
ENISA CYBERSECURITY CERTIFICATION OF CLOUD SERVICES
Cybersecurity certification is a global trade and trust instrument
January 11 2021 | 14.00–16.30 CET
Webinar
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ABOUT EUCS:
A DRAFT CERTIFICATION SCHEME FOR CLOUD SERVICES

Eric Vetillard, Ph.D.
Lead Certification Expert, ENISA

11 | 01 | 2021

ABOUT THIS WEBINAR

The Webinar is organized in two parts

An overview of the scheme

Answers to questions from the public

Please use the “Q&A” to ask your questions

We will only get questions from there to answer during the webinar

We will strive to answer all questions, during or after the webinar

AGENDA

Where we stand

- Currently a draft, to become a candidate scheme

The draft candidate scheme

- Overview and assurance levels
- Assessment methodology
- Requirements on controls

Challenges ahead

- Main challenges
- Being useful

CHAPTER 1

WHERE WE STAND

Over one year after the request, 10 months after the beginning of the work in the ad hoc working group, an advanced draft is available, as initially planned.

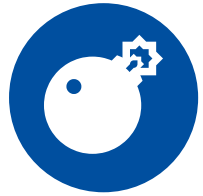
A lot of work has been done, and a lot of work remains.

CONTEXT OF THE WORK

Ambitious objectives

From the Commission's request and from early discussions

- Covering all kinds of cloud services
- Covering all assurance levels defined in the Cybersecurity Act
- Enabling the free flow of information in Europe
- Following preparatory work from CSP-CERT



Expected difficulties

Some topics were already identified as difficult or treacherous

- Two major assessment methods available
- Many partial sources for requirements, but no obvious authority
- Scope to be clarified around key topics such as privacy and location information

WHERE DO WE STAND TODAY?

A draft candidate scheme is available for review.

It contains (almost) all answers to the questions in Article 54(1)

- Missing a few things, like the format of a certificate

It contains the definition of assessment methodologies for all levels

- The methodologies are fully defined at a high level
- The “details”, such as document templates and accreditation rules, still need some work

It contains the definition of requirements for security controls

- There is a full draft of these requirements
- They still need to be polished and “played with”

It even contains recommendations about supply chain and about adoption/transition

WHAT'S NEXT?

Finalize the body

The basis for the forthcoming implementing act

- All answers to Article 54(1) questions
- All required complements, for instance related to supply chain
- Most urgent, as precondition for work on implementing act

Finalize the annexes

Mostly requirements on controls and on assessment

- General consolidation
- Development of missing parts
- Some work could continue in parallel with the development of the implementing act

Produce guidance

Necessary complement to the scheme

- Contains all elements that are too detailed or too volatile
- References for providers, CABs, accreditation bodies, NCCAs
- Not mandatory, but a reference to be judged against

CHAPTER 2

THE DRAFT CANDIDATE SCHEME

The draft candidate scheme defines rules for the management of certificates and of the scheme, as well as a number of technical documents that define requirements for security controls, for assessment processes, among other things.

FOREWORD

The scheme, including its annexes, is a formal document, in which the intention is not always easy to identify. The goal of this presentation is to give a few keys.

Some information need to be connected

- Scheme components are often refined in annexes
- Some components and annexes refer to guidance which remains TBD
- Connections between chapters are not always obvious (e.g., composition section & assessment methodology)

Some information is very formal

- The requirements on controls have been sliced into levels and described using a language as formal as possible, and they don’t read like a novel…
- The assessment methods are defined quite formally, combining vocabulary from several sources, and linking to the various terminologies is essential

SCHEME PRINCIPLES

The principles have been mostly stable, but some discussions have lingered

The main decisions were taken before the summer of 2020

- Cloud services are defined like in ISO/IEC 17788 (wide definition)
- Three assurance levels are to be defined
- Assessment methods to be combinable with both ISO and ISAE audits
- Requirements on controls to be inspired from standards (ISO/IEC 270xx) and national schemes (C5, SecNumCloud)

Key discussions continued until the end of 2020

- About the structure of the requirements on security controls
- About the organization and details of the assessment methodologies
- About the precise definition of the levels

SUBJECT MATTER
DEFINING CLOUD SERVICES

There are many different definitions of the cloud, in schemes, in reports, in regulations.

For the scheme, we refer to standard ISO/IEC 17788, which defines terminology for the cloud

- **cloud computing**: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
  - NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
- **cloud service**: One or more capabilities offered via **cloud computing** invoked using a defined interface.

➔Explicit reference to scalability and elasticity

➔But not at the level of the services themselves

➔A cloud service is not just an ISMS

➔A cloud service includes a full stack

VOCABULARY
TWO MAIN SOURCES

ISO/IEC 17000 and friends

The scheme is based on ISO/IEC 17065, so this is the main source of vocabulary for the scheme.

- Organisation of the conformity assessment
- Roles and tasks

Also other standards, such as ISO 9000, ISO/IEC 27005, ISO/IEC 29147, …

IAASB Handbook

Some definitions are taken from this source, which provides good definitions of complex concepts.

- Limited and reasonable assurance
- Design and operating effectiveness

And of course the Cybersecurity Act and related European regulations

VOCABULARY
TWO MAIN SOURCES

ISO/IEC 17000 and friends

The scheme is based on ISO/IEC 17065, so this is the main source of vocabulary for the scheme.

- Organisation of the
- Roles and tasks

Also other standard
ISO/IEC 27005, IS

IAASB Handbook

Some definitions are taken from this source, which provides good definitions of

le assurance

effectiveness

If it does not make sense, check the glossaries before assuming that there is something wrong…

And of course the Cybersecurity Act and related European regulations

INTERLUDE

WHAT IS ASSURANCE?

In the past few year, we have struggled with definitions, like ‘audit’, ‘effectiveness’ (operative or not), ‘evaluation’, and a few more.

Today, back to basics…

WHAT IS ASSURANCE?

Assurance is a very loaded word, used in many different contexts, so having a shared understanding is really necessary.

Webster's, 1913 (from Wikipedia)

- The **act** of assuring; a **declaration** tending to inspire full confidence; that which is designed to give **confidence**.

SOC2, one century later

- An objective examination of evidence for the purpose of providing the reader or user of the report with a **level** of comfort that security **goals** have been adequately **met** through the organization's risk management and governance processes

Common Criteria, circa 2000

- *assurance level:* **grounds** for **confidence** that a TOE **meets** the **SFRs**

A set of **actions** to bring some **level** of **confidence** that some **requirements** are **met**

GENERATING ASSURANCE

So, assurance is what we do with a scheme…

Definitions in ISAE 3000

- *Assurance engagement:* An engagement in which a practitioner aims to **obtain sufficient appropriate evidence** in order to express a conclusion designed to **enhance the degree of confidence** of the intended users other than the responsible party about the subject matter information…
- *Reasonable assurance engagement:* An assurance engagement in which the practitioner **reduces engagement risk** to an acceptably **low level in the circumstances** of the engagement as the basis for the practitioner's conclusion…

Definition in SOC2

- *Reasonable assurance:* A **high**, but not absolute, **level** of assurance

ASSURANCE CONTROLS AND REQUIREMENTS

Every framework defines how assurance is generated.

In NIST SP 800-53r5 (draft)

- “Assurance is the measure of confidence that the system functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system—thus possessing the capability to accurately mediate and enforce established security and privacy policies.”
- Assurance-related controls “narrow the analysis for instance by increasing the discipline applied to the system architecture, software design, specifications, code style, and configuration management”

In ISO/IEC 15408-3 (Common Criteria)

- CC defines Security Assurance Requirements (SARs) that look a lot like assurance-related controls
- These SARs are combined in sets that define Evaluation Assurance Levels (EALs)

SO, WHAT IS AN ASSURANCE LEVEL?

This is a central question in the definition of a scheme.

Definition from EC 881/2019 (EU Cybersecurity Act):

- *assurance level:* a **basis for confidence** that an [ICT service] **meets** the security **requirements** of a specific European cybersecurity certification scheme, indicates the **level** at which an [ICT service] has been **evaluated** but as such **does not measure the security** of the [ICT service] concerned

What we need to be careful about in our cloud scheme:

- Assurance is about building confidence that a cloud service meets our scheme's requirements
- An assurance level reflects the level of scrutiny to which the cloud service is submitted
- Higher assurance levels will include more assurance-related controls
- Higher assurance levels will have increased assessment requirements to match the circumstances of the audit
- Higher assurance levels may have higher functional requirements if they help to build confidence

DEFINITION OF ASSURANCE LEVELS

The high-level definition of the assurance levels focuses on a number of important factors to be considered in the analysis.

The Assurance Levels are currently differentiated by:

a) **Intention**. High-level description, mostly based on requirement from the EU Cybersecurity Act

b) **Suitability**. Potential restrictions of the types and categories to be covered at a given level

c) **Assumed Attacker profile**. Basic characteristics of expected attackers addressed by the assurance level

d) **Scope**. Elements of the service and requirements to be included in the evaluation

e) **Depth**. Level of design and implementation details to be provided for a given assurance level

f) **Rigour**. Level of structure of the methods used to design, implement and assess the service

INTENTION

‘basic’ level

Minimise the **known basic** risks of incidents and cyberattacks

- Limited assurance
- Self-assessment reviewed by a third-party
- Focus on the definition and existence of procedures and mechanisms

‘substantial’ level

Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources**

- Reasonable assurance
- Design and operating effectiveness
- Functional testing

‘high’ level

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources**

- Reasonable assurance
- Design and operating effectiveness
- Automated controls
- Penetration testing

SUITABILITY

‘basic’ level

Designed for services

- For **non-critical** data and systems
- Low risk profile

‘substantial’ level

Designed for services

- For **business-critical** data and systems
- Mainstream risk profile for sensitive cloud operations

‘high’ level

Designed for services

- For **mission-critical** data and systems
- Elevated risk profile for critical data and systems that are typically not cloud-based

THE BASIC LEVEL

Designed as an entry point to certification, a first step that demonstrates an early commitment to security.

The general scope is the same as for other levels, with requirements in all 20 categories

- Some themes may be skipped (open question), requirements are very light
- Limited obligations to comply to standards and use strict methods, but guidance to do so

Self-assessment performed by the CSP, reviewed by an accredited CAB

- The CSP needs to gather supporting documentation as proposed evidence
- Limited assurance, focus on the existence of policies and procedures, no study of effectiveness
- At least two physical meetings, maybe one on CSP premises (open question)

Limited maintenance obligations

- Mostly focused on service/controls changes, vulnerabilities and incidents

THE SUBSTANTIAL LEVEL

Designed as mainstream certification, demonstrating an effective commitment to security.

The general scope is very similar to the basic criteria of C5

- Including all requirements defined for the basic level
- Complemented with additional requirements from C5, SecNumCloud, ISO27001 and other sources

Reasonable assurance assessment performed by an accredited CAB

- The CAB gathers evidence through documentation requests/reviews, interviews, site visits
- Focus on design effectiveness (theory) and on operating effectiveness (practice)

Yearly maintenance obligations

- Operating effectiveness to be demonstrated since last assessment (covering incidents and vulnerabilities)
- Design effectiveness to be demonstrated on service/controls changes and every three years

EU STATEMENTS OF CONFORMITY

EU statements of conformity are *not* supported in the draft scheme

Cloud Service Providers perform a self-assessment at level Basic

- But they cannot make a self-declaration about conformity to the scheme
- The only way to claim conformity is to undergo a certification
- This means that the self-assessment must be audited by a third-party

This decision may not be final

- The main reason behind it is that the scheme is not mature enough to support EU statements of conformity
- The first assessments will require professional auditors to properly apply the guidance
- EU statements of conformity are more demanding in terms of surveillance
- This decision will be reconsidered when the scheme is reviewed

THE HIGH LEVEL

Designed as a demanding certification, demonstrating an effective commitment to security with state-of-the-art controls.

Substantial requirements on controls are augmented in several ways

- More precise/demanding requirements from SecNumCloud, C5's additional criteria, and from CSP-CERT
- Dedicated requirements on penetration testing and on automated monitoring of controls

Same assessment methodology as for the Substantial level for now

- Automated monitoring requirements included as first step towards continuous assessment
- Some requirements on penetration testing or development have a significant impact

Same maintenance obligations as for Substantial

- Possible additional yearly requirements on design effectiveness
- Specific controls have yearly requirements (such as the maintenance of a penetration testing plan)

KEY QUESTIONS ON ASSURANCE LEVELS

There are many question on the absolute and relative positioning of levels

About the Basic assurance level

- Is the Basic assurance level accessible enough? — We hope so, ongoing work to confirm
- Is the Basic assurance level meaningful? — Yes, with wide basis and CAB review

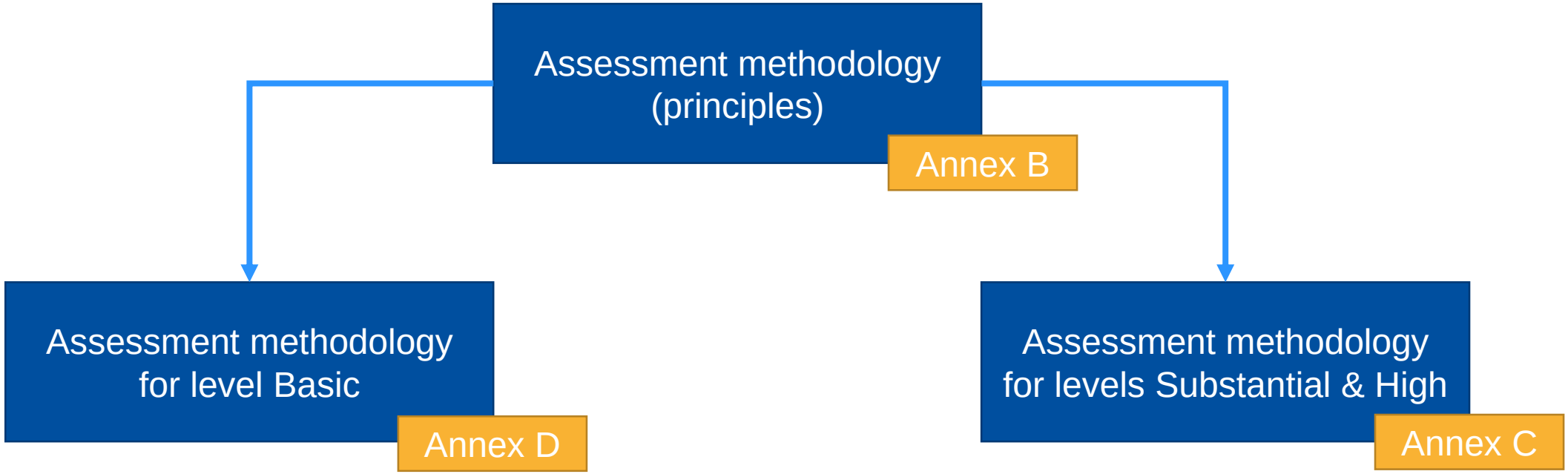
About the Substantial assurance level

- Is the Substantial level different from the Basic level? — Yes, full audit, far more constrained
- Is the Substantial assurance level a proper mainstream? — Yes, similar to C5/SecNumCloud

About the High assurance level

- Is the High level differentiated from the Substantial level? — Yes, with strong additional requirements
- Is the High level reachable in practice? — We hope so, need some work to confirm

ASSESSMENT METHODOLOGIES



ASSESSMENT PRINCIPLES

Submitting an application and reviewing the application

Preparing an audit plan

Performing the audit activities

Reviewing the subservices' assurance documentation

Reviewing the assessment activities and taking a certification decision

The assessment follows the principles defined in ISO/IEC 17065

Starting with an application

- Providing information and then reviewing it

Then performing an audit

- Start by an audit plan, followed by its execution

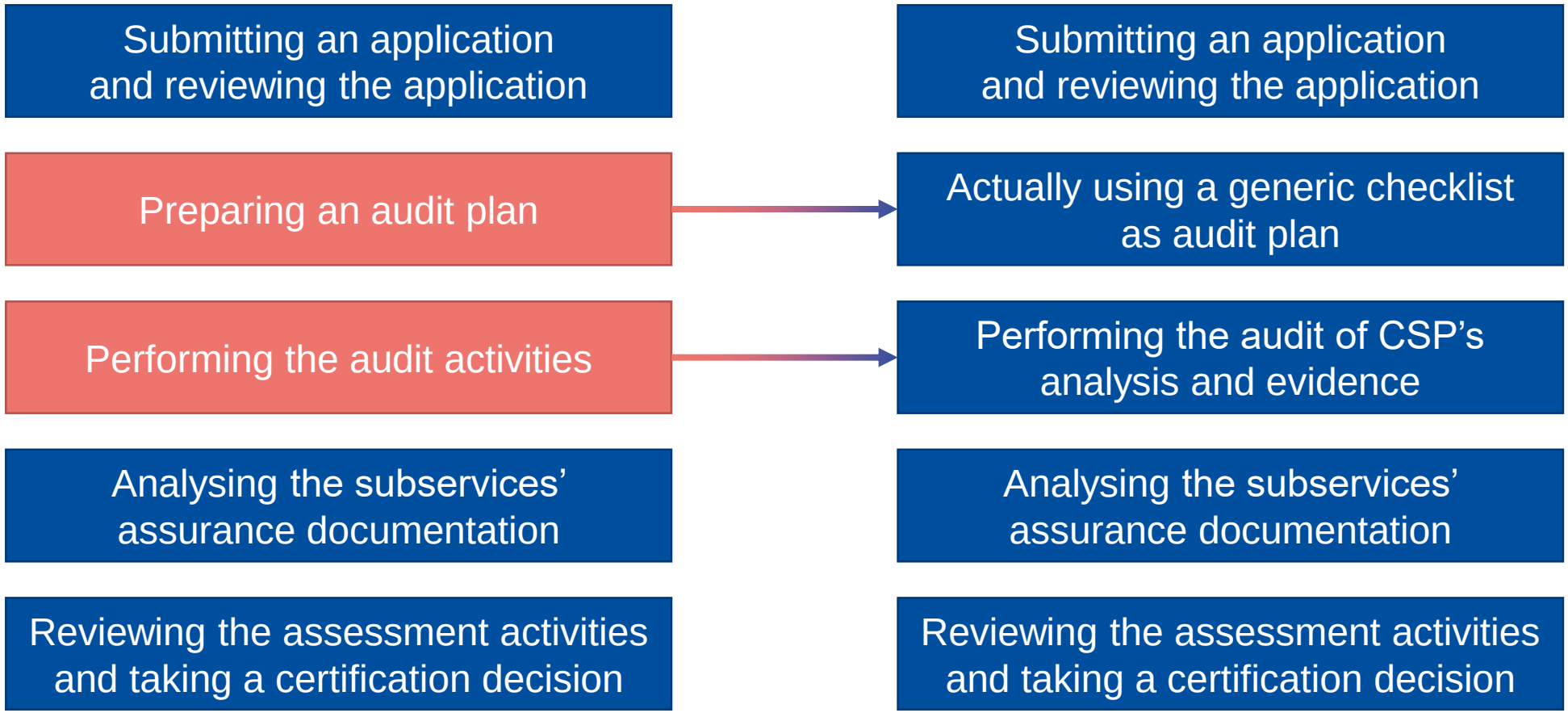
Adding a specific step to manage the supply chain

- Reviewing available assurance on subservices

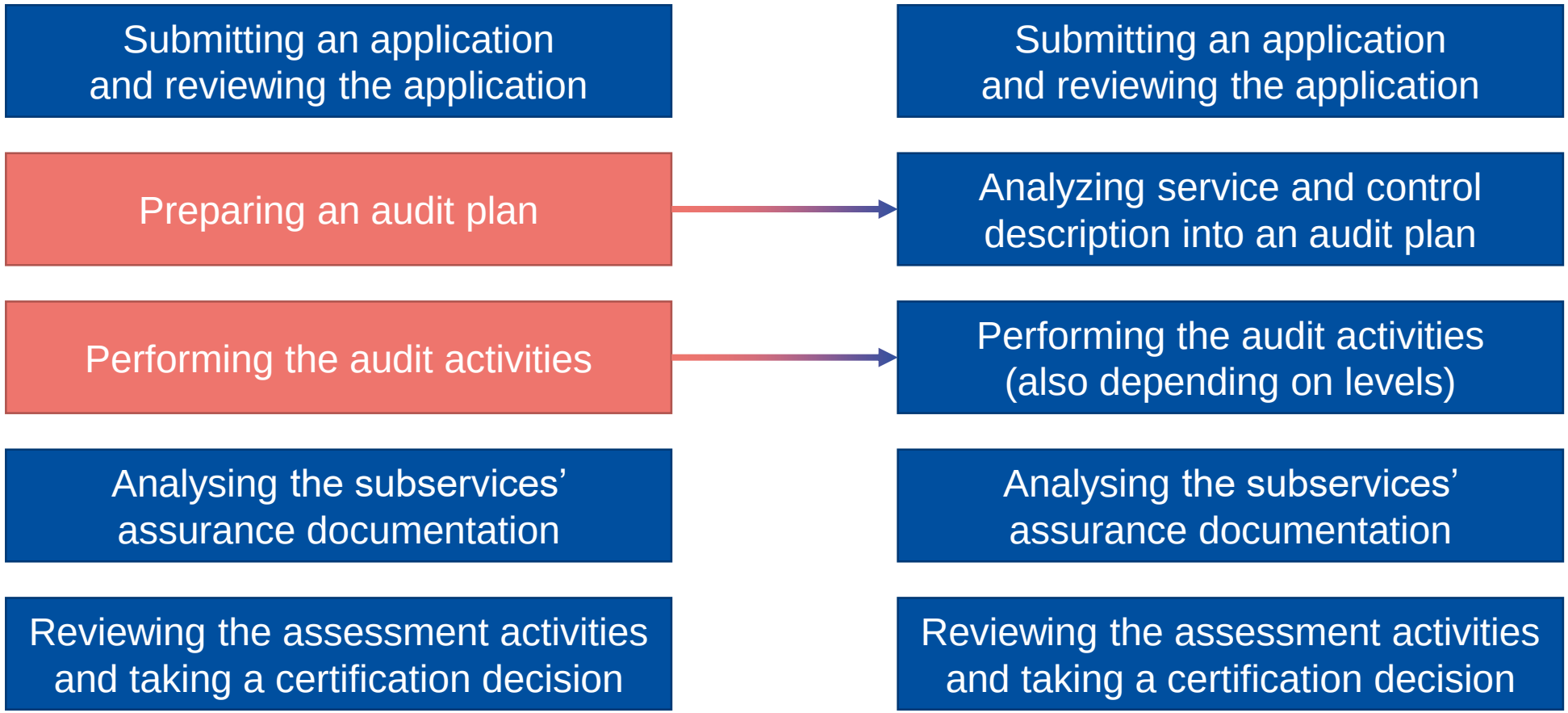
Finally, performing a review

- By an independent team in the CAB, to validate the audit work and take the certification decision

ASSESSMENT FOR LEVEL BASIC



ASSESSMENT FOR LEVELS SUBSTANTIAL AND HIGH



CLOUD SUPPLY CHAIN: SUBSERVICE ANALYSIS AND COMPOSITION

Subservice analysis is mandatory for all cloud services that rely on subservices, and composition is here a simplifying hypothesis

Many cloud services use subservices in the provision of their own service

- EUCS covers the full stack, so the subservices are always in scope of the certification
- The interface must be well-defined and properly implemented by the cloud service
- Sufficient documentation (dependent on assurance level) must be available for the cloud service

Composition is possible for subservices that have been certified in EUCS

- These subservices need to fulfill additional requirements, in which they detail how they help their customers in meeting the scheme requirements, including the definition of guidance as actionable requirements
- The customers then need to satisfy these actionable requirements
- The documentation of the certified subservice is automatically validated through composition

PRINCIPLES FOR REQUIREMENTS ON CONTROLS

Requirements need to be read with a clear understanding of the intention.

Annex A

High level of abstraction

- The requirements will be annexed to the implementing act, becoming law (hard to maintain)
- They will be complemented by guidance, which must be understood as the reference implementation
  - If you follow the guidance, no explanation required; otherwise, you need to explain why you are at least equivalent
  - This “strong” guidance is currently being defined for EUCC, and EUCS will follow the same rules

Regular organization

- Requirements organized in themes, grouped in chapters, loosely related to ISO/IEC 27001
- Cross-references are important (*e.g.*, document, communicate and implement policies and procedures according to ISP-02)

Split in assurance levels

- Requirements labeled Basic are applicable to all certified cloud services
- Requirements labeled Substantial are applicable to cloud services certified at the Substantial and High levels
- Requirements labeled High are applicable to cloud services certified at the High level

THE ROLE OF C5

The German C5 scheme has been used as a starting point for its consistency and completeness, but there are a few significant differences.

On the form

- The criteria are further split into requirements and assigned to assurance levels
- The use of vocabulary is even more consistent and strict
- As a result, guidance should include a more accessible version of the requirements

On the content and organization

- The content is organized differently into categories
- Some categories are significantly different, such as the IAM category
- Many criteria have been modified, with additional content from SecNumCloud and other sources
- Some requirements, for instance on location, are replaced by transparency requirements

ONE EXAMPLE FROM C5

IDM-05 Regular review of access rights

Basic Criterion
Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorisation processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorised persons from the Cloud Service Provider's organisational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights.

Additional Criterion
Privileged access rights are reviewed at least every six months.

Regular review of access rights

Split into a Basic Criterion and an Additional Criterion

- The Basic Criterion contains several components with a basic statement and additional details.
- Checking compliance to this criterion is likely to require several actions to verify all components
- The Additional Criterion defines an optional criterion that some CSPs may elect to meet

FROM C5 AND SECNUMCLOUD TO EUCS

IDM-05 Regular review of access rights

Basic Criterion
Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorisation processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorised persons from the Cloud Service Provider's organisational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7 days after their detection, by appropriate modification or withdrawal of the access rights.

Additional Criterion
Privileged access rights are reviewed at least every six months.

Ref	Description	Ass. Level
IAM-05.1	The CSP shall review the access rights of all the user accounts under its responsibility at least once a year to ensure that they still correspond to the current needs	Basic
IAM-05.2	The review defined in IAM-05.1 shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies.	Substantial
IAM-05.3	The CSP handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights.	Substantial
IAM-05.4	The CSP shall provide CSCs with a tool that facilitates the review of the access rights of user accounts under their responsibility	Substantial
IAM-05.5	The CSP shall perform the review defined in IAM-05.1 at least every six (6) months	High

IAM-05 REGULAR REVIEW OF ACCESS RIGHTS

Objective

- The fitness for purpose of the user accounts of all types and their associated access rights are reviewed regularly.

Requirements

Ref	Description	Ass. Level	
IAM-05.1	The CSP shall review the access rights of all the user accounts under its responsibility at least once a year to ensure that they still correspond to the current needs	Basic	From C5 Basic
IAM-05.2	The review defined in IAM-05.1 shall be performed by authorised persons under the responsibility of the authorised body that has approved the access rights policies.	Substantial	
IAM-05.3	The CSP handles identified deviations timely, but no later than 7 days after their detection, by appropriately revoking or updating access rights.	Substantial	
IAM-05.4	The CSP shall provide CSCs with a tool that facilitates the review of the access rights of user accounts under their responsibility	Substantial	From SecNumCloud
IAM-05.5	The CSP shall perform the review defined in IAM-05.1 at least every six (6) months	High	From C5 Additional

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

- Must be publicly available, as required by the Cybersecurity Act, Article 55(a)
- Plus information on risk sharing (Substantial) and analysis of customer behavior (High)

It is the accumulation of details like that make the level High more demanding.

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

DOC-02 Online Register of Known Vulnerabilities

- As required by the Cybersecurity Act, Article 55(d)
- Including further details on required information, as needed by customers for a risk analysis

Article 55 also requires the disclosure of a period for security support and contact information for receiving vulnerabilities, which are handled elsewhere.

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

DOC-02 Online Register of Known Vulnerabilities

DOC-03 Locations of Data Processing and Storage

- Transparency required on location of processing and storage of data
- Also information on the jurisdiction
- Specific information on admin and supervision and on meta-data and derived data (Substantial)
- Additional information about support operations (High)

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

DOC-02 Online Register of Known Vulnerabilities

DOC-03 Locations of Data Processing and Storage

DOC-04 Justification of the Targeted Assurance Level

- Making sure that the assurance level is commensurate with the risk associated to the cloud service
- Based on a formal risk analysis (Substantial)

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

DOC-02 Online Register of Known Vulnerabilities

DOC-03 Locations of Data Processing and Storage

DOC-04 Justification of the Targeted Assurance Level

DOC-05 Guidelines and Recommendations for Composition (optional)

- Specific guidelines for customers who want to certify their own services
- Based on actionable (and auditable) requirements
- Associated to a targeted level (Substantial)

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

DOC-02 Online Register of Known Vulnerabilities

DOC-03 Locations of Data Processing and Storage

DOC-04 Justification of the Targeted Assurance Level

DOC-05 Guidelines and Recommendations for Composition (optional)

DOC-06 Contribution to the Fulfilment of Requirements for Composition (optional)

- How the service contributes to the security of its customers' own services

DOCUMENTATION REQUIREMENTS

A lot of information must be made available to customers.

DOC-01 Guidelines and Recommendations for Cloud Customers

DOC-02 Online Register of Known Vulnerabilities

DOC-03 Locations of Data Processing and Storage

DOC-04 Justification of the Targeted Assurance Level

DOC-05 Guidelines and Recommendations for Composition (optional)

DOC-06 Contribution to the Fulfilment of Requirements for Composition (optional)

The value of these documentation requirements also comes from the fact that the documents listed here are in the scope of the audit

CHAPTER 3

THE CHALLENGES AHEAD

The release of a draft candidate scheme is not the end of he work, rather a new beginning. There are many more tasks ahead of us, and finalizing the candidate scheme is only one of them.

ACCREDITATION AND AUTHORIZATION

Accreditation

Organizational and technical requirements to be assessed by a NAB

- New scheme, new criteria. No direct reuse from ISO and ISAE
- Adaptation to guarantee the possibility of combined assessments
- Discussions under way with NABs

Authorization

Technical requirements to be validated through an authorization from the NCCA

- A possibility opened by the Cybersecurity Act, coming in addition to accreditation
- Currently envisaged for skills on penetration testing and code analysis for level High
- Could be extended to other skills and levels

APPLICABILITY

SMEs

Can SMEs get a Basic certificate? What about Substantial?

- Hopefully yes, provided that they are implementing security measures
- Looking at what needs to be in place, and roughly what the costs may be
- In particular, looking at how a certified Infrastructure can help certify an Application

The High level

Is the High level right (sufficient and achievable)? By whom?

- Need specific scrutiny on the controls specific to the High assurance level
- In particular, a strong hard look is required to our path to continuous assessment
- Also, details are required on penetration testing mechanisms

THE CLOUD SUPPLY CHAIN

Building clouds on clouds

Many cloud services are based on other services, often other cloud services

- Certification work should be simplified, but getting information on subservices may be hard
- How to get the right level of assurance on these subservices?
- How to simplify procedures for certified services?
- The procedures need to be experimented

A chicken and egg problem

Composition (reuse of certification results) is a good solution

- Especially from the same scheme/framework
- More difficult on a starting scheme
- Few other schemes in the framework
- Transition from existing schemes, in particular National schemes, is essential

THREE MAIN TASKS AHEAD

Enhance

Finalize the scheme, make it usable, relevant, clear

- Add the missing parts and finalize the incomplete ones
- Work on the consistency and sufficiency of descriptions
- Integrate feedback and results of experiments

Experiment

Try out on practical cases the new aspects of the scheme

- Identify key use cases and different CABs
- Define security controls that meet a selection of requirements
- Experiment the assessment procedures

Refine

Define guidance to make the scheme more concrete

- Structure the guidance for the three levels
- Harmonize/coordinate guidance between different sources
- Validate the sufficiency of proposed guidance

BEING USEFUL

Cybersecurity certification is about increasing security, recognizing efforts by vendors; it is not about creating armies of box-tickers.

Multiple levels define a path to progression

- The scheme is intended to bring more CSPs to formal certification
- Some vendors may also reach higher levels than they have today

This is about convincing auditors, not just ticking boxes

- Assurance is about trust, about the opinion built by auditors
- The implementation of the schemes by CABs and NCCAs will be essential

Giving back to the community

- Parts of the scheme may be considered for standardization
- The scheme will form a basis for defining best practices and encouraging better security

THANK YOU FOR YOUR ATTENTION!

Thank you to all contributors from the ad hoc working group, from member states and from European institutions, and to my ENISA colleagues who made this happen!

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

certification@enisa.europa.eu

www.enisa.europa.eu

EUROPEAN CYBERSECURITY CERTIFICATION SCHEME FOR *CLOUD SERVICES*

Public Review has started

Until 07 February 2021

Make your voice heard!

Time to answer the Webinar poll