework and the techniques required to implement the framework in practice."	
Relation to CSA	
No direct relation.	
Weblink(s)	**Accessibility**
https://owasp.org/www-project-web-security-testing-guide/	*Free*

https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf

Specific relevance for CORAL

The OWASP WSTG is a testing framework, not a requirements framework. However, the listed test categories can be used to derive security requirements (or questions) for web applications. There is a fair share of redundancy between the categories listed here and those found in the ASVP list.
There is no attempt at defining security levels. The testing categories and subcategories are:

- *4.1 Information Gathering*
  - *4.1.1 Conduct Search Engine Discovery Reconnaissance for Information Leakage*
  - *4.1.2 Fingerprint Web Server*
  - *4.1.3 Review Webserver Metafiles for Information Leakage*
  - *4.1.4 Enumerate Applications on Webserver*
  - *4.1.5 Review Webpage Content for Information Leakage*
  - *4.1.6 Identify Application Entry Points*
  - *4.1.7 Map Execution Paths Through Application*
  - *4.1.8 Fingerprint Web Application Framework*
  - *4.1.9 Fingerprint Web Application*
  - *4.1.10 Map Application Architecture*
- *4.2 Configuration and Deployment Management Testing*
  - *4.2.1 Test Network Infrastructure Configuration*
  - *4.2.2 Test Application Platform Configuration*
  - *4.2.3 Test File Extensions Handling for Sensitive Information*
  - *4.2.4 Review Old Backup and Unreferenced Files for Sensitive Information*
  - *4.2.5 Enumerate Infrastructure and Application Admin Interfaces*
  - *4.2.6 Test HTTP Methods*
  - *4.2.7 Test HTTP Strict Transport Security*
  - *4.2.8 Test RIA Cross Domain Policy*
  - *4.2.9 Test File Permission*
  - *4.2.10 Test for Subdomain Takeover*
  - *4.2.11 Test Cloud Storage*
- *4.3 Identity Management Testing*
  - *4.3.1 Test Role Definitions*
  - *4.3.2 Test User Registration Process*
  - *4.3.3 Test Account Provisioning Process*
  - *4.3.4 Testing for Account Enumeration and Guessable User Account*
  - *4.3.5 Testing for Weak or Unenforced Username Policy*
- *4.4 Authentication Testing*
  - *4.4.1 Testing for Credentials Transported over an Encrypted Channel*
  - *4.4.2 Testing for Default Credentials*
  - *4.4.3 Testing for Weak Lock Out Mechanism*
  - *4.4.4 Testing for Bypassing Authentication Schema*

- *4.8 Testing for Error Handling*
  - *4.8.1 Testing for Improper Error Handling*
  - *4.8.2 Testing for Stack Traces*
- *4.9 Testing for Weak Cryptography*
  - *4.9.1 Testing for Weak Transport Layer Security*
  - *4.9.2 Testing for Padding Oracle*
  - *4.9.3 Testing for Sensitive Information Sent via Unencrypted Channels*
  - *4.9.4 Testing for Weak Encryption*
- *4.10 Business Logic Testing*
  - *4.10.1 Test Business Logic Data Validation*
  - *4.10.2 Test Ability to Forge Requests*
  - *4.10.3 Test Integrity Checks*
  - *4.10.4 Test for Process Timing*
  - *4.10.5 Test Number of Times a Function Can Be Used Limits*
  - *4.10.6 Testing for the Circumvention of Work Flows*
  - *4.10.7 Test Defenses Against Application Misuse*
  - *4.10.8 Test Upload of Unexpected File Types*
  - *4.10.9 Test Upload of Malicious Files*
- *4.11 Client-side Testing*
  - *4.11.1 Testing for DOM-Based Cross Site Scripting*
  - *4.11.2 Testing for JavaScript Execution*
  - *4.11.3 Testing for HTML Injection*
  - *4.11.4 Testing for Client-side URL Redirect*
  - *4.11.5 Testing for CSS Injection*
  - *4.11.6 Testing for Client-side Resource Manipulation*
  - *4.11.7 Testing Cross Origin Resource Sharing*
  - *4.11.8 Testing for Cross Site Flashing*
  - *4.11.9 Testing for Clickjacking*
  - *4.11.10 Testing WebSockets*
  - *4.11.11 Testing Web Messaging*
  - *4.11.12 Testing Browser Storage*
  - *4.11.13 Testing for Cross Site Script Inclusion*
- *4.12 API Testing*
  - *4.12.1 Testing GraphQL*

Note that, oddly enough, there is no apparent direct relation between the WSTG and the OWASP Application Security Verification Standard (see the corresponding card in this document).

Artificial Intelligence

The Assessment List for Trustworthy Artificial Intelligence (ALTAI)

Name	
The Assessment List for Trustworthy Artificial Intelligence (ALTAI)	
Developing body	**Date of publication**
Independent high-level expert group on Artificial Intelligence set up by the European Commission	*07/2020*
Type	**Applies to**
Requirements/guidelines/controls	*Products: AI systems*
Scope	
This document contains the Assessment List for Trustworthy AI (ALTAI) intended for self-evaluation purposes, see [24]. It provides an initial approach in the form of a questionnaire for the evaluation of trustworthy AI, covering a number of requirements such as: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability.	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342 *https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-assessment-list-trustworthy-artificial-intelligence-altai?language=fr*	*Free*

Specific relevance for CORAL

The questionnaire that is proposed in the document covers many categories from the scope. The authors of the present document consider that the requirements regarding Technical Robustness and Safety, which include those related to security, are the most relevant for the project.

In [24], considerations on technical robustness and security are translated among others into questions about AI system resilience to attacks (see p. 9 of [24]). Since these are not very long, they are included here in their entirety. The control questions proposed to ensure the AI security are as follows:

- *Could the AI system have adversarial, critical or damaging effects (e.g. to human or societal safety) in case of risks or threats such as design or technical faults, defects, outages, attacks, misuse, inappropriate or malicious use?*
- *Is the AI system certified for cybersecurity (e.g. the certification scheme created by the Cybersecurity Act in Europe) or is it compliant with specific security standards?*
- *How exposed is the AI system to cyber-attacks?*
    - *Did you assess potential forms of attacks to which the AI system could be vulnerable?*
    - *Did you consider different types of vulnerabilities and potential entry points for attacks such as:*
        - *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)*

- *Did you put measures in place to ensure the integrity, robustness and overall security of the AI system against potential attacks over its lifecycle?*
- *Did you red-team/pentest the system?*
- *Did you inform end-users of the duration of security coverage and updates?*
  - *What length is the expected timeframe within which you provide security updates for the AI system?*

Securing Machine Learning Algorithms

Name	
Securing Machine Learning Algorithms	
Developing body	**Date of publication**
ENISA – European Union Agency for Cybersecurity	*12/2021*
Type	**Applies to**
Requirements/guidelines/controls	*Products: AI systems*
Scope	
"This report provides a taxonomy for machine learning algorithms, a detailed analysis of threats and security controls in widely adopted standards." – p. 3 of [25]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms *https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms/@@download/fullReport*	*Free*
Specific relevance for CORAL	

The document introduces three categories of security controls. "Organisational and Policy" are more traditional security controls, either organizational or linked to security policies. "Technical" are more classic technical security controls. "Specific to ML" are security controls that are specific to applications using ML.
 	
- *Organisational and Policy*
  - *Apply a RBAC model, respecting the least privileged principle*
  - *Apply documentation requirements to AI projects*
  - *Assess the regulations and laws the ML application must comply with*
  - *Ensure ML applications comply with data security requirements*
  - *Ensure ML applications comply with identity management, authentication, and access control policies*
  - *Ensure ML applications comply with protection policies and are integrated to security operations processes*
  - *Ensure ML applications comply with security policies*	

- *Include ML applications into detection and response to security incident processes*
- *Include ML applications in asset management processes*
- *Integrate ML applications into the overall cyber-resilience strategy*
- *Integrate ML specificities to existing security policies*

- *Technical*
  - *Assess the exposure level of the model used*
  - *Check the vulnerabilities of the components used so that they have an appropriate security level*
  - *Conduct a risk analysis of the ML application*
  - *Control all data used by the ML model*
    - *Ensure reliable sources are used*
    - *Use methods to clean the training dataset from suspicious samples*
  - *Define and monitor indicators for proper functioning of the model*
  - *Ensure appropriate protection is deployed for test environments*
  - *Ensure ML applications comply with third parties' security requirements*
  - *Ensure ML projects follow the global process for integrating security into projects*
- *Specific to ML*
  - *Add some adversarial examples to the training dataset*
  - *Apply modifications on inputs*
  - *Build explainable models*
  - *Choose and define a more resilient model design*
  - *Enlarge the training dataset*
  - *Ensure that models are unbiased*
  - *Ensure that models respect differential privacy to a sufficient degree*
  - *Ensure that the model is sufficiently resilient to the environment in which it will operate*
  - *Implement processes to maintain security levels of ML components over time*
  - *Implement tools to detect if a data point is an adversarial example or not*
  - *Integrate ML specificities to awareness strategy and ensure all ML stakeholders are receiving it*
  - *Integrate poisoning control after the "model evaluation" phase*
  - *Reduce the available information about the model*
  - *Reduce the information given by the model*
  - *Use federated learning to minimize risk of data breaches*
  - ***Use less easily transferable models***

In an annex, the document provides operational implementation examples for each of the security controls identified.

ETSI GR SAI 002 V1.1.1 Securing Artificial Intelligence (SAI); Data Supply Chain Security

Name		
ETSI GR SAI 002 V1.1.1 Securing Artificial Intelligence (SAI); Data Supply Chain Security		
Developing body	**Development stage**	**Date of publication**
ETSI ISG SAI Securing Artificial Intelligence	*Published*	*08/2021*
Type	**Applies to**	
Requirements/guidelines/controls	*Products: AI systems*	
Scope		
"Data is a critical component in the development of Artificial Intelligence (AI) and Machine Learning (ML) systems. Compromising the integrity of data has been demonstrated to be a viable attack vector against such systems (see clause 4). The present document summarizes the methods currently used to source data for training AI, along with a review of existing initiatives for developing data sharing protocols. It then provides a gap analysis on these methods and initiatives to scope possible requirements for standards for ensuring integrity and confidentiality of the shared data, information and feedback. *The present document relates primarily to the security of data, rather than the security of models themselves. It is recognized, however, that AI supply chains can be complex and that models can themselves be part of the supply chain, generating new data for onward training purposes. Model security is therefore influenced by, and in turn influences, the security of the data supply chain. Mitigation and detection methods can be similar for data and models, with poisoning of one being detected by analysis of the other.* *The present document focuses on security; however, data integrity is not only a security issue. Techniques for assessing and understanding data quality for performance, transparency or ethics purposes are applicable to security assurance too. An adversary aim can be to disrupt or degrade the functionality of a model to achieve a destructive effect. The adoption of mitigations for security purposes will likely improve performance and transparency, and vice versa.* *The present document does not discuss data theft, which can be considered a traditional cybersecurity problem. The focus is instead specifically on data manipulation in, and its effect on, AI/ML systems." – Scope of* [26]		
Relation to CSA		
No direct relation.		
Weblinks		**Accessibility**
https://www.etsi.org/deliver/etsi_gr/SAI/001_099/002/01.01.01_60/gr_SAI002v010101p.pdf		*Free*
Specific relevance for CORAL		
With respect to security, the focus of the document is on the preservation of data integrity.		

Various mechanisms to preserve data integrity are identified, including standard cybersecurity good practices, polices and legal frameworks, standards and technologies. Among mechanisms relevant to the current deliverable, there are suggestions on standard cybersecurity practices and technology-specific proposals.

Standard cybersecurity practices, including cybersecurity hygiene and data supply chain security, are (see section 6.1.2 of [26]):

- *Good training and employee awareness remain the best defence against phishing attacks seeking to gain credentials or access to the system.*
- *System patch levels should be kept updated to protect systems against exploitation of known vulnerabilities.*
- *A robust password policy and multi-factor authentication should be in place.*
- *Strong access controls should be in place, applying the principle of least privilege. These stand alongside limits to the number of queries allowed to be made against a model in a period of time.*
- *A good CI/CD (continuous integration/continuous deployment) pipeline.*
- *Following deployment of a service, auditing and logging enables the detection of possible anomalies. In an AI context, this could include a representation of the inputs to the ML model.*
- *A cyber incident response plan should be in place and audit processes should be established.*
- *A cyber incident response plan should be in place and audit processes should be established.*
- *Building data and model security considerations into the contracting processes.*

Technology-based mechanisms to ensure the integrity of data (see section 6.4 of [26]) include:

- *Federated learning: allows models to be trained on large amounts of data while limiting the exposure or movement of raw data, and can hence be seen as a special means of data exchange.*
- *Cryptographic mechanisms: should be used on raw data at the acquisition stage, information on preprocessing techniques used, information on training procedure (architecture, model parameters, pseudorandom seeds), output of training/testing.*
- *Mitigating the attempts of data poisoning before it can impact a model: identify poisoned data in the training dataset (for ex. through outlier sanitization or reject on negative impact, RONI)*
- *Reduce damage from data or model poisoning in case it happens: feature squeezing, de-noising of data, deliberate including of properly classified adversarial examples in a dataset, frequent model retraining.*
- *Fine-tuning and/or regular retraining of models with locally-verified or otherwise trusted data, where possible.*

ETSI GR SAI 005 V1.1.1 Securing Artificial Intelligence (SAI); Mitigation Strategy Report

Name	
ETIS GR SAI 005 V1.1.1 Securing Artificial Intelligence (SAI); Mitigation Strategy Report	
Developing body	**Date of publication**
ETSI ISG SAI Securing Artificial Intelligence	*03/2021*
Type	**Applies to**
Requirements/guidelines/controls	*Products: AI systems*
Scope	
"The present document summarizes and analyses existing and potential mitigation against threats for AI-based systems as discussed in ETSI GR SAI 004 [27]*. The goal is to have a technical survey for mitigating against threats introduced by adopting AI into systems. The technical survey shed light on available methods of securing AI-based systems by mitigating against known or potential security threats. It also addresses security capabilities, challenges, and limitations when adopting mitigation for AI-based systems in certain potential use cases." – Scope of* [28]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.etsi.org/deliver/etsi_gr/SAI/001_099/005/01.01.01_60/gr_SAI005v010101p.pdf	*Free*
Specific relevance for CORAL	
Mitigations are summarized as approaches in a framework where a feasible strategy can be built against attacks under specific assumptions. In addition to being categorized by which attack they address, mitigations are further classified by whether the addressed model is modified when the mitigation is applied. Two types of attacks are considered: attacks on training (poisoning and backdoor attacks) and attacks on inference (evasion attack, model stealing, data extraction). The following summarizes the content of Sections 5 and 6 in [28]*; also see Table 1, p. 14 of* [27]*.* *Mitigation approaches against attacks on training:* - *Enhance data quality: model enhancement approach that helps to prevent both poisoning and backdoor attacks* - *Data sanitization: model enhancement approach that helps to prevent both poisoning and backdoor attacks* - *Block poisoning: model enhancement approach against poisoning attacks* - *Output restoration: model-agnostic approach against poisoning attacks* - *Model restoration: model enhancement approach against backdoor attack* - *Trigger detection: could be both model enhancement and model-agnostic approach against backdoor attack* - *Trigger deactivation: model-agnostic approach against backdoor attack* - *Backdoor detection: model-agnostic approach against backdoor attack*	

Mitigation approaches against attacks on inference:

- *Data preprocessing: model enhancement approach against evasion attacks*
- *Model hardening: model enhancement approach against evasion attacks*
- *Robustness evaluation: model enhancement approach against evasion attacks*
- *AE detection: model-agnostic approach against evasion attacks*
- *Input or output restoration: model-agnostic approaches against evasion attacks*
- *IP management: model enhancement approach against model stealing*
- *Stealing detection: model-agnostic approach against model stealing*
- *Fingerprinting: model-agnostic approach against model stealing*
- *Obfuscation of outputs and confidence scores: model-agnostic approaches against model stealing and data extraction, respectively*
- *Limit the number of queries: model-agnostic approach against model stealing or data extraction*
- *Embed data privacy: model enhancement approach against data extraction*
- *Training with privacy: model enhancement approach against data extraction*

3. Services

Generic

ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements

Name	
ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements	
Developing body	**Date of publication**
ISO/IEC JTC 1 SC 40 IT service management and IT governance	*09/2018*
Type	**Applies to**
Requirements/guidelines/controls	*Services: generic*
Scope	
"This document specifies requirements for an organization to establish, implement, maintain and continually improve a service management system (SMS). The requirements specified in this document include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value. […] *The term "service" as used in this document refers to the service or services in the scope of the SMS. The term "organization" as used in this document refers to the organization in the scope of the SMS that manages and delivers services to customers. […]" – Extract of scope of* [29]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.iso.org/standard/70636.html	*Not free*
Specific relevance for CORAL	

This standard provides requirements for a service management system destined to manage a generic IT service. It is structured according to the management system standard prescribed structure from the ISO directives [30].
 	
The standard's requirements for such a system are listed below. It is the view of the authors of this document that secure generic IT service delivery should begin with well-managed IT service delivery. ***In bold are those requirements that pertain to information security.***
 	
- *5 Leadership*
  o *5.1 Leadership and commitment*
  o *5.2 Policy*
  ▪ *5.2.1 Establishing the service management policy*
  ▪ *5.2.2 Communicating the service management policy*	

- *5.3 Organizational roles, responsibilities and authorities*

- *6 Planning*
  - *6.1 Actions to address risks and opportunities*
  - *6.2 Service management objectives and planning to achieve them*
    - *6.2.1 Establish objectives*
    - *6.2.2 Plan to achieve objectives*
  - *6.3 Plan the service management system*
- *7 Support of the service management system*
  - *7.1 Resources*
  - *7.2 Competence*
  - *7.3 Awareness*
  - *7.4 Communication*
  - *7.5 Documented information*
    - *7.5.1 General*
    - *7.5.2 Creating and updating documented information*
    - *7.5.3 Control of documented information*
    - *7.5.4 Service management system documented information*
  - *7.6 Knowledge*
- ***8 Operation of a service management system***
  - *8.1 Operational planning and control*
  - *8.2 Service portfolio*
    - *8.2.1 Service delivery*
    - *8.2.2 Plan the services*
    - *8.2.3 Control of parties involved in the service lifecycle*
    - *8.2.4 Service catalogue management*
    - *8.2.5 Asset management*
    - *8.2.6 Configuration management*
  - *8.3 Relationship and agreement*
    - *8.3.1 General*
    - *8.3.2 Business relationship management*
    - *8.3.3 Service level management*
    - *8.3.4 Supplier management*
  - *8.4 Supply and demand*
    - *8.4.1 Budgeting and accounting for services*
    - *8.4.2 Demand management*
    - *8.4.3 Capacity management*
  - *8.5 Service design, build and transition*
    - *8.5.1 Change management*
    - *8.5.2 Service design and transition*
    - *8.5.3 Release and deployment management*
  - *8.6 Resolution and fulfillment*
    - *8.6.1 Incident management*

- *8.6.2 Service request management*
- *8.6.3 Problem management*

- ***8.7 Service assurance***
  - *8.7.1 Service availability management*
  - *8.7.2 Service continuity management*
  - ***8.7.3 Information security management***

- *9 Performance evaluation*
  - *9.1 Monitoring, measurement, analysis and evaluation*
  - *9.2 Internal audit*
  - *9.3 Management review*
  - *9.4 Service reporting*
- *10 Improvement*
  - *10.1 Nonconformity and corrective action*
  - *10.2 Continual improvement*

Note also that there exist standards that offer guidance on the integration of this standard with ISO/IEC 27001 (see [31]), in particular in support of clause 8.7.3 of ISO/IEC 20000-1. These standards are:

- *ISO/IEC ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1* [32];
- *ISO/IEC TR 20000-7:2019 Information technology — Service management — Part 7: Guidance on the integration and correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015 and ISO/IEC 27001:2013* [33]

Cloud

StarAudit

Name	
StarAudit	
Developing body	**Date of publication**
EuroCloud Europe	*12/2020 (4th edition of the StarAudit control catalogue)*
Type	**Applies to**
Requirements/guidelines/controls	*Service: Cloud services*
Scope	
The StarAudit scheme is essentially an evaluation system for cloud services overall, including security aspects. The evaluation scheme is based on a set of requirements, see [34]. To quote from the StarAudit website (https://staraudit.org/home/about/): "The StarAudit scheme evaluates cloud services according to a well-defined and transparent catalogue of criteria. The result of this audit process shows the respective maturity and compliance levels of a service. *The certification procedure is based on best practices and provides answers to the fundamental*	

questions managers are likely to ask when looking for a suitable cloud service provider. Unlike pure security or data protection audits, it covers the entire range of cloud service functions and validates compliance against the requirements in clearly understandable terms."
The scheme covers all three classic cloud service models of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Relation to CSA

No direct relation.

Weblink(s)	**Accessibility**
https://staraudit.org/ *https://staraudit.org/publications/staraudit-controls/*	*Freely available but watermarked download*

Specific relevance for CORAL

The scheme essentially evaluates cloud services from a general service provisioning point-of-view, including security aspects. Thus, the evaluation scope is wider than that of the CORAL project, à priori. It is equipped with a maturity level rating from three to five stars. This suggests that a "basic" level of service is achieved using the three-star rating, achievable in principle by modestly-sized cloud providers.
The controls catalogue lists controls in Introduction Areas (IA), then subcategories of these areas, and a further subdivision of each subcategory. Each control is accompanied by a corresponding question to address that control, which might be of particular interest to CORAL in terms of question-and-answer formatting. In the following list, those clauses in bold pertain to security (according to the author of the present report) and the "basic" three-star (***) rating:

- *IA 1 General information on a CSP*
  - *Profile, service, location, governing law, certificates*
- *IA 2 Contract*
  - *Adequate contract terms*
    - *Conclusion of contract*
    - *Terms of cancellation*
  - *Rules for data management*
    - *Location of data*
    - *Data accessed by customer*
  - *Legal data protection requirements*
    - *Technical and organizational procedures*
    - *Local data protection requirements*
  - *Service level agreements*
    - *General requirements*
    - *Verifiability*
    - *Service disruption*
    - *Terms in case of bankruptcy*
  - *Terms for pricing and cost allocation*

        - *Terms for pricing and cost allocation*
    - *Specific questions (optional)*
        - *Special use case requirements*
- ***IA 3 Security and data protection***
    - ***Security management***
        - ***Organizational requirements***
        - ***Preventive measures***
        - *Audit ability*
    - ***Technical security measures***
        - ***Cyber security***
        - *Resilience*
        - ***Password management***
    - ***Data confidentiality***
        - ***Data encryption***
        - *Access control*
        - ***Separation control***
    - *Cryptographic assessment*
        - *Credential cryptographic controls*
- ***IA 4 CSP Data center***
    - ***Proper facility and IT co-location management***
        - *Proof of minimum requirements of data center operations and facility management*
        - *Basic area security*
        - ***Access control***
        - ***Fail-safe operation***
        - *Data center organization*
- ***IA 5 Service management and customer support***
    - *Appropriate customer support*
        - *Validation of support service*
    - ***Appropriate service management***
        - *Validation of basic principles of service management*
        - *Incident management*
        - *Problem management*
        - *Change management*
        - *Configuration management*
        - *Release management*
        - *Capacity management*
        - *Availability management*
        - *Emergency management*
        - *Risk management*
        - *Operation management*
        - *Backup management*

        - *Quality management*
- ***IA 6I Fundamentals of IaaS***
    - *Reference architecture*
        - *Analysis of employed technology*
    - *System management*
        - *Self-provisioning*
    - ***Security***
        - ***Access hypervisor***
    - *License management*
        - *Operating system*
- ***IA 6P Fundamentals of PaaS***
    - *Reference architecture*
        - *Analysis of employed technologies*
    - ***Security***
        - ***Isolation***
    - *Management*
        - *Deployment*
- *IA 6S Fundamentals of SaaS*
    - *Interoperability and portability*
        - *Export format*
        - *Integration*
    - *User support*
        - *Documentation*
- *IA 7 GDPR*
    - *Provider-related data protection criteria*
        - *Data protection representative*
        - *Data protection organization*
    - *Product-related data protection criteria*
        - *Support for data subject rights*
    - *Process-related data protection criteria*
        - *Data protection planning*
        - *Data protection design*
    - *Other data-protection-related criteria*
        - *Record of processing activities*
        - *GDPR and IT security*
        - *Training of employees of the cloud service provider*
        - *Data protection impact assessment*
        - *Contractual compliance with GDPR*
        - *GDPR organization and documentation*
    - *Technical data privacy assessment*
        - *Credential add-on controls*

ITU-T X.1631 (07/2015) | ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Name	
ITU-T X.1631 (07/2015) | ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services	
Developing body	**Date of publication**
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection *ITU-T Study Group 17 Security*	*12/2015*
Type	**Applies to**
Requirements/guidelines/controls	*Services: Cloud*
Scope	
"ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: - *additional implementation guidance for relevant controls specified in ISO/IEC 27002;* - *additional controls with implementation guidance that specifically relate to cloud services.* *This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers." – Scope of* [35]	
Relation to CSA	
This standard is used as one among several sources of sets of Cloud security controls to consider in the candidate EUCS scheme [8].	
Weblinks	**Accessibility**
https://www.iso.org/standard/43757.html *https://www.itu.int/itu-t/recommendations/rec.aspx?id=12490*	*Not free*
Specific relevance for CORAL	

The standard provides a list of controls for Cloud service providers and Cloud service customers.
The structure of the topics covered is that of ISO/IEC 27002:2013 [36] - since this is a list of controls that complements those of that standard - to which are added the clauses of the extended control set for Cloud provided in Annex A of ISO/IEC 27017:2015 [35]. In the list below, in bold are those control sets that have either cloud-provider-specific "guidance" or cloud-provider-specific "other information". The clause numbering is that of the standard. Those with "CLD" appended to them are from the ISO/IEC 27017:2015 annex.
 	
- ***5 Information security policies***
  - ***5.1 Management direction for information security***
  - ***5.1.1 Policies for information security***
  - *5.1.2 Review of the policies for information security*
- ***6 Organization of information security***
  - ***6.1 Internal organization***
  - ***6.1.1 Information security roles and responsibilities***	

- ***6.1.2 Segregation of duties***
- ***6.1.3 Contact with authorities***
- ***6.1.4 Contact with special interest groups***
- ***6.1.5 Information security in project management***

- ***6.2 Mobile devices and teleworking***
- ***6.2.1 Mobile device policy***
- ***6.2.2 Teleworking***

- ***CLD.6.3 Relationship between cloud service customer and cloud service provider***
- ***CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment***

- ***7 Human resource security***
  - ***7.1 Prior to employment***
    - ***7.1.1 Screening***
    - ***7.1.2 Terms and conditions of employment***
  - ***7.2 During employment***
    - ***7.2.1 Management responsibilities***
    - ***7.2.2 Information security awareness, education and training***
    - ***7.2.3 Disciplinary process***
  - ***7.3 Termination and change of employment***
    - ***7.3.1 Termination or change of employment responsibilities***
- ***8 Asset management***
  - ***8.1 Responsibility for assets***
    - ***8.1.1 Inventory of assets***
    - ***8.1.2 Ownership of assets***
    - ***8.1.3 The acceptable use of assets***
    - ***8.1.4 Return of assets***
    - ***CLD.8.1.5 Removal of cloud service customer assets***
  - ***8.2 Information classification***
    - ***8.2.1 Classification of information***
    - ***8.2.2 Labelling of information***
    - ***8.2.3 Handling of assets***
  - ***8.3 Media handling***
    - ***8.3.1 Management of removable media***
    - ***8.3.2 Disposal of media***
    - ***8.3.3 Physical media transfer***
- ***9 Access control***
  - ***9.1 Business requirements of access control***
    - ***9.1.1 Access control policy***
    - ***9.1.2 Access to networks and network services***
  - ***9.2 User access management***
    - ***9.2.1 User registration and deregistration***
    - ***9.2.2 User access provisioning***

- ***9.2.3 Management of privileged access rights***
- ***9.2.4 Management of secret authentication information of users***
- *9.2.5 Review of user access rights*
- *9.2.6 Removal or adjustment of access rights*

o *9.3 User responsibilities*

- *9.3.1 Use of secret authentication information*

o ***9.4 System and application access control***

- ***9.4.1 Information access restriction***
- *9.4.2 Secure log-on procedures*
- *9.4.3 Password management system*
- ***9.4.4 Use of privileged utility programs***
- *9.4.5 Access control to program source code*

o ***CLD.9.5 Access control of cloud service customer data in shared virtual environment***

- ***CLD.9.5.1 Segregation in virtual computing environments***
- ***CLD.9.5.2 Virtual machine hardening***

- ***10 Cryptography***
  - o ***10.1 Cryptographic controls***
    - ***10.1.1 Policy on the use of cryptographic controls***
    - *10.1.2 Key management*
- ***11 Physical and environmental security***
  - o *11.1 Secure areas*
    - *11.1.1 Physical security perimeter*
    - *11.1.2 Physical entry controls*
    - *11.1.3 Securing offices, rooms and facilities*
    - *11.1.4 Protecting against external and environmental threats*
    - *11.1.5 Working in secure areas*
    - *11.1.6 Delivery and loading areas*
  - o ***11.2 Equipment***
    - *11.2.1 Equipment siting and protection*
    - *11.2.2 Supporting utilities*
    - *11.2.3 Cabling security*
    - *11.2.4 Equipment maintenance*
    - *11.2.5 Removal of assets*
    - *11.2.6 Security of equipment and assets off-premises*
    - ***11.2.7 Secure disposal or reuse of equipment***
    - *11.2.8 Unattended user equipment*
    - *11.2.9 Clear desk and clear screen policy*
- ***12 Operations security***
  - o ***12.1 Operational procedures and responsibilities***
    - *12.1.1 Documented operating procedures*
    - ***12.1.2 Change management***
    - ***12.1.3 Capacity management***

- *12.1.4 Separation of development, testing and operational environments*
- ***CLD.12.1.5 Administrator's operational security***

o *12.2 Protection from malware*
- *12.2.1 Controls against malware*

o ***12.3 Backup***
- ***12.3.1 Information backup***

o ***12.4 Logging and monitoring***
- ***12.4.1 Event logging***
- *12.4.2 Protection of log information*
- ***12.4.3 Administrator and operator logs***
- ***12.4.4 Clock synchronization***
- ***CLD.12.4.5 Monitoring of Cloud Services***

o *12.5 Control of operational software*
- *12.5.1 Installation of software on operational systems*

o ***12.6 Technical vulnerability management***
- ***12.6.1 Management of technical vulnerabilities***
- *12.6.2 Restrictions on software installation*

o *12.7 Information systems audit considerations*
- *12.7.1 Information systems audit controls*

- ***13 Communications security***

o ***13.1 Network security management***
- *13.1.1 Network controls*
- *13.1.2 Security of network services*
- ***13.1.3 Segregation in networks***
- ***CLD.13.1.4 Alignment of security management for virtual and physical networks***

o *13.2 Information transfer*
- *13.2.1 Information transfer policies and procedures*
- *13.2.2 Agreements on information transfer*
- *13.2.3 Electronic messaging*
- *13.2.4 Confidentiality or non-disclosure agreements*

- ***14 System acquisition, development and maintenance***

o ***14.1 Security requirements of information systems***
- ***14.1.1 Information security requirements analysis and specification***
- *14.1.2 Securing applications services on public networks*
- *14.1.3 Protecting application services transactions*

o ***14.2 Security in development and support processes***
- ***14.2.1 Secure development policy***
- *14.2.2 System change control procedures*
- *14.2.3 Technical review of applications after operating platform changes*
- *14.2.4 Restrictions on changes to software packages*
- *14.2.5 Secure system engineering principles*

- *14.2.6 Secure development environment*
- *14.2.7 Outsourced development*
- *14.2.8 System security testing*
- *14.2.9 System acceptance testing*

o *14.3 Test data*

- *14.3.1 Protection of test data*

- ***15 Supplier relationships***

o ***15.1 Information security in supplier relationships***

- *15.1.1 Information security policy for supplier relationships*
- ***15.1.2 Addressing security within supplier agreements***
- ***15.1.3 Information and communication technology supply chain***

o *15.2 Supplier service delivery management*

- *15.2.1 Monitoring and review of supplier services*
- *15.2.2 Managing changes to supplier services*

- ***16 Information security incident management***

o ***16.1 Management of information security incidents and improvements***

- ***16.1.1 Responsibilities and procedures***
- ***16.1.2 Reporting information security events***
- *16.1.3 Reporting information security weaknesses*
- *16.1.4 Assessment of and decision on information security events*
- *16.1.5 Response to information security incidents*
- *16.1.6 Learning from information security incidents*
- ***16.1.7 Collection of evidence***

- *17 Information security aspects of business continuity management*

o *17.1 Information security continuity*

- *17.1.1 Planning information security continuity*
- *17.1.2 Implementing information security continuity*
- *17.1.3 Verify, review and evaluate information security continuity*

o *17.2 Redundancies*

- *17.2.1 Availability of information processing facilities*

- ***18 Compliance***

o ***18.1 Compliance with legal and contractual requirements***

- ***18.1.1 Identification of applicable legislation and contractual requirements***
- ***18.1.2 Intellectual property rights***
- ***18.1.3 Protection of records***
- ***18.1.4 Privacy and protection of personally identifiable information***
- ***18.1.5 Regulation of cryptographic controls***

o ***18.2 Information security reviews***

- ***18.2.1 Independent review of information security***
- *18.2.2 Compliance with security policies and standards*
- *18.2.3 Technical compliance review*

SecNumCloud

Name	
Prestataires de services d'informatique en nuage (SecNumCloud) v3.1	
Developing body	**Date of publication**
ANSSI (France)	*11/06/2018*
Type	**Applies to**
Requirements/guidelines/controls	*Services: Cloud*
Scope	
This document is a requirements list proposed by the French national cybersecurity agency ANSSI ("Agence Nationale de la Sécurité des Systèmes d'Information") for Cloud computing service provision. Service providers that are assessed as compliant to this requirements list are labelled "qualifiés" by ANSSI, who thus vouches for a good level of security. A service provider shall be "qualifié" in order to be used by a French public administration. The framework covers the three classic cloud service models of IaaS, PaaS, and SaaS. The standard is heavily based on ISO/IEC 27001 [31]. *See* [37] *for more details.*	
Relation to CSA	
This standard is used as one among several sources of sets of Cloud security controls to consider in the candidate EUCS scheme [8]. In particular, the scheme follows a similar structure.	
Weblinks	**Accessibility**
https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/ *https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf*	*Free*
Specific relevance for CORAL	

The stated level of security achieved by the document is one deemed sufficient when handling the storage and processing of data for which a security incident would have limited consequences on the customer (author translation of "le stockage et le traitement de données pour lesquelles un incident de sécurité aurait une conséquence limitée pour le commanditaire", see Clause 4 of [37]). Thus, the guideline is for a security level corresponding to this deliverable.
The document claims to be structured as Annex A in ISO/IEC 27001, but this appears to be not exactly the case, at least not between this particular version and ISO/IEC 27001:2013. Furthermore, while the structures may be similar, the requirements as written in the document appear directly tailored to a cloud service provider, and not just a generic organization.
The requirements are listed in their original language (French).
 	
- *5. Politiques de sécurité de l'information et gestion du risque*
  - *5.1. Principes*
  - *5.2. Politique de sécurité de l'information*
  - *5.3. Appréciation des risques*
- *6. Organisation de la sécurité de l'information*
  - *6.1. Fonctions et responsabilités liées à la sécurité de l'information*
  - *6.2. Séparation des tâches*	

- *11.7. Maintenance des matériels*
- *11.8. Sortie des actifs*
- *11.9. Recyclage sécurisé du matériel*
- *11.10. Matériel en attente d'utilisation*

- *12. Sécurité liée à l'exploitation*
  - *12.1. Procédures d'exploitation documentées*
  - *12.2. Gestion des changements*
  - *12.3. Séparation des environnements de développement, de test et d'exploitation*
  - *12.4. Mesures contre les codes malveillants*
  - *12.5. Sauvegarde des informations*
  - *12.6. Journalisation des événements*
  - *12.7. Protection de l'information journalisée*
  - *12.8. Synchronisation des horloges*
  - *12.9. Analyse et corrélation des événements*
  - *12.10. Installation de logiciels sur des systèmes en exploitation*
  - *12.11. Gestion des vulnérabilités techniques*
  - *12.12. Administration*
- *13. Sécurité des communications*
  - *13.1. Cartographie du système d'information.*
  - *13.2. Cloisonnement des réseaux*
  - *13.3. Surveillance des réseaux*
- *14. Acquisition, développement et maintenance des systèmes d'information*
  - *14.1. Politique de développement sécurisé*
  - *14.2. Procédures de contrôle des changements de système*
  - *14.3. Revue technique des applications après changement apporté à la plateforme d'exploitation*
  - *14.4. Environnement de développement sécurisé*
  - *14.5. Développement externalisé*
  - *14.6. Test de la sécurité et conformité du système*
  - *14.7. Protection des données de test*
- *15. Relations avec les tiers*
  - *15.1. Identification des tiers*
  - *15.2. La sécurité dans les accords conclus avec les tiers*
  - *15.3. Surveillance et revue des services des tiers*
  - *15.4. Gestion des changements apportés dans les services des tiers*
  - *15.5. Engagements de confidentialité*
- *16. Gestion des incidents liés à la sécurité de l'information*
  - *16.1. Responsabilités et procédures*
  - *16.2. Signalements liés à la sécurité de l'information*
  - *16.3. Appréciation des événements liés à la sécurité de l'information et prise de décision*

- *o 16.4. Réponse aux incidents liés à la sécurité de l'information*
- *o 16.5. Tirer des enseignements des incidents liés à la sécurité de l'information*
- *o 16.6. Recueil de preuves*

- *17. Continuité d'activité*
  - *o 17.1. Organisation de la continuité d'activité*
  - *o 17.2. Mise en œuvre de la continuité d'activité*
  - *o 17.3. Vérifier, revoir et évaluer la continuité d'activité*
  - *o 17.4. Disponibilité des moyens de traitement de l'information*
- *18. Conformité*
  - *o 18.1. Identification de la législation et des exigences contractuelles applicables*
  - *o 18.2. Revue indépendante de la sécurité de l'information*
  - *o 18.3. Conformité avec les politiques et les normes de sécurité*
  - *o 18.4. Examen de la conformité technique*
- *19. Exigences supplémentaires*
  - *o 19.1. Convention de service*
  - *o 19.2. Localisation des données*
  - *o 19.3. Régionalisation*
  - *o 19.4. Fin de contrat*
  - ***o** 19.5. Protection des données à caractère personnel*

The Cloud Computing Compliance Criteria Catalogue (C5)

Name	
Cloud Computing Compliance Criteria Catalogue - C5:2020	
Developing body	**Date of publication**
Federal Office for Information Security (Germany)	*10/2020*
Type	**Applies to**
Evaluation/assessment/testing	*Services: Cloud*
Scope	
This is a catalogue of criteria [38] *established by the German BSI (Bundesamt für Sicherheit in der Informationstechnik) for assessing the information security level of cloud service providers.*	
Relation to CSA	
This standard is used as one among several sources of sets of Cloud security controls to consider in the candidate EUCS scheme [8]. In particular, the scheme follows a similar structure.	
Weblinks	**Accessibility**
https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=3*	*Free*
Specific relevance for CORAL	
The criteria can be examined to provide a list of questions to answer for a cloud service provider.	

Within each criteria category, the criteria that are given are divided between basic criteria and additional criteria. Basic criteria are considered sufficient for ensuring a basic level of protection that is for the "minimum level of information security that a cloud service must offer when cloud customers use it to process information that has a normal need for protection" (Clause 2.1, p. 14 in [38]). Note that every single criteria category has both basic and additional criteria. Thus, for a "low level, low complexity" service, all criteria categories should be considered.

- *4 Information on the General Conditions of the Cloud Service*
  - *BC-01 Information on jurisdiction and locations*
  - *BC-02 Information on availability and incident handling during regular operation*
  - *BC-03 Information on recovery parameters in emergency operation*
  - *BC-04 Information on the availability of the data centre*
  - *BC-05 Information on how investigation enquiries from government authorities are handled*
  - *BC-06 Information on certifications or attestations*
- *5 Basic Criteria, Additional Criteria and Supplementary Information*
  - *5.1 Organisation of Information Security (OIS)*
    - *OIS-01 Information Security Management System (ISMS)*
    - *OIS-02 Information Security Policy*
    - *OIS-03 Interfaces and Dependencies*
    - *OIS-04 Segregation of Duties*
    - *OIS-05 Contact with Relevant Government Agencies and Interest Groups*
    - *OIS-06 Risk Management Policy*
    - *OIS-07 Application of the Risk Management Policy*
  - *5.2 Security Policies and Instructions (SP)*
    - *SP-01 Documentation, communication and provision of policies and instructions*
    - *SP-02 Review and Approval of Policies and Instructions*
    - *SP-03 Exceptions from Existing Policies and Instructions*
  - *5.3 Personnel (HR)*
    - *HR-01 Verification of qualification and trustworthiness*
    - *HR-02 Employment terms and conditions*
    - *HR-03 Security training and awareness programme*
    - *HR-04 Disciplinary measures*
    - *HR-05 Responsibilities in the event of termination or change of employment*
    - *HR-06 Confidentiality agreements*
  - *5.4 Asset Management (AM)*
    - *AM-01 Asset Inventory*
    - *AM-02 Acceptable Use and Safe Handling of Assets Policy*
    - *AM-03 Commissioning of Hardware*
    - *AM-04 Decommissioning of Hardware*

- *AM-05 Commitment to Permissible Use, Safe Handling and Return of Assets*
- *AM-06 Asset Classification and Labelling 50*

o *5.5 Physical Security (PS)*

- *PS-01 Physical Security and Environmental Control Requirements*
- *PS-02 Redundancy model*
- *PS-03 Perimeter Protection*
- *PS-04 Physical site access control*
- *PS-05 Protection from fire and smoke*
- *PS-06 Protection against interruptions caused by power failures and other such risks*
- *PS-07 Surveillance of operational and environmental parameters*

o *5.6 Operations (OPS)*

- *OPS-01 Capacity Management – Planning*
- *OPS-02 Capacity Management – Monitoring*
- *OPS-03 Capacity Management – Controlling of Resources*
- *OPS-04 Protection Against Malware – Concept*
- *OPS-05 Protection Against Malware – Implementation*
- *OPS-06 Data Backup and Recovery – Concept*
- *OPS-07 Data Backup and Recovery – Monitoring*
- *OPS-08 Data Backup and Recovery – Regular Testing*
- *OPS-09 Data Backup and Recovery – Storage*
- *OPS-10 Logging and Monitoring – Concept*
- *OPS-11 Logging and Monitoring – Metadata Management Concept*
- *OPS-12 Logging and Monitoring – Access, Storage and Deletion*
- *OPS-13 Logging and Monitoring – Identification of Events*
- *OPS-14 Logging and Monitoring – Storage of the Logging Data*
- *OPS-15 Logging and Monitoring – Accountability*
- *OPS-16 Logging and Monitoring – Configuration*
- *OPS-17 Logging and Monitoring – Availability of the Monitoring Software*
- *OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Concept*
- *OPS-19 Managing Vulnerabilities, Malfunctions and Errors – Penetration Tests*
- *OPS-20 Managing Vulnerabilities, Malfunctions and Errors – Measurements, Analyses and Assessments of Procedures*
- *OPS-21 Involvement of Cloud Customers in the Event of Incidents*
- *OPS-22 Testing and Documentation of known Vulnerabilities*
- *OPS-23 Managing Vulnerabilities, Malfunctions and Errors – System Hardening*
- *OPS-24 Separation of Datasets in the Cloud Infrastructure*

o *5.7 Identity and Access Management (IDM)*

- *IDM-01 Policy for user accounts and access rights*
- *IDM-02 Granting and change of user accounts and access rights*
- *IDM-03 Locking and withdrawal of user accounts in the event of inactivity or*

multiple failed logins
- *IDM-04 Withdraw or adjust access rights as the task area changes*
- *IDM-05 Regular review of access rights*
- *IDM-06 Privileged access rights*
- *IDM-07 Access to cloud customer data*
- *IDM-08 Confidentiality of authentication information*
- *IDM-09 Authentication mechanisms*

o *5.8 Cryptography and Key Management (CRY)*
- *CRY-01 Policy for the use of encryption procedures and key management*
- *CRY-02 Encryption of data for transmission (transport encryption)*
- *CRY-03 Encryption of sensitive data for storage*
- *CRY-04 Secure key management*

o *5.9 Communication Security (COS)*
- *COS-01 Technical safeguards*
- *COS-02 Security requirements for connections in the Cloud Service Provider's network*
- *COS-03 Monitoring of connections in the Cloud Service Provider's network*
- *COS-04 Cross-network access*
- *COS-05 Networks for administration*
- *COS-06 Segregation of data traffic in jointly used network environments*
- *COS-07 Documentation of the network topology*
- *COS-08 Policies for data transmission*

o *5.10 Portability and Interoperability (PI)*
- *PI-01 Documentation and safety of input and output interfaces*
- *PI-02 Contractual agreements for the provision of data*
- *PI-03 Secure deletion of data*

o *5.11 Procurement, Development and Modification of Information Systems (DEV)*
- *DEV-01 Policies for the development/procurement of information systems*
- *DEV-02 Outsourcing of the development*
- *DEV-03 Policies for changes to information systems*
- *DEV-04 Safety training and awareness programme regarding continuous software delivery and associated systems, components or tools*
- *DEV-05 Risk assessment, categorisation and prioritisation of changes*
- *DEV-06 Testing changes*
- *DEV-07 Logging of changes*
- *DEV-08 Version Control*
- *DEV-09 Approvals for provision in the production environment*
- *DEV-10 Separation of environments*

o *5.12 Control and Monitoring of Service Providers and Suppliers (SSO)*
- *SSO-01 Policies and instructions for controlling and monitoring third parties*
- *SSO-02 Risk assessment of service providers and suppliers*
- *SSO-03 Directory of service providers and suppliers*

- *SSO-04 Monitoring of compliance with requirements*
- *SSO-05 Exit strategy for the receipt of benefits*

o *5.13 Security Incident Management (SIM)*
- *SIM-01 Policy for security incident management*
- *SIM-02 Processing of security incidents*
- *SIM-03 Documentation and reporting of security incidents*
- *SIM-04 Duty of the users to report security incidents to a central body*
- *SIM-05 Evaluation and learning process*

o *5.14 Business Continuity Management (BCM)*
- *BCM-01 Top management responsibility*
- *BCM-02 Business impact analysis policies and instructions*
- *BCM-03 Planning business continuity*
- *BCM-04 Verification, updating and testing of the business continuity*

o *5.15 Compliance (COM)*
- *COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements*
- *COM-02 Policy for planning and conducting audits*
- *COM-03 Internal audits of the information security management system*
- *COM-04 Information on information security performance and management assessment of the ISMS*

o *5.16 Dealing with investigation requests from government agencies (INQ)*
- *INQ-01 Legal Assessment of Investigative Inquiries*
- *INQ-02 Informing Cloud Customers about Investigation Requests*
- *INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests*
- *INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests*

o *5.17 Product Safety and Security (PSS)*
- *PSS-01 Guidelines and Recommendations for Cloud Customers*
- *PSS-02 Identification of Vulnerabilities of the Cloud Service*
- *PSS-03 Online Register of Known Vulnerabilities*
- *PSS-04 Error handling and Logging Mechanisms*
- *PSS-05 Authentication Mechanisms*
- *PSS-06 Session Management*
- *PSS-07 Confidentiality of Authentication Information*
- *PSS-08 Roles and Rights Concept*
- *PSS-09 Authorisation Mechanisms*
- *PSS-10 Software Defined Networking*
- *PSS-11 Images for Virtual Machines and Containers*
- *PSS-12 Locations of Data Processing and Storage*

The Cloud Security Alliance Cloud Control Matrix and Consensus Assessments Initiative Questionnaire

Name	
Cloud Security Alliance Cloud Control Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ) v4.0.2	
Developing body	**Date of publication**
Cloud Security Alliance	*06/07/2021*
Type	**Applies to**
Requirements/guidelines/controls	*Services: Cloud*
Scope	
The Cloud Security Alliance Cloud Control Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ) are used by the Cloud Security Alliance in their Security, Trust, Assurance, and Risk (STAR) program. This is a program that offers increasing levels of assurance regarding compliance with the CCM. There are two base STAR levels, within which are level variations. See [39].	
Relation to CSA	
The Cloud Security Alliance is mentioned as a body of interest regarding Cloud security in ENISA's publication [4]. *However, it appears that neither the CCM nor the CAIQ are directly related to the proposed EUCS scheme* [8].	
Weblinks	**Accessibility**
https://cloudsecurityalliance.org/ *https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/*	*Free*
Specific relevance for CORAL	

There are questions readily available for a self-assessment here.
According to the STAR system framework, all CCM controls are applicable regardless of which STAR level is pursued, so none of the controls below are "privileged" (that is, marked in bold) in this sense. However, not all controls apply to a Cloud Service Provider (CSP). Some apply exclusively to the Cloud Service Customer (CSC). Thus, in bold one finds those controls that are considered owned entirely or in part by the CSP (some are co-owned between CSC and CSP). Furthermore, this also typically depends on the cloud service model considered, which can be one of IaaS, PaaS, or SaaS. When applicable, this is also specified (by the authors) in parentheses.
 	
- ***Audit & Assurance***
  - ***A&A-01Audit and Assurance Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***A&A-02Independent Assessments (IaaS, PaaS, SaaS)***
  - ***A&A-03Risk Based Planning Assessment (IaaS, PaaS, SaaS)***
  - ***A&A-04Requirements Compliance (IaaS, PaaS, SaaS)***
  - ***A&A-05Audit Management Process (IaaS, PaaS, SaaS)***
  - ***A&A-06Remediation (IaaS, PaaS, SaaS)***
- ***Application & Interface Security***
  - ***AIS-01 Application and Interface Security Policy and Procedures (IaaS, SaaS)***
  - ***AIS-02 Application Security Baseline Requirements (IaaS, PaaS, SaaS)***	

- *AIS-03 Application Security Metrics (IaaS, PaaS, SaaS)*
- *AIS-04 Secure Application Design and Development (IaaS, PaaS, SaaS)*
- *AIS-05 Automated Application Security Testing (IaaS, PaaS, SaaS)*
- *AIS-06 Automated Secure Application Deployment (IaaS, PaaS, SaaS)*
- *AIS-07 Application Vulnerability Remediation (IaaS, PaaS, SaaS)*

- *Business Continuity Management and Operational Resilience*
  - *BCR-01 Business Continuity Management Policy and Procedures (IaaS, PaaS, SaaS)*
  - *BCR-02 Risk Assessment and Impact Analysis (IaaS, PaaS, SaaS)*
  - *BCR-03 Business Continuity Strategy (IaaS, PaaS, SaaS)*
  - *BCR-04 Business Continuity Planning (IaaS, PaaS, SaaS)*
  - *BCR-05 Documentation (IaaS, PaaS, SaaS)*
  - *BCR-06 Business Continuity Exercises (IaaS, PaaS, SaaS)*
  - *BCR-07 Communication (IaaS, PaaS, SaaS)*
  - *BCR-08 Backup (IaaS, PaaS, SaaS)*
  - *BCR-09 Disaster Response Plan (IaaS, PaaS, SaaS)*
  - *BCR-10 Response Plan Exercise (IaaS, PaaS, SaaS)*
  - *BCR-11 Equipment Redundancy (IaaS, PaaS, SaaS)*
- *Change Control and Configuration Management*
  - *CCC-01 Change Management Policy and Procedures (IaaS, PaaS, SaaS)*
  - *CCC-02 Quality Testing (IaaS, PaaS, SaaS)*
  - *CCC-03 Change Management Technology (IaaS, PaaS, SaaS)*
  - *CCC-04 Unauthorized Change Protection (IaaS, PaaS, SaaS)*
  - *CCC-05 Change Agreements (IaaS, PaaS, SaaS)*
  - *CCC-06 Change Management Baseline (IaaS, PaaS, SaaS)*
  - *CCC-07 Detection of Baseline Deviation (IaaS, PaaS, SaaS)*
  - *CCC-08 Exception Management (IaaS, PaaS, SaaS)*
  - *CCC-09 Change Restoration (IaaS, PaaS, SaaS)*
- *Cryptography, Encryption & Key Management*
  - *CEK-01 Encryption and Key Management Policy and Procedures (IaaS, PaaS, SaaS)*
  - *CEK-02 CEK Roles and Responsibilities (IaaS, PaaS, SaaS)*
  - *CEK-03 Data Encryption (IaaS, PaaS, SaaS)*
  - *CEK-04 Encryption Algorithm (IaaS, PaaS, SaaS)*
  - *CEK-05 Encryption Change Management (IaaS, PaaS, SaaS)*
  - *CEK-06 Encryption Change Cost Benefit Analysis (IaaS, PaaS, SaaS)*
  - *CEK-07 Encryption Risk Management (IaaS, PaaS, SaaS)*
  - *CEK-08 CSC Key Management Capability (IaaS, PaaS, SaaS)*
  - *CEK-09 Encryption and Key Management Audit (IaaS, PaaS, SaaS)*
  - *CEK-10 Key Generation (IaaS, PaaS, SaaS)*
  - *CEK-11 Key Purpose (IaaS, PaaS, SaaS)*
  - *CEK-12 Key Rotation (IaaS, PaaS, SaaS)*
  - *CEK-13 Key Revocation (IaaS, PaaS, SaaS)*

- ***CEK-14 Key Destruction (IaaS, PaaS, SaaS)***
- ***CEK-15 Key Activation (IaaS, PaaS, SaaS)***
- ***CEK-16 Key Suspension (IaaS, PaaS, SaaS)***
- ***CEK-17 Key Deactivation (IaaS, PaaS, SaaS)***
- ***CEK-18 Key Archival (IaaS, PaaS, SaaS)***
- ***CEK-19 Key Compromise (IaaS, PaaS, SaaS)***
- ***CEK-20 Key Recovery (IaaS, PaaS, SaaS)***
- ***CEK-21 Key Inventory Management (IaaS, PaaS, SaaS)***

- ***Datacenter Security***
  - ***DCS-01 Off-Site Equipment Disposal Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***DCS-02 Off-Site Transfer Authorization Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***DCS-03 Secure Area Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***DCS-04 Secure Media Transportation Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***DCS-05 Assets Classification (IaaS, PaaS, SaaS)***
  - ***DCS-06 Assets Cataloguing and Tracking (IaaS, PaaS, SaaS)***
  - ***DCS-07 Controlled Access Points (IaaS, PaaS, SaaS)***
  - ***DCS-08 Equipment Identification (IaaS, PaaS, SaaS)***
  - ***DCS-09 Secure Area Authorization (IaaS, PaaS, SaaS)***
  - ***DCS-10 Surveillance System (IaaS, PaaS, SaaS)***
  - ***DCS-11 Unauthorized Access Response Training (IaaS, PaaS, SaaS)***
  - ***DCS-12 Cabling Security (IaaS, PaaS, SaaS)***
  - ***DCS-13 Environmental Systems (IaaS, PaaS, SaaS)***
  - ***DCS-14 Secure Utilities (IaaS, PaaS, SaaS)***
  - ***DCS-15 Equipment Location (IaaS, PaaS, SaaS)***
- ***Data Security and Privacy Lifecycle Management***
  - *DSP-01 Security and Privacy Policy and Procedures*
  - ***DSP-02 Secure Disposal (IaaS, PaaS, SaaS)***
  - ***DSP-03 Data Inventory (IaaS, PaaS, SaaS)***
  - *DSP-04 Data Classification*
  - *DSP-05 Data Flow Documentation*
  - *DSP-06 Data Ownership and Stewardship*
  - ***DSP-07 Data Protection by Design and Default (IaaS, PaaS, SaaS)***
  - *DSP-08 Data Privacy by Design and Default*
  - *DSP-09 Data Protection Impact Assessment*
  - *DSP-10 Sensitive Data Transfer*
  - *DSP-11 Personal Data Access, Reversal, Rectification and Deletion*
  - *DSP-12 Limitation of Purpose in Personal Data Processing*
  - *DSP-13 Personal Data Sub-processing*
  - *DSP-14 Disclosure of Data Sub-processors*
  - *DSP-15 Limitation of Production Data Use*
  - *DSP-16 Data Retention and Deletion*

- *DSP-17 Sensitive Data Protection*
- ***DSP-18 Disclosure Notification (IaaS, PaaS, SaaS)***
- ***DSP-19 Data Location (IaaS, PaaS, SaaS)***

- ***Governance, Risk and Compliance***
  - ***GRC-01 Governance Program Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***GRC-02 Risk Management Program (IaaS, PaaS, SaaS)***
  - ***GRC-03 Organizational Policy Reviews (IaaS, PaaS, SaaS)***
  - ***GRC-04 Policy Exception Process (IaaS, PaaS, SaaS)***
  - ***GRC-05 Information Security Program (IaaS, PaaS, SaaS)***
  - ***GRC-06 Governance Responsibility Model (IaaS, PaaS, SaaS)***
  - ***GRC-07 Information System Regulatory Mapping (IaaS, PaaS, SaaS)***
  - ***GRC-08 Special Interest Groups (IaaS, PaaS, SaaS)***
- ***Human Resources***
  - ***HRS-01 Background Screening Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***HRS-02 Acceptable Use of Technology Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***HRS-03 Clean Desk Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***HRS-04 Remote and Home Working Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***HRS-05 Asset returns (IaaS, PaaS, SaaS)***
  - ***HRS-06 Employment Termination (IaaS, PaaS, SaaS)***
  - ***HRS-07 Employment Agreement Process (IaaS, PaaS, SaaS)***
  - ***HRS-08 Employment Agreement Content (IaaS, PaaS, SaaS)***
  - ***HRS-09 Personnel Roles and Responsibilities (IaaS, PaaS, SaaS)***
  - ***HRS-10 Non-Disclosure Agreements (IaaS, PaaS, SaaS)***
  - ***HRS-11 Security Awareness Training (IaaS, PaaS, SaaS)***
  - ***HRS-12 Personal and Sensitive Data Awareness and Training (IaaS, PaaS, SaaS)***
  - ***HRS-13 Compliance User Responsibility (IaaS, PaaS, SaaS)***
- ***Identity & Access Management***
  - ***IAM-01 Identity and Access Management Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***IAM-02 Strong Password Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***IAM-03 Identity Inventory (IaaS, PaaS, SaaS)***
  - ***IAM-04 Separation of Duties (IaaS, PaaS, SaaS)***
  - ***IAM-05 Least Privilege (IaaS, PaaS, SaaS)***
  - ***IAM-06 User Access Provisioning (IaaS, PaaS, SaaS)***
  - ***IAM-07 User Access Changes and Revocation (IaaS, PaaS, SaaS)***
  - ***IAM-08 User Access Review (IaaS, PaaS, SaaS)***
  - ***IAM-09 Segregation of Privileged Access Roles (IaaS, PaaS, SaaS)***
  - ***IAM-10 Management of Privileged Access Roles (IaaS, PaaS, SaaS)***
  - ***IAM-11 CSCs Approval for Agreed Privileged Access Roles (IaaS, PaaS, SaaS)***
  - ***IAM-12 Safeguard Logs Integrity (IaaS, PaaS, SaaS)***
  - ***IAM-13 Uniquely Identifiable Users (IaaS, PaaS, SaaS)***
  - ***IAM-14 Strong Authentication (IaaS, PaaS, SaaS)***

- *IAM-15 Passwords Management (IaaS, PaaS, SaaS)*
- *IAM-16 Authorization Mechanisms (IaaS, PaaS, SaaS)*

- *Interoperability & Portability*
  - *IPY-01 Interoperability and Portability Policy and Procedures (PaaS, SaaS)*
  - *IPY-02 Application Interface Availability (PaaS, SaaS)*
  - *IPY-03 Secure Interoperability and Portability Management (PaaS, SaaS)*
  - *IPY-04 Data Portability Contractual Obligations (PaaS, SaaS)*
- *Infrastructure & Virtualization Security*
  - *IVS-01 Infrastructure and Virtualization Security Policy and Procedures (IaaS, PaaS, SaaS)*
  - *IVS-02 Capacity and Resource Planning (IaaS, PaaS, SaaS)*
  - *IVS-03 Network Security (IaaS, PaaS, SaaS)*
  - *IVS-04 OS Hardening and Base Controls (IaaS, PaaS, SaaS)*
  - *IVS-05 Production and Non-Production Environments (IaaS, PaaS, SaaS)*
  - *IVS-06 Segmentation and Segregation (IaaS, PaaS, SaaS)*
  - *IVS-07 Migration to Cloud Environments (IaaS, PaaS, SaaS)*
  - *IVS-08 Network Architecture Documentation (IaaS, PaaS, SaaS)*
  - *IVS-09 Network Defense (IaaS, PaaS, SaaS)*
- *Logging and Monitoring*
  - *LOG-01 Logging and Monitoring Policy and Procedures (IaaS, PaaS, SaaS)*
  - *LOG-02 Audit Logs Protection (IaaS, PaaS, SaaS)*
  - *LOG-03 Security Monitoring and Alerting (PaaS, SaaS)*
  - *LOG-04 Audit Logs Access and Accountability (IaaS, PaaS, SaaS)*
  - *LOG-05 Audit Logs Monitoring and Response (IaaS, PaaS, SaaS)*
  - *LOG-06 Clock Synchronization (IaaS, PaaS, SaaS)*
  - *LOG-07 Logging Scope (IaaS, PaaS, SaaS)*
  - *LOG-08 Log Records (IaaS, PaaS, SaaS)*
  - *LOG-09 Log Protection (IaaS, PaaS, SaaS)*
  - *LOG-10 Encryption Monitoring and Reporting (IaaS, PaaS, SaaS)*
  - *LOG-11 Transaction/Activity Logging (IaaS, PaaS, SaaS)*
  - *LOG-12 Access Control Logs (IaaS, PaaS, SaaS)*
  - *LOG-13 Failures and Anomalies Reporting (IaaS, PaaS, SaaS)*
- *Security Incident Management, E-Discovery, & Cloud Forensics*
  - *SEF-01 Security Incident Management Policy and Procedures (IaaS, PaaS, SaaS)*
  - *SEF-02 Service Management Policy and Procedures (IaaS, PaaS, SaaS)*
  - *SEF-03 Incident Response Plans (IaaS, PaaS, SaaS)*
  - *SEF-04 Incident Response Testing (IaaS, PaaS, SaaS)*
  - *SEF-05 Incident Response Metrics (IaaS, PaaS, SaaS)*
  - *SEF-06 Event Triage Processes (IaaS, PaaS, SaaS)*
  - *SEF-07 Security Breach Notification (IaaS, PaaS, SaaS)*
  - *SEF-08 Points of Contact Maintenance (IaaS, PaaS, SaaS)*

- ***Supply Chain Management, Transparency, and Accountability***
  - ***STA-01 SSRM Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***STA-02 SSRM Supply Chain (IaaS, PaaS, SaaS)***
  - ***STA-03 SSRM Guidance (IaaS, PaaS, SaaS)***
  - ***STA-04 SSRM Control Ownership (IaaS, PaaS, SaaS)***
  - ***STA-05 SSRM Documentation Review (IaaS, PaaS, SaaS)***
  - ***STA-06 SSRM Control Implementation (IaaS, PaaS, SaaS)***
  - ***STA-07 Supply Chain Inventory (IaaS, PaaS, SaaS)***
  - ***STA-08 Supply Chain Risk Management (IaaS, PaaS, SaaS)***
  - ***STA-09 Primary Service and Contractual Agreement (IaaS, PaaS, SaaS)***
  - ***STA-10 Supply Chain Agreement Review (IaaS, PaaS, SaaS)***
  - ***STA-11 Internal Compliance Testing (IaaS, PaaS, SaaS)***
  - ***STA-12 Supply Chain Service Agreement Compliance (IaaS, PaaS, SaaS)***
  - ***STA-13 Supply Chain Governance Review (IaaS, PaaS, SaaS)***
  - *STA-14 Supply Chain Data Security Assessment (IaaS, PaaS, SaaS)*
- ***Threat & Vulnerability Management***
  - ***TVM-01 Threat and Vulnerability Management Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***TVM-02 Malware Protection Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***TVM-03 Vulnerability Remediation Schedule (IaaS, PaaS, SaaS)***
  - ***TVM-04 Detection Updates (IaaS, PaaS, SaaS)***
  - ***TVM-05 External Library Vulnerabilities (IaaS, PaaS, SaaS)***
  - ***TVM-06 Penetration Testing (IaaS, PaaS, SaaS)***
  - ***TVM-07 Vulnerability Identification (IaaS, PaaS, SaaS)***
  - ***TVM-08 Vulnerability Prioritization (IaaS, PaaS, SaaS)***
  - ***TVM-09 Vulnerability Management Reporting (IaaS, PaaS, SaaS)***
  - *TVM-10 Vulnerability Management Metrics (IaaS, PaaS, SaaS)*
- ***Universal Endpoint Management***
  - ***UEM-01 Endpoint Devices Policy and Procedures (IaaS, PaaS, SaaS)***
  - ***UEM-02 Application and Service Approval (IaaS, PaaS, SaaS)***
  - *UEM-03 Compatibility (PaaS, SaaS)*
  - *UEM-04 Endpoint Inventory*
  - ***UEM-05 Endpoint Management (SaaS)***
  - ***UEM-06 Automatic Lock Screen (SaaS)***
  - *UEM-07 Operating Systems (PaaS, SaaS)*
  - *UEM-08 Storage Encryption*
  - ***UEM-09 Anti-Malware Detection and Prevention (SaaS)***
  - ***UEM-10 Software Firewall (SaaS)***
  - ***UEM-11 Data Loss Prevention (SaaS)***
  - ***UEM-12 Remote Locate (SaaS)***
  - ***UEM-13 Remote Wipe (SaaS)***

- *UEM-14 Third-Party Endpoint Security Posture (SaaS)*

Internet of Things services

GSMA IoT Security Guidelines for IoT Service Ecosystems v2.2

Name	
GSMA IoT Security Guidelines for IoT Service Ecosystems v2.2	
Developing body	**Date of publication**
GSMA	*29/02/2020*
Type	**Applies to**
Requirements/guidelines/controls	*Products: IoT*

Scope

From the introduction of [40]: "This document is one part of a set of [...] security guideline documents that are intended to help the nascent "Internet of Things" (IoT) industry establish a common understanding of IoT security issues. The set of non-binding guideline documents promotes methodology for developing secure IoT Services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT Services."
The particular document at hand is targeted towards the elements of the "service ecosystem", that is "all components that make up the core of the IoT infrastructure" (see Section 1.2, p. 6 of [40]). This includes IoT services.

Relation to CSA

No direct relation.

Weblinks	**Accessibility**
https://www.gsma.com/ *https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/*	*Free*

Specific relevance for CORAL

The recommendations are categorized as critical, high-priority, medium-priority, and low-priority. ***According to the framework, only the critical recommendations are to be implemented in all cases. Thus, these can be reasonably interpreted as providing a baseline model of security, and hence are in bold.*** *The other recommendations are also listed, as baseline security will inevitably vary according to the specific product ("endpoint") considered. The nomenclature is that of the document.*

- ***5 Critical Recommendations***
  - ***5.1 Implement a Service Trusted Computing Base***
  - ***5.2 Define an Organizational Root of Trust***
  - ***5.3 Define a Bootstrap Method***
  - ***5.4 Define a Security Infrastructure for Systems Exposed to the Public Internet***
  - ***5.5 Define a Persistent Storage Model***
  - ***5.6 Define an Administration Model***
  - ***5.7 Define a Systems Logging and Monitoring Approach***

- ***5.8 Define an Incident Response Model***
- ***5.9 Define a Recovery Model***
- ***5.10 Define a Sunsetting Model***
- ***5.11 Define a Set of Security Classifications***
- ***5.12 Define Classifications for Sets of Data Types***

- *6 High-Priority Recommendations*
  - *6.1 Define a Clear Authorization Model*
  - *6.2 Manage the Cryptographic Architecture*
  - *6.3 Define a Communications Model*
  - *6.4 Use Network Authentication Services*
  - *6.5 Provision Servers Where Possible*
  - *6.6 Define an Update Model*
  - *6.7 Define a Breach Policy for Exposed Data*
  - *6.8 Force Authentication Through the Service Ecosystem*
  - *6.9 Implement Input Validation*
  - *6.10 Implement Output Filtering*
  - *6.11 Enforce Strong Password Policy*
  - *6.12 Define Application Layer Authentication and Authorization*
  - *6.13 Default-Open or Fail-Open Firewall Rules and System Hardening*
  - *6.14 Evaluate the Communications Privacy Mode*
- *7 Medium-Priority Recommendations*
  - *7.1 Define an Application Execution Environment*
  - *7.2 Use Partner-Enhanced Monitoring Services*
  - *7.3 Use a Private APN for Cellular Connectivity*
  - *7.4 Define a Third-Party Data Distribution Policy*
  - *7.5 Build a Third-Party Data Filter*
- *8 Low-Priority Recommendations*
  - *8.1 Rowhammer and Similar Attacks*
  - *8.2 Virtual Machine Compromises*
  - *8.3 Build an API for Users to Control Privacy Attributes*
  - *8.4 Define a False Negative/Positive Assessment Model*

Note that this guideline is part of an overall package of guidelines from GSMA, where another part covers IoT products. See the corresponding card for GSMA IoT Security Guidelines for Endpoint Ecosystems v2.2 in this document.

Telecommunications

ITU-T X.1051 (2016) | ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

Name	
ITU-T X.1051 (2016) | ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	
Developing body	**Date of publication**
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection *ITU-T Study Group 17 Security*	*12/2016*
Type	**Applies to**
Requirements/guidelines/controls	*Services: Telecommunications*
Scope	
"The scope of this Recommendation | ISO/IEC 27011:2016 is to define guidelines supporting the implementation of information security controls in telecommunications organizations. *The adoption of this Recommendation | ISO/IEC 27011:2016 will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property." – Scope of* [41]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.iso.org/standard/64143.html *https://www.itu.int/itu-t/recommendations/rec.aspx?id=12845*	*Not free*
Specific relevance for CORAL	

The standard provides a list of controls for telecommunications providers.
The structure of the topics covered is that of ISO/IEC 27002:2013 - since this is a list of controls that complements those of that standard - to which are added the clauses of the extended control set for telecommunications provided in Annex A of ISO/IEC 27011:2016. In the list below, in bold are those control sets that have either telecommunications-specific "guidance" or telecommunications-specific "other information". The clause numbering is that of the standard. Those with "TEL" appended to them are from the ISO/IEC 27011:2016 annex.
- *5 Information security policies*
  - *5.1 Management direction for information security*
  - *5.1.1 Policies for information security*
  - *5.1.2 Review of the policies for information security*
- ***6 Organization of information security***
  - ***6.1 Internal organization***
  - ***6.1.1 Information security roles and responsibilities***	

- *9.3 User responsibilities*
  - *9.3.1 Use of secret authentication information*
- *9.4 System and application access control*
  - *9.4.1 Information access restriction*
  - *9.4.2 Secure log-on procedures*
  - *9.4.3 Password management system*
  - *9.4.4 Use of privileged utility programs*
  - *9.4.5 Access control to program source code*
- ***TEL.9.5 Network access control***
  - ***TEL.9.5.1 Telecommunications carrier identification and authentication by users***

- *10 Cryptography*
  - *10.1 Cryptographic controls*
    - *10.1.1 Policy on the use of cryptographic controls*
    - *10.1.2 Key management*
- ***11 Physical and environmental security***
  - ***11.1 Secure areas***
    - ***11.1.1 Physical security perimeter***
    - ***11.1.2 Physical entry controls***
    - *11.1.3 Securing offices, rooms and facilities*
    - *11.1.4 Protecting against external and environmental threats*
    - *11.1.5 Working in secure areas*
    - *11.1.6 Delivery and loading areas*
    - ***TEL.11.1.7 Securing communication centres***
    - ***TEL.11.1.8 Securing telecommunications equipment room***
    - ***TEL.11.1.9 Securing physically isolated operation areas***
  - ***11.2 Equipment***
    - ***11.2.1 Equipment siting and protection***
    - ***11.2.2 Supporting utilities***
    - ***11.2.3 Cabling security***
    - *11.2.4 Equipment maintenance*
    - *11.2.5 Removal of assets*
    - *11.2.6 Security of equipment and assets off-premises*
    - *11.2.7 Secure disposal or reuse of equipment*
    - *11.2.8 Unattended user equipment*
    - *11.2.9 Clear desk and clear screen policy*
  - ***TEL.11.3 Security under the control of other party***
    - ***TEL.11.3.1 Equipment sited in other carriers' premises***
    - ***TEL.11.3.2 Equipment sited in user premises***
    - ***TEL.11.3.3 Interconnected telecommunications services***
- ***12 Operations security***
  - ***12.1 Operational procedures and responsibilities***

- ***12.1.1 Documented operating procedures***
- ***12.1.2 Change management***
- *12.1.3 Capacity management*
- ***12.1.4 Separation of development, testing and operational environments***

o *12.2 Protection from malware*
- *12.2.1 Controls against malware*

o *12.3 Backup*
- *12.3.1 Information backup*

o ***12.4 Logging and monitoring***
- ***12.4.1 Event logging***
- *12.4.2 Protection of log information*
- *12.4.3 Administrator and operator logs*
- *12.4.4 Clock synchronization*

o ***12.5 Control of operational software***
- ***12.5.1 Installation of software on operational systems***

o ***12.6 Technical vulnerability management***
- *12.6.1 Management of technical vulnerabilities*
- ***12.6.2 Restrictions on software installation***

o *12.7 Information systems audit considerations*
- *12.7.1 Information systems audit controls*

- ***13 Communications security***

o ***13.1 Network security management***
- *13.1.1 Network controls*
- ***13.1.2 Security of network services***
- ***13.1.3 Segregation in networks***
- ***TEL.13.1.4 Security management of telecommunications services delivery***
- ***TEL.13.1.5 Response to spam***
- ***TEL.13.1.6 Response to DoS/DDoS attacks***

o *13.2 Information transfer*
- *13.2.1 Information transfer policies and procedures*
- *13.2.2 Agreements on information transfer*
- *13.2.3 Electronic messaging*
- *13.2.4 Confidentiality or non-disclosure agreements*

- *14 System acquisition, development and maintenance*

o *14.1 Security requirements of information systems*
- *14.1.1 Information security requirements analysis and specification*
- *14.1.2 Securing applications services on public networks*
- *14.1.3 Protecting application services transactions*

o *14.2 Security in development and support processes*
- *14.2.1 Secure development policy*
- *14.2.2 System change control procedures*
- *14.2.3 Technical review of applications after operating platform changes*

- *14.2.4 Restrictions on changes to software packages*
- *14.2.5 Secure system engineering principles*
- *14.2.6 Secure development environment*
- *14.2.7 Outsourced development*
- *14.2.8 System security testing*
- *14.2.9 System acceptance testing*

o *14.3 Test data*

- *14.3.1 Protection of test data*

- ***15 Supplier relationships***

o ***15.1 Information security in supplier relationships***

- ***15.1.1 Information security policy for supplier relationships***
- ***15.1.2 Addressing security within supplier agreements***
- ***15.1.3 Information and communication technology supply chain***

o *15.2 Supplier service delivery management*

- *15.2.1 Monitoring and review of supplier services*
- *15.2.2 Managing changes to supplier services*

- ***16 Information security incident management***

o ***16.1 Management of information security incidents and improvements***

- ***16.1.1 Responsibilities and procedures***
- *16.1.2 Reporting information security events*
- *16.1.3 Reporting information security weaknesses*
- ***16.1.4 Assessment of and decision on information security events***
- ***16.1.5 Response to information security incidents***
- ***16.1.6 Learning from information security incidents***
- *16.1.7 Collection of evidence*

- ***17 Information security aspects of business continuity management***

o ***17.1 Information security continuity***

- *17.1.1 Planning information security continuity*
- ***17.1.2 Implementing information security continuity***
- *17.1.3 Verify, review and evaluate information security continuity*

o ***17.2 Redundancies***

- ***17.2.1 Availability of information processing facilities***

- ***18 Compliance***

o ***18.1 Compliance with legal and contractual requirements***

- *18.1.1 Identification of applicable legislation and contractual requirements*
- *18.1.2 Intellectual property rights*
- *18.1.3 Protection of records*
- *18.1.4 Privacy and protection of personally identifiable information*
- *18.1.5 Regulation of cryptographic controls*
- ***TEL.18.1.6 Non-disclosure of communications***
- ***TEL.18.1.7 Essential communications***
- ***TEL.18.1.8 Legality of emergency actions***

- *18.2 Information security reviews*
  - *18.2.1 Independent review of information security*
  - *18.2.2 Compliance with security policies and standards*
  - *18.2.3 Technical compliance review*

ITU-T X.1033 (04/2016) Guidelines on security of individual information services provided by operators

Name	
ITU-T X.1033 (04/2016) Guidelines on security of individual information services provided by operators	
Developing body	**Date of publication**
ITU-T Study Group 17 Security	*04/2016*
Type	**Applies to**
Requirements/guidelines/controls	*Services: Telecommunications*
Scope	
"This Recommendation provides guidelines on the security of individual information services provided by telecommunication operators. It describes the classification of the individual information services provided by telecommunication operators as well as security objectives, requirements, mechanisms and coordination of individual information services." – Scope of [42]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.itu.int/itu-t/recommendations/rec.aspx?id=12849	*Free*
Specific relevance for CORAL	

This standard provides requirements for providers of telecommunications services, split into three identified types of service: traditional telecommunication services, content services, and informationization services.
 	
The content of this recommendation is very high-level. There is a categorization of requirements first depending on which type of service is provided and second depending on whether the requirement is regulatory, operational, or user-based. Then, the requirements are directly described. These are very succinctly presented in the document, thus they are reproduced in full below. Some requirements do not appear to apply to the service provider, e.g. some are clearly under the responsibility of a regulator. Therefore, in bold are those requirement categories that the authors of this document believe do pertain to the provider.
 	
- ***8.1 Security requirements of traditional telecommunication services***
  - ***8.1.1 Security requirements given by regulators***
  - *Recommend and/or supervise the enforcement of regulations based on the hierarchical importance of the traditional telecommunication services. Recommend and/or supervise the enforcement of security ratings and risk*	

assessment to services and underlying infrastructures.

- ***The following capabilities should be provided: network security monitoring, network security incident announcement and emergency security coordination.***
- *Establish the rules to promote fair business competition between operators.*
- *Set the rules to prevent users from utilizing the traditional telecommunication services for illegal purposes.*

- ***8.1.2 Security requirements for operators***
  - ***Maintain the infrastructures operating securely and steadily.***
  - ***Provide adequate authentication to prevent illegal users from accessing the services.***
  - ***Provide measures to prevent users from utilizing the services illegally.***
  - ***Ensure service availability and protect the services from malicious attacks.***
  - ***Ensure the capability of emergency recovery from disasters, attacks and other unexpected service breakdowns.***
  - ***Provide protection against unintended information leakage or intentional attacks.***
- ***8.1.3 Security requirements given by users***
  - ***Have access to pre-authorized services without obstacles.***
  - ***User privacy information is protected from unintended leakage or intentional attacks.***

- ***8.2 Security requirements of content services***
  - *8.2.1 Security requirements given by regulators*
    - *Establish the rules to maintain fair business competition for operators and third-party service providers.*
    - *Set the rules for service providers (operators and third-party service providers) to avoid publishing harmful content or services.*
    - *Require providers (operators and third-party service providers) to provide the capability to control, when necessary, the spread of harmful content and/or other harmful behaviour utilizing the content services.*
  - ***8.2.2 Security requirements for operators***
    - ***Maintain service availability, especially real-time service operational consistency.***
    - ***Ensure that service users are authorized.***
    - ***Ensure that users' operations are pre-authorized.***
    - ***Ensure that the outsourced third-party content services provided via the operator's systems and networks are authorized, controllable and clean from fake/illegal contents.***
    - ***Protect the services from malicious attacks (especially phishing attacks on personal data and properties).***
    - ***Have the ability to properly handle service interruptions, provide quick recovery and keep service operational consistency.***

- ***Prevent information leakage either unintentionally or by attackers stealing the information.***

- ***8.2.3 Security requirements for third-party service providers***
  - ***Ensure that the provided content is delivered to clients correctly and ensure that the normal interactions between service providers and users are conducted according to the established norms.***
  - ***Protect information integrity and protect information from being tampered with or lost.***
  - ***Protect provided content from being illegally stolen or leaked.***
- ***8.2.4. Security requirements given by users***
  - ***Service availability and privacy are ensured.***
  - ***Stable service performance (especially for paid services) is provided.***
  - ***Personal information especially bank cards, passwords, home addresses and phone numbers are protected from unauthorized access or leakage.***
  - ***In cases of unexpected service breakdown, personal data can be recovered and restored and personal information leakage is prevented.***

- ***8.3 Security requirements of informationization services***
  - *8.3.1 Security requirements for regulators*
    - *Set the rules to protect key information confidentiality, such as business information, technical information and so on.*
    - *Establish the rules to maintain fair business competition among the different operators.*
  - ***8.3.2 Security requirements for operators***
    - ***Maintain service availability to keep normal work or business activities.***
    - ***Ensure that the service users are authorised users; and ensure that the authorized users' operations are pre-authorised.***
    - ***Protect the services especially those of the financial sector from malicious attacks.***
    - ***Have the ability to properly handle service interruption; provide quick recovery and maintain service operational consistency.***
    - ***Prevent information leakage either unintentionally or by an attacker stealing the information.***
  - ***8.3.3 Security requirements given by users***
    - ***Ensure service availability. Ensure that work or business processes run efficiently and continue to do so as expected.***
    - ***Ensure confidentiality. Maintain key information confidentiality such as geolocation, business information and technical information.***
    - ***Ensure service stability. Ensure that work or business processes are not disrupted by service breakdown in key process activities, especially for group users.***

ITU-T X.1053 (11/2017) Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations

Name	
ITU-T X.1053 (11/2017) Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations	
Developing body	**Date of publication**
ITU-T Study Group 17 Security	*11/2017*
Type	**Applies to**
Requirements/guidelines/controls	*Services: Telecommunications*
Scope	
"This Recommendation defines guidelines supporting the implementation of information security controls in small and medium-sized telecommunication organizations (SMTOs) based on [ITU-T X.1051] and [ISO/IEC 27002]. *The adoption of this Recommendation will allow SMTOs to meet baseline security requirements of confidentiality, integrity, availability, and any other relevant security property specific to these organizations." – Scope of* [43]	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.itu.int/itu-t/recommendations/rec.aspx?id=13367	*Free*
Specific relevance for CORAL	

This standard, which is structured as ITU-T X.1051 (2016) | ISO/IEC 27011:2016 (which is itself structured as ISO/IEC 27002:2013), has the particularity of targeting small and medium-sized telecommunications organizations, which are particularly relevant to the objectives of the CORAL project.
 	
In the list below, in bold are those control sets that have either SMTO-specific "guidance" or SMTO-specific "other information". For control sets that contain general telecommunications-specific "guidance" or general telecommunications-specific "other information", refer to the card on ITU-T X.1051 (2016) | ISO/IEC 27011:2016, as these are not re-flagged here. The essential difference is that some of the guidance in the general case is down-scaled in order to fit the case of a small or medium-sized organization.
 	
- ***5 Information security policies***
  - ***5.1 Management direction for information security***
  - ***5.1.1 Policies for information security***
  - *5.1.2 Review of the policies for information security*
- ***6 Organization of information security***
  - ***6.1 Internal organization***
  - *6.1.1 Information security roles and responsibilities*	

- *9.3 User responsibilities*
  - *9.3.1 Use of secret authentication information*
- *9.4 System and application access control*
  - *9.4.1 Information access restriction*
  - *9.4.2 Secure log-on procedures*
  - *9.4.3 Password management system*
  - *9.4.4 Use of privileged utility programs*
  - *9.4.5 Access control to program source code*
- *TEL.9.5 Network access control*
  - *TEL.9.5.1 Telecommunications carrier identification and authentication by users*

- ***10 Cryptography***
  - ***10.1 Cryptographic controls***
    - ***10.1.1 Policy on the use of cryptographic controls***
    - ***10.1.2 Key management***
- ***11 Physical and environmental security***
  - ***11.1 Secure areas***
    - ***11.1.1 Physical security perimeter***
    - ***11.1.2 Physical entry controls***
    - *11.1.3 Securing offices, rooms and facilities*
    - *11.1.4 Protecting against external and environmental threats*
    - ***11.1.5 Working in secure areas***
    - ***11.1.6 Delivery and loading areas***
    - *TEL.11.1.7 Securing communication centres*
    - *TEL.11.1.8 Securing telecommunications equipment room*
    - *TEL.11.1.9 Securing physically isolated operation areas*
  - ***11.2 Equipment***
    - ***11.2.1 Equipment siting and protection***
    - ***11.2.2 Supporting utilities***
    - *11.2.3 Cabling security*
    - ***11.2.4 Equipment maintenance***
    - ***11.2.5 Removal of assets***
    - *11.2.6 Security of equipment and assets off-premises*
    - *11.2.7 Secure disposal or reuse of equipment*
    - *11.2.8 Unattended user equipment*
    - *11.2.9 Clear desk and clear screen policy*
  - *TEL.11.3 Security under the control of other party*
    - *TEL.11.3.1 Equipment sited in other carriers' premises*
    - *TEL.11.3.2 Equipment sited in user premises*
    - *TEL.11.3.3 Interconnected telecommunications services*
- ***12 Operations security***
  - ***12.1 Operational procedures and responsibilities***

- ***12.1.1 Documented operating procedures***
- ***12.1.2 Change management***
- ***12.1.3 Capacity management***
- ***12.1.4 Separation of development, testing and operational environments***

o ***12.2 Protection from malware***
- ***12.2.1 Controls against malware***

o ***12.3 Backup***
- ***12.3.1 Information backup***

o ***12.4 Logging and monitoring***
- *12.4.1 Event logging*
- *12.4.2 Protection of log information*
- ***12.4.3 Administrator and operator logs***
- *12.4.4 Clock synchronization*

o ***12.5 Control of operational software***
- ***12.5.1 Installation of software on operational systems***

o ***12.6 Technical vulnerability management***
- *12.6.1 Management of technical vulnerabilities*
- ***12.6.2 Restrictions on software installation***

o *12.7 Information systems audit considerations*
- *12.7.1 Information systems audit controls*

- ***13 Communications security***

o ***13.1 Network security management***
- *13.1.1 Network controls*
- ***13.1.2 Security of network services***
- ***13.1.3 Segregation in networks***
- *TEL.13.1.4 Security management of telecommunications services delivery*
- *TEL.13.1.5 Response to spam*
- *TEL.13.1.6 Response to DoS/DDoS attacks*

o ***13.2 Information transfer***
- ***13.2.1 Information transfer policies and procedures***
- ***13.2.2 Agreements on information transfer***
- *13.2.3 Electronic messaging*
- *13.2.4 Confidentiality or non-disclosure agreements*

- ***14 System acquisition, development and maintenance***

o ***14.1 Security requirements of information systems***
- ***14.1.1 Information security requirements analysis and specification***
- *14.1.2 Securing applications services on public networks*
- ***14.1.3 Protecting application services transactions***

o *14.2 Security in development and support processes*
- *14.2.1 Secure development policy*
- *14.2.2 System change control procedures*
- *14.2.3 Technical review of applications after operating platform changes*

- ***18.2 Information security reviews***
  - ***18.2.1 Independent review of information security***
  - *18.2.2 Compliance with security policies and standards*
  - *18.2.3 Technical compliance review*

4. Processes

The ISO/IEC 27036 series "Information security for supplier relationships"

Name	
ISO/IEC 27036 series of standards on Information technology — Security techniques — Information security for supplier relationships	
Developing body	**Date of publication**
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	*Part 1: 09/2021* *Part 2: 08/2014* *Part 3: 11/2013* *Part 4: 10/2016*
Type	**Applies to**
Requirements/guidelines/controls	*Processes: supplier relationships, cloud*
Scope	
This four-part series of standards is destined to give guidance on managing information security in the context of supplier relationships, whether for products or services, and regardless of complexity. It applies to both acquirers of supplies or providers of IT supplies. *Part 1 [44] is the general model.* *Part 2 [45] formulates requirements for acquirers and suppliers.* *Part 3 [46] specifies additional guidelines in the particular case of IT supplies.* *Part 4 [47] specifies additional guidance in the particular case of Cloud service provisioning.*	
Relation to CSA	
No direct relation.	
Weblinks	**Accessibility**
https://www.iso.org/standard/82905.html (Part 1) *https://www.iso.org/standard/59680.html (Part 2)* *https://www.iso.org/standard/59688.html (Part 3)* *https://www.iso.org/standard/59689.html (Part 4)*	*Not free*
Specific relevance for CORAL	
Part 1 is the general model. Parts 2, 3, and 4 give requirements to manage information security through the underlying processes both on the acquirer and supplier side of a supplier relationship, in the general case, the case of provisioning an IT supply, and the case of provisioning a Cloud service, respectively. They are all fundamentally structured very similarly in terms of process requirements (and this structure is in accordance with that of ISO/IEC 15288 ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes [48]). Thus, the requirements come in the form of activities to be performed per process. ***In all three parts, requirements are formulated for the acquirer, or supplier, or both. In order to not introduce too much redundancy in this card, below are placed in bold those requirements that concern the supplier in Part 3, covering the case of general IT products or services. This is also done in the case a clause directly refers to the corresponding guidance in Part 2.***	

- ***6.1 Agreement Processes***
  - *6.1.1 Acquisition Process*
  - ***6.1.2 Supply Process***
- ***6.2 Organizational Project-Enabling Processes***
  - ***6.2.1 Life Cycle Model Management Process***
  - ***6.2.2 Infrastructure Management Process***
  - ***6.2.3 Project Portfolio Management Process***
  - ***6.2.4 Human Resource Management Process***
  - ***6.2.5 Quality Management Process***
- ***6.3 Project Processes***
  - ***6.3.1 Project Planning Process***
  - ***6.3.2 Project Assessment and Control Process***
  - ***6.3.3 Decision Management Process***
  - ***6.3.4 Risk Management Process***
  - ***6.3.5 Configuration Management Process***
  - *6.3.6 Information Management Process*
  - *6.3.7 Measurement Process*
- ***6.4 Technical Processes***
  - ***6.4.1 Stakeholder Requirements Definition Process***
  - ***6.4.2 Requirements Analysis Process***
  - ***6.4.3 Architectural Design Process***
  - ***6.4.4 Implementation Process***
  - ***6.4.5 Integration Process***
  - ***6.4.6 Verification Process***
  - *6.4.7 Transition Process*
  - *6.4.8 Validation Process*
  - ***6.4.9 Operation Process***
  - ***6.4.10 Maintenance Process***
  - ***6.4.11 Disposal Process***

In Part 2, there is also a clause (Clause 7) specifically dedicated to requirements to manage information security in particular processes in a single acquirer-supplier relationship instance. In bold are those that concern the supplier.

- *7.1 Supplier relationship planning process*
- ***7.2 Supplier selection process***
- ***7.3 Supplier relationship agreement process***
- ***7.4 Supplier relationship management process***
- ***7.5 Supplier relationship termination process***

ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

Name	
ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)	
Developing body	**Date of publication**
ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection	*10/2008*
Type	**Applies to**
Requirements/guidelines/controls	*Processes: security engineering*

Scope

"This International Standard specifies the Systems Security Engineering – Capability Maturity Model® (SSE-CMM®). The SSE-CMM® is a process reference model focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain. Within the ITS domain, the SSE-CMM® is focused on the processes used to achieve ITS, most specifically on the maturity of those processes. There is no intent within the SSE-CMM® to dictate a specific process to be used by an organization, let alone a specific methodology. Rather the intent is that the organization making use of the SSE-CMM® should use its existing processes, be those processes based upon any other ITS guidance document. The scope encompasses:

- *the system security engineering activities for a secure product or a trusted system addressing the complete life cycle of concept definition, requirements analysis, design, development, integration, installation, operation, maintenance and de-commissioning;*
- *requirements for product developers, secure systems developers and integrators, organizations that provide computer security services and computer security engineering; and*
- *all types and sizes of security engineering organization, from commercial to government and the academe.*

[…]" – Extract of scope of [49]

Relation to CSA

No direct relation.

Weblinks	**Accessibility**
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html *(search for "21827")* https://www.iso.org/standard/44716.html	*Free*

Specific relevance for CORAL

The standard identifies topics to take into account for sound security engineering in general.

The standard categorizes base practices into process areas. 11 of these are directly related to security engineering and another 11 are for project and organizational base practices. Those for security engineering are:

- *7.1 PA01 Administer Security Controls*

- *7.7.4 BP.07.03 - Facilitate Coordination*
- *7.7.5 BP.07.04 - Coordinate Security Decisions and Recommendations*

- *7.8 PA08 - Monitor Security Posture*
  - *7.8.2 BP.08.01 - Analyse Event Records*
  - *7.8.3 BP.08.02 - Monitor Changes*
  - *7.8.4 BP.08.03 - Identify Security Incidents*
  - *7.8.5 BP.08.04 - Monitor Security Safeguards*
  - *7.8.6 BP.08.05 - Review Security Posture*
  - *7.8.7 BP.08.06 - Manage Security Incident Response*
  - *7.8.8 BP.08.07 - Protect Security Monitoring Artifacts*
- *7.9 PA09 - Provide Security Input*
  - *7.9.2 BP.09.01 - Understand Security Input Needs*
  - *7.9.3 BP.09.02 - Determine Security Constraints and Considerations*
  - *7.9.4 BP.09.03 - Identify Security Alternatives*
  - *7.9.5 BP.09.04 - Analyse Security of Engineering Alternatives*
  - *7.9.6 BP.09.05 - Provide Security Engineering Guidance*
  - *7.9.7 BP.09.06 - Provide Operational Security Guidance*
- *7.10 PA10 – Specify Security Needs*
  - *7.10.2 BP.10.01 - Gain Understanding of Customer's Security Needs*
  - *7.10.3 BP.10.02 - Identify Applicable Laws, Policies, And Constraints*
  - *7.10.4 BP.10.03 - Identify System Security Context*
  - *7.10.5 BP.10.04 - Capture Security View of System Operation*
  - *7.10.6 BP.10.05 - Capture High-Level Security Goals*
  - *7.10.7 BP.10.06 - Define Security Related Requirements*
  - *7.10.8 BP.10.07 - Obtain Agreement On Security*
- *7.11 PA11 - Verify and Validate Security*
  - *7.11.2 BP.11.01 - Identify Verification and Validation Targets*
  - *7.11.3 BP.11.02 - Define Verification and Validation Approach*
  - *7.11.4 BP.11.03 - Perform Verification*
  - *7.11.5 BP.11.04 - Perform Validation*
  - *7.11.6 BP.11.05 - Provide Verification and Validation Results*

Those for security project and organizational base practices (from Annex B) are:

- *B.3 PA12 - Ensure Quality*
  - *B.3.2 BP.12.01 - Identify the requirements for work product quality*
  - *B.3.3 BP.12.02 - Monitor Conformance to the Defined Process*
  - *B.3.4 BP.12.03 - Measure Quality of the Work Product*
  - *B.3.5 BP.12.04 - Measure Quality of the Process*
  - *B.3.6 BP.12.05 - Analyse Quality Measurements*
  - *B.3.7 BP.12.06 - Obtain Participation*
  - *B.3.8 BP.12.07 - Initiate Quality Improvement Activities*

- *o B.3.9 BP.12.08 - Detect Need for Corrective Actions*
- *B.4 PA13 - Manage Configurations*
  - *o B.4.2 BP.13.01 - Establish Configuration Management Method*
  - *o B.4.3 BP.13.02 - Identify Configuration Units*
  - *o B.4.4 BP.13.03 - Maintain Work Product Baselines*
  - *o B.4.5 BP.13.04 - Control Changes*
  - *o B.4.6 BP.13.05 - Communicate Configuration Status*
- *B.5 PA14 - Manage Project Risks*
  - *o B.5.2 BP.14.01 - Develop Risk Management Approach*
  - *o B.5.3 BP.14.02 - Identify Risks*
  - *o B.5.4 BP.14.03 - Assess Risks*
  - *o B.5.5 BP.14.04 - Review Risk Assessment*
  - *o B.5.6 BP.14.05 - Execute Risk Mitigation*
  - *o B.5.7 BP.14.06 - Track Risk Mitigation*
- *B.6 PA15 - Monitor and Control Technical Effort*
  - *o B.6.2 BP.15.01 - Direct Technical Effort*
  - *o B.6.3 BP.15.02 - Track Project Resources*
  - *o B.6.4 BP.15.03 - Track Technical Parameters*
  - *o B.6.5 BP.15.04 - Review Project Performance*
  - *o B.6.6 BP.15.05 - Analyse Project Issues*
  - *o B.6.7 BP.15.06 - Take Corrective Action*
- *B.7 PA16 - Plan Technical Effort*
  - *o B.7.2 BP.16.01 - Identify Critical Resources*
  - *o B.7.3 BP.16.02 - Estimate Project Scope*
  - *o B.7.4 BP.16.03 - Estimate Project Costs*
  - *o B.7.5 BP.16.04 - Determine Project's Process*
  - *o B.7.6 BP.16.05 - Identify Technical Activities*
  - *o B.7.7 BP.16.06 - Define Project Interface*
  - *o B.7.8 BP.16.07 - Develop Project Schedules*
  - *o B.7.9 BP.16.08 - Establish Technical Parameters*
  - *o B.7.10 BP.16.09 - Develop Technical Management Plan*
  - *o B.7.11 BP.16.10 - Review and Approve Project Plans*
- *B.8 PA17 - Define Organization's Systems Engineering Process*
  - *o B.8.2 BP.17.01 - Establish Process Goals*
  - *o B.8.3 BP.17.02 - Collect Process Assets*
  - *o B.8.4 BP.17.03 - Develop Organization's Systems Engineering Process*
  - *o B.8.5 BP.17.04 - Define Tailoring Guidelines*
- *B.9 PA18 - Improve Organization's Systems Engineering Processes*
  - *o B.9.2 BP.18.01 - Appraise the Process*
  - *o B.9.3 BP.18.02 - Plan Process Improvements*
  - *o B.9.4 BP.18.03 - Change the Standard Process*

- *o B.9.5 BP.18.04 - Communicate Process Improvements*
- *B.10 PA19 - Manage Product Line Evolution*
  - *o B.10.2 BP.19.01 - Define Product Evolution*
  - *o B.10.3 BP.19.02 - Identify New Product Technologies*
  - *o B.10.4 BP.19.03 - Adapt Development Processes*
  - *o B.10.5 BP.19.04 - Ensure Critical Component Availability*
  - *o B.10.6 BP.19.05 - Insert Product Technology*
- *B.11 PA20 - Manage Systems Engineering Support Environment*
  - *o B.11.2 BP.20.01 - Maintain Technical Awareness*
  - *o B.11.3 BP.20.02 - Determine Support Requirements*
  - *o B.11.4 BP.20.03 - Obtain Systems Engineering Support Environment*
  - *o B.11.5 BP.20.04 - Tailor Systems Engineering Support Environment*
  - *o B.11.6 BP.20.05 - Insert New Technology*
  - *o B.11.7 BP.20.06 - Maintain Environment*
  - *o B.11.8 BP.20.07 - Monitor Systems Engineering Support Environment*
- *B.12 PA21 - Provide Ongoing Skills and Knowledge*
  - *o B.12.2 BP.21.01 - Identify Training Needs*
  - *o B.12.3 BP.21.02 - Select Mode of Knowledge or Skills Acquisition*
  - *o B.12.4 BP.21.03 - Assure Availability of Skills and Knowledge*
  - *o B.12.5 BP.21.04 - Prepare Training Materials*
  - *o B.12.6 BP.21.05 - Train Personnel*
  - *o B.12.7 BP.21.06 - Assess Training Effectiveness*
  - *o B.12.8 BP.21.07 - Maintain Training Records*
  - *o B.12.9 BP.21.08 - Maintain Training Materials*
- *B.13 PA22 - Coordinate with Suppliers*
  - *o B.13.2 BP.22.01 - Identify Systems Components or Services*
  - *o B.13.3 BP.22.02 - Identify Competent Suppliers or Vendors*
  - *o B.13.4 BP.22.03 - Choose Supplier or Vendors*
  - *o B.13.5 BP.22.04 - Provide Expectations*
  - *o B.13.6 BP.22.05 - Maintain Communications*

5. Standards projects under development

This chapter contains some tables listing standards projects under development that may be of interest to CORAL. The projects are from the following technical standardization committees: *ISO/IEC JTC 1 SC 27 Information security, cybersecurity and privacy protection*, *CEN/CLC/JTC 13 Cybersecurity and Data Protection*, and *ETSI TC CYBER (Cybersecurity)*.

Access to these projects' ongoing work and documentation is only possible by registering experts within these committees. Note that for Luxembourg-based organizations, it is possible to register technical standardization delegates free-of-charge in committees within ISO, IEC, CEN, and CENELEC, by submitting a registration form to Luxembourg's national standards body, ILNAS[8].

ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection

Project	Scope
ISO/IEC DIS 27400 Cybersecurity — IoT security and privacy — Guidelines	*This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.*
ISO/IEC CD 27402.2 Cybersecurity — IoT security and privacy — Device baseline requirements	*This document provides baseline requirements for IoT devices and their manufacturers to support information security and privacy controls.*
ISO/IEC WD 27403.6 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	*This document provides guidelines to analyze security and privacy risks and identifies controls that need to be implemented in IoT-domotics systems.*
ISO/IEC WD TR 6114.2 Information technology – Security techniques – Security assurance throughout the product life cycle	*This document describes following items for supplier, end users (consumer), intermediaries of the ICT supply chain, service provider, and regulators.* - *definition of phases in ICT product life cycle from concept to retirement,* - *threat vectors possible in each phase of the life cycle,* - *potential controls against those threat vectors.*
ISO/IEC FDIS 15408-4 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4:	*This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and*

[8] See here https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html for more details. Also note that membership in ETSI or ITU-T is not managed by ILNAS. Entities that wish to participate in those bodies' work must register within them directly.

Framework for the specification of evaluation methods and activities	*evaluation activities.* *This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities. These aspects are a matter for those originating the evaluation methods and evaluation activities in their particular area of interest.*
ISO/IEC FDIS 15408-5 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements	*This document provides packages of security assurance and security functional requirements that have been identified as useful in support of common usage by stakeholders. EXAMPLE: Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs).* *This document presents:* - *evaluation assurance level (EAL) family of packages that specify pre-defined sets of security assurance components that may be referenced in PPs and STs and which specify appropriate security assurances to be provided during an evaluation of a TOE;* - *composition assurance (CAP) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of composed TOEs;* - *composite product (COMP) package that specifies a set of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of a composite product TOEs;* - *protection profile assurance (PPA) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during a protection profile evaluation;*

	- *security target assurance (STA) family of packages specify sets of security assurance components used for specifying appropriate security assurances to be provided during a security target evaluation.* *The audience for this document includes consumers, developers, and evaluators of secure IT products.*
ISO/IEC CD 27071.2 Information technology – Security techniques – Security recommendations for establishing trusted connections between devices and services	*This International Standard provides a framework and recommendations for establishing trusted connection between device and service based on hardware security modules, including recommendations for components such as: hardware security module, roots of trust, identity, authentication and key establishment, environment attestation, data integrity and unforgeability.*

CEN/CLC/JTC 13 Cybersecurity and Data Protection

Project	Scope
prCEN/CLC/TS XXX Multi-layered approach for a set of requirements for information/cyber security controls for Cloud Services	*This Technical Specification (TS) provides a set of information security requirements for information/cyber security controls for Cloud Services This TS is applicable for organizations providing cloud services and their subservice organizations.*
prEN 17640 Fixed time cybersecurity evaluation methodology for ICT products	*This document describes the cybersecurity evaluation methodology for ICT products. It is intended for use for all three assurance levels as defined in the Cybersecurity Act (i.e. basic, substantial and high). The methodology is comprised of different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA for the three levels. Where appropriate, it can be applied both to 3rd party evaluation and self-assessment. It is expected that this methodology may be used by different candidate schemes and verticals providing a common framework to evaluate ICT*

	products.
prEN XXX Common framework for vertical information security or cybersecurity control sets	*This standard specifies a framework for further vertical information security or cybersecurity control sets. It contains a common structure, common terms and definitions, and a common set of controls including control objectives. This standard shall be applied by any TC/SC/PC within CEN/CENELEC when developing their own vertical set of information security controls contain their sector-specific control requirements. The main purpose of this standard is the harmonization of vertical control sets including the easing of comparison between different sectors. This standard will not address management system standard topics. This standard will not contain any specific control requirements itself.*
prEN XXXXX Security Evaluation Standard for IoT Platforms (SESIP). An effective methodology for applying cybersecurity assessment and re-use for connected products.	*This document describes a cybersecurity evaluation methodology, named SESIP, for components of connected ICT products. Security claims in SESIP are made based on the security services offered by those components. Components can be in hardware and software. SESIP aims to support comparability between and reuse of independent security evaluations. SESIP provides a common set of requirements for the security functionality of components which apply to the foundational components of devices that are not application specific. The methodology describes the re-use of evaluation results.*

ETSI TC CYBER (Cybersecurity)

Project	Scope
DTR/CYBER-0057 (TR 103 621) *Guide to Cyber Security for Consumer Internet of Things*	*This technical report will serve as a guidance document to help manufacturers and other stakeholders to meet the provisions defined for Consumer IoT devices in EN 303 645 and TS 103 645.* *This work is complementary to EN 303 645 and TS 103 701. The relationship between these specifications and how they can be used together will be explained. A non-exhaustive set of*

	example implementations that meet the provisions will be provided. Not all possible implementations will be included. Pointers to supporting specifications will be included where relevant. Usage by industry players as well as future development of standards will be considered (e.g. specialisation for specific use cases, certification aspects).

6. Conclusion

This document's aim is to serve as a starting point in the CORAL project to come up with a series of questions or requirements to consider for the security of low-complexity, low-risk products, services, or processes. To do so, a state-of-the-art or existing standards and frameworks was established, based on the already quite complete state-of-the art in [1], and making logical exclusions and inclusions.

The surveyed frameworks cover the following sub-topics: generic products, Internet of Things products, Web applications, and Artificial Intelligence products, generic services, Cloud Computing services, Internet of Things services, telecommunications services, and generic processes.

Each surveyed framework is described by means of a table that lists the categories of security requirements considered within that framework, and how it might be relevant to the objectives of CORAL.

7. References

[1] ECSO, WG1 – Standardisation, certification, labelling and supply chain management, "STATE OF THE ART SYLLABUS Overview of existing Cybersecurity standards and certification schemes v2, December 2017," [Online]. Available: https://ecs-org.eu/documents/publications/5a31129ea8e97.pdf. [Accessed 24 12 2021].

[2] ENISA, "CYBERSECURITY CERTIFICATION MARKET STUDY Towards a research and analysis methodology," April 2021. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study. [Accessed 06 12 2021].

[3] ENISA, "METHODOLOGY FOR SECTORAL CYBERSECURITY ASSESSMENTS EU Cybersecurity Certification Framework," 09 2021. [Online]. Available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment. [Accessed 06 12 2021].

[4] ENISA, "STANDARDISATION IN SUPPORT OF THE CYBERSECURITY CERTIFICATION Recommendations for European standardisation in relation to the Cybersecurity Act," 12 2019. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i. [Accessed 06 12 2021].

[5] ENISA, "ADVANCING SOFTWARE SECURITY IN THE EU The role of the EU cybersecurity certification framework," 11 2019. [Online]. Available: https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework. [Accessed 06 12 2021].

[6] ENISA, "CYBERSECURITY CERTIFICATION EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS v1.1.1," 05 2021. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1. [Accessed 06 12 2021].

[7] ENISA, "PUBLIC CONSULTATION ON THE DRAFT CANDIDATE EUCC SCHEME Report on Public Consultation," 05 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme. [Accessed 06 12 2021].

[8] ENISA, "EUCS – CLOUD SERVICES SCHEME EUCS, a candidate cybersecurity certification scheme for cloud services," 12 2020. [Online]. Available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme. [Accessed 06 12 2021].

[9] *ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT*

security — Part 1: Introduction and general model.

[10] *ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.*

[11] *ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.*

[12] *ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security evaluation.*

[13] *ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications.*

[14] *ETSI EN 303 645 V2.1.1 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.*

[15] *ETSI TS 103 645 V2.1.2 (2020-06) CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.*

[16] *ETSI TS 103 701 V1.1.1 (2021-08) CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements.*

[17] ICSA, "ICSA Labs Internet of Things (IoT) Security testing framework," 14 07 2021. [Online]. Available: https://www.icsalabs.com/sites/default/files/ICSALABS_IoT_reqts_framework_v2.01_210714.pdf. [Accessed 23 12 2021].

[18] BITAG, "Internet of Things (IoT) Security and Privacy Recommendations," [Online]. Available: https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php. [Accessed 23 12 2021].

[19] GSMA, "IoT Security Guidelines for Endpoint Ecosystems," 29 02 2020. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf. [Accessed 23 12 2021].

[20] IoTSF, "IoT Security Assurance Framework, Release 3.0, November 2021," 11 2021. [Online]. Available: https://www.iotsecurityfoundation.org/best-practice-guidelines/. [Accessed 05 01 2022].

[21] Internet Society, "Internet of Things (IoT) Trust Framework v2.5," 05 2018. [Online]. Available: https://www.internetsociety.org/resources/doc/2018/iot-trust-framework-v2-5/. [Accessed 05 01 2022].

[22] U.S. Department of Homelnad Security, *Strategic principles for securing the Internet of Things (ioT),*

v1.0 November 15, 2016, 2016.

[23] OWASP, "OWASP Web Security Testing Guide," [Online]. Available: https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf. [Accessed 23 12 2021].

[24] AI HLEG, "AI HLEG - Assessment List for Trustworthy Artificial Intelligence (ALTAI)," 23 07 2020. [Online]. Available: https://futurium.ec.europa.eu/en/european-ai-alliance/document/ai-hleg-assessment-list-trustworthy-artificial-intelligence-altai?language=fr. [Accessed 03 01 2022].

[25] ENISA, "Securing Machine Learning Algorithms," 12 2021. [Online]. Available: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms. [Accessed 03 01 2022].

[26] *ETSI GR SAI 002 V1.1.1 Securing Artificial Intelligence (SAI); Data Supply Chain Security.*

[27] *ETSI GR SAI 004 V1.1.1 (2020-12) Securing Artificial Intelligence (SAI); Problem Statement.*

[28] *ETSI GR SAI 005 V1.1.1 Securing Artificial Intelligence (SAI); Mitigation Strategy Report.*

[29] *ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements.*

[30] *ISO/IEC Directives, Part 1 Consolidated ISO Supplement — Procedures for the technical work — Procedures specific to ISO, Twelfth edition, 2021.*

[31] *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.*

[32] *ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.*

[33] *ISO/IEC TR 20000-7:2019 Information technology — Service management — Part 7: Guidance on the integration and correlation of ISO/IEC 20000-1:2018 to ISO 9001:2015 and ISO/IEC 27001:2013.*

[34] *EuroCloud, StarAudit catalogue, Part D, V4.0, 15/12/2020.*

[35] *ITU-T X.1631 (07/2015) | ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[36] *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.*

[37] ANSSI, "Prestataires de services d'informatique en nuage (SecNumCloud)," 11 06 2018. [Online]. Available: https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.1_anssi.pdf. [Accessed 23 12 2021].

[38] *BSI, Cloud Computing Compliance Criteria Catalogue - C5:2020.*

[39] Cloud Security Alliance, "Cloud Controls Matrix and CAIQ v4," [Online]. Available: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/. [Accessed 23 12 2021].

[40] GSMA, "IoT Security Guidelines for IoT Service Ecosystems," 29 02 2020. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.12-v2.2-GSMA-IoT-Security-Guidelines-for-Service-Ecosystems.pdf. [Accessed 23 12 2021].

[41] *ITU-T X.1051 (2016) | ISO/IEC 27011:2016 Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.*

[42] *ITU-T X.1033 (04/2016) Guidelines on security of individual information services provided by operators.*

[43] *ITU-T X.1053 (11/2017) Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations.*

[44] *ISO/IEC 27036-1:2021 Cybersecurity — Supplier relationships — Part 1: Overview and concepts.*

[45] *ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements.*

[46] *ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security.*

[47] *ISO/IEC 27036-4:2016 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services.*

[48] *ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes.*

[49] *ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®).*