EUSEC
EU SECURITY CERTIFICATION

A GUIDE FOR STANDARD OWNERS

Implementing Multi-Party Recognition for Cloud Security Certifications

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

The multi-party recognition framework (MPRF) developed by EU-SEC aims to minimise the burden of becoming accredited to multiple cloud security certifications. It does this by providing a unified set of systematic and consistent activities towards achieving certification.

As the trusted parties responsible for a certification or compliance scheme, standard owners play an essential part in this. These guidelines explain the MPRF processes, details how standard owners (also referred to as 'scheme owners') and auditors can participate, and outlines the benefits for doing so.

MPRF: an overview of the actors

The actors listed below all play important roles in the MPRF process. This section focuses on standard owners. Guidelines are also available for auditors and auditees.

Governance Body
The EU-SEC Governance Body is a trusted party that qualifies external auditors to perform audits and establishes rules for recognition of external auditors. It also deals with complaints from stakeholders.

Standard owners
Owners or custodians of a proposed standard or framework. This can include owners of regulatory and industry sector standards.

Authorised auditors
Accredited assessment bodies that have been approved by the EU-SEC Governance Board

Auditees
Cloud Service Providers who are looking for a way to improve the effectiveness and cost efficiency of their cloud certification process.

Stakeholders Group – The stakeholders group includes the individual bodies of standard owners and EU regulators/agencies (e.g., EC, ENISA, EDPB). The role of the group is to provide guidance and eventually endorse the requirements comparison results of the MPRF's working groups.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

1. MPRF Operational Process Overview

The image below illustrates multiparty recognition framework's core operational processes. More information on the activities defined per process are to be found in EU-SEC project's deliverable 'D2.1. The multiparty recognition framework'[1].

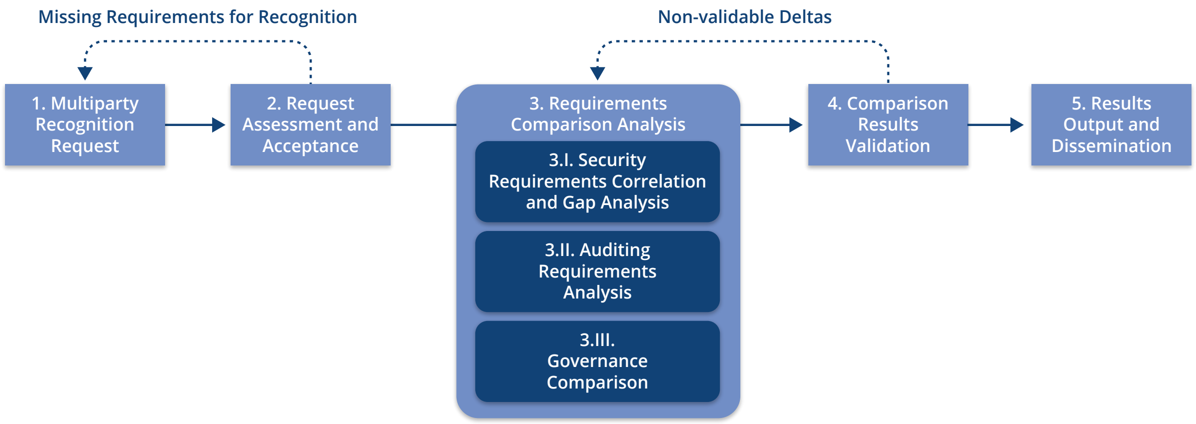
Missing Requirements for Recognition
Non-validable Deltas
1. Multiparty Recognition Request
2. Request Assessment and Acceptance
3. Requirements Comparison Analysis
3.I. Security Requirements Correlation and Gap Analysis
3.II. Auditing Requirements Analysis
3.III. Governance Comparison
4. Comparison Results Validation
5. Results Output and Dissemination

Figure 1: *Multiparty Recognition Framework Process Diagram*

The MPRF's operational processes interact with the framework's governance processes, which deal with change and complaint management.

Why should standard owners work with the MPRF?

Standard owners can realise significant synergies by connecting to a single management system that manages multiple aspects of organisational performance to meet the requirements of more than one standard and/or framework. This meets the intent of all international standards by *applying a risk management process that gives confidence to interested parties that risks are adequately managed and* ***they are part of, and integrated with****, the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls.*[2]

- Identify overlapping requirements
- Leverage efficiencies
- Reduce costs
- Minimise the level of risk
- Provide greater visibility and assurance to the organisation.

[1] D2.1 MULTIPARTY RECOGNITION FRAMEWORK FOR CLOUD SECURITY CERTIFICATIONS

[2] ISO/IEC 27001

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

a) How to interact with the MPRF's governance structure?

Standards owners have a key contribution to make by lending their collective intelligence to ensure the MPRF:

- reflects the current state of the art for cloud certifications and standards
- a governance framework is implemented and that the governance system that is applied throughout all framework activities are consistent, internationally harmonised
- ensure its long-term management, maintenance and synchronisation to the evolving cloud certification landscape.
- This includes information relating to the level of integration management system elements and responsibilities.

b) How does participating in the MPRF's operational processes help standard owners?

The output will add considerable value to standards owners as the data can serve as a valuable contribution to working groups during review and updates of said standards. This ensures future revisions of these standards are in line with industry requirements and internationally harmonised, in turn increasing the adoption of said standard(s) globally. Additionally, standard owners make a valuable contribution in decreasing the exponential rise in complexity, compliance fatigue and decreasing overall risk within the cloud ecosystem.

How can standard owners engage with MPRF operational and governance processes?

The assigned responsibilities are based on the RACI[3] model and are illustrated below, corresponding to each of the MPRF's operational processes. Full details of the standard owners' roles and responsibilities can be found in the D2.1 document.

Table 1: Standard owners' roles and responsibilities mapped to multiparty recognition activities

Multiparty Recognition Party Process		Activities				
		#1	#2	#3	#4	#5
Roles	EU-SEC Governing Body	R	AR	R	R	AR
	Standard Owners	AR	C	AR	AR	R
	Authorized Owners	AR	C	C	C	CI
	Auditees (the Cloud Service Providers)	-	-	C	C	CI

[3] https://en.wikipedia.org/wiki/Responsibility_assignment_matrix

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Process #1

- **Submit new certification standard**: A standard owner submits its certification standard for comparison against the reference framework and requests to have it included in the MPRF's requirements repository. CSA's CCM has been chosen as the reference standard for EU-SEC's MPRF. The request is to be placed to the MPRF governance body, and should include a certification standard's security requirements, auditing requirements and governance model.

- **Request access to requirements repository:** Standard owners place a request to access the requirements repository in order to compare their own certification with other standards in the repository (through the reference framework). Mappings, gap analysis and compensating measures to possible gaps will be available for retrieval.

- **(optional) Request to join the External Stakeholders Group[4]:** The governance structure of the EU-SEC framework introduces the concept of an external stakeholders group. Its role is to provide an active consulting, validating and endorsing role to the requirements comparison works performed

Process #2

- **Support standard's eligibility evaluation:** This process involves the MPRF governance body evaluating the submitted standard against the MPRF's criteria and requirements for the new standard's acceptance. The standard owner has a consulting and supportive role in this process; that is, maintaining contact with the governance body throughout the whole process, and assisting with the evaluation by providing additional clarifications whenever it is required.

  The standard owner's participation in this process ensures that the MPRF will only comprise certification standards with an equivalent level of quality and maturity.

Process #3

- **Support analysis of requirements comparison:** In this process, the standard owner's certification standard is to be compared with other standards in the MPRF's repository of requirements. The process will run either automatically by the MPRF (i.e., a certification standard publicly available is automatically included to the framework) or after a standard owner places a request.

[4] This request will be possible placed under EU-SEC governance (e.g., D2.4. Policy and role management process)

This project has received funding from the European Union's HORIZON Framework Programme
for research, technological development and demonstration under grant agreement no 731845.

- Standard owners are asked to contribute to the comparison works and provide their valuable insights into a semantic interpretation of their standard's requirements. The comparison activities involve mappings, gap analysis and compensating controls' formulation between the standards and the reference framework.

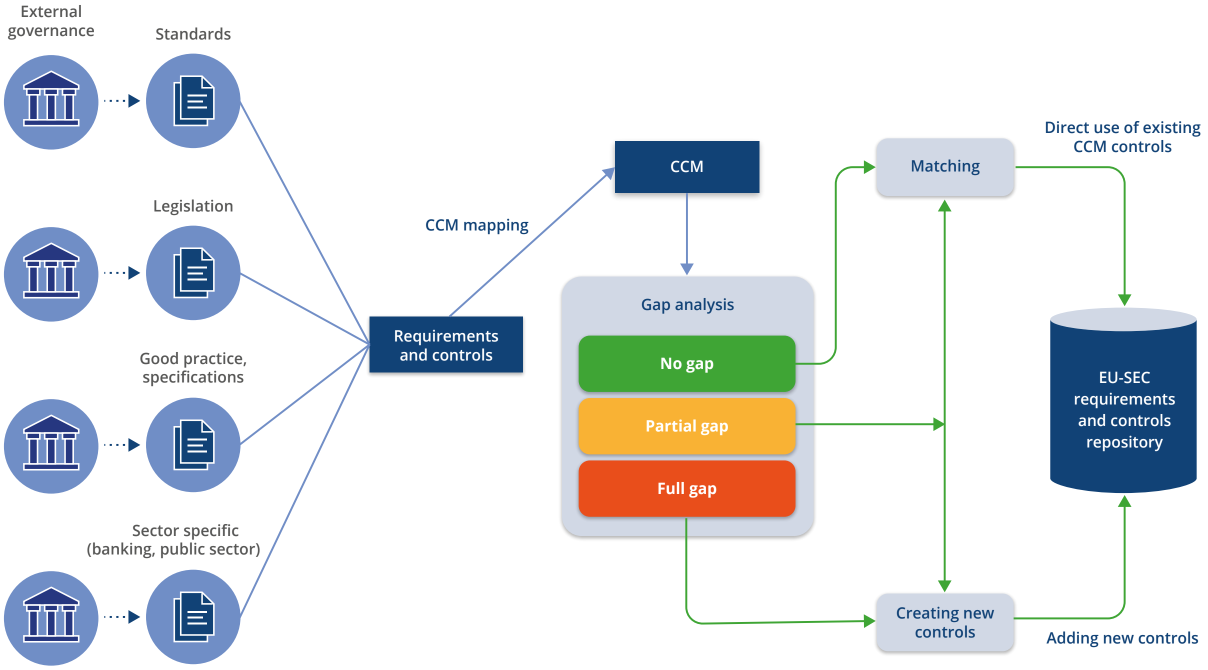
External governance
Standards
Legislation
Good practice, specifications
Sector specific (banking, public sector)
Requirements and controls
CCM mapping
CCM
Gap analysis
No gap
Partial gap
Full gap
Matching
Direct use of existing CCM controls
EU-SEC requirements and controls repository
Creating new controls
Adding new controls

***Figure 2:** Requirements collection and analysis process to establishing the EU-SEC repository*

Process #4

- **Validate results of requirements comparison:** In this activity, standard owners work collaboratively with other MPRF stakeholders (e.g., governance body, auditors) to validate the methodology and results of the requirements comparison. This MPRF process encourages the establishment of mutual agreements between the parties involved, and most importantly standard owners, to recognise full or partial equivalences that are found between the certification and/or attestation they govern and

Process #5

- **Acquire access to MPRF results:** Standard owners gain access to the MPRF's requirements repository, which is an archive of the requirements comparison analysis between the standard owner's certification standard and the reference framework.

Standard owners can use the repository to

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

keep track of multiple standards' differences and their evolution. It also provides the opportunity to review their own standards regularly, or to identify possible missing requirements and update them accordingly, if required.

Governance - Complaint Management Process (CoMP)

- **Submit a complaint:** Standard owners can submit a complaint through the MPRF's complaints management process. This could, for example, refer to operational or governance-related objections that a standard owner may have with regards to the MPRF's processing methodology and outputs. For instance, objections could refer to the MPRF's derived comparison mappings and gap analysis results, the comparison methodology used, or other operational matters.

Governance – Change Management Process (ChaMP)

- **Submit changes to certification standards included in repository:** In cases where a certification standard is updated, the standard owner provides the EU-SEC's governance body with the changes introduced to the certification standard's requirements and controls catalogue. This input will trigger the MPRF's change management process, which in turn will initialise the MPRF's requirements comparison process and will result in the integration of the new requirements in the requirements repository. Dependencies of the standard's new requirements with the reference framework will be identified and updated.

PROCESS #N	PROCESS NAME	STANDARD OWNER ACTIVITY
#1	Request Assessment and Acceptance	Submit new certification standard Request access to requirements repository Request to join the MPRF's stakeholders group
#2	Request Assessment and Acceptance	Support standard's eligibility evaluation
#3	Requirements Comparison Analysis	Support requirements comparison analysis
#4	Comparison Results Validation	Validate results of requirements comparison
#5	Results Output and Dissemination	Acquire access to MPRF results
COMP	Complaint management process	Submit a complaint
CHAMP	Complaint management process	Submit changes to certification standards included in the repository

Figure 3: *Standard owners involvement in MPRF processes*

ANNEX A – MPRF USE CASE SCENARIO FOR STANDARD OWNERS

For illustrative purposes, the following scenario is considered from the standpoint of a national organisation that wants to sign a contract with a foreign CSP and a national standard owner.

The scenario assumes that:

1. The foreign CSP holds a CSA STAR certification;
2. The national organisation wants to understand which of their standard's national requirements are already covered by the CSA STAR certification;
3. The CSP can focus on addressing the national requirements of the organisation that are not covered by CSA STAR;
4. The standard owner wants to identify missing requirements in their own standard and ensure the soundness of the multiparty recognition activities, especially with respect to the interpretation of their own standard's requirements by the EU-SEC working groups during the comparison works.

The standard owner's contribution per process of the MPRF based on the above scenario is described below in more detail:

Process #1

The EU-SEC governance body will contact and engage the standard owner upon receipt of a request for multiparty recognition between the national standard and CSA CCM.

The standard owner will have the opportunity to apply and join the stakeholders group whose purpose is to validate and potentially endorse the comparison results with their subject matter expertise.

Collaboration between the standard owner and the EU-SEC governance body can be triggered at any time, thus allowing the standard owner to communicate any changes or updates of its own standard (and hence to the multiparty recognition results).

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Process #2

The standard owner will be asked by the EU-SEC governance body to participate in its own standard's eligibility evaluation process against the established principles, criteria and requirements of the framework. In this phase, the standard owner will ensure that all eligibility requirements are met in collaboration with the EU-SEC governance body.

The CSA STAR certification scheme has already passed the eligibility evaluation and its requirements are at the core of the EU-SEC repository.

Process #3

In this process the security, auditing and governance requirements of the national standard will be compared with the corresponding requirements of the CSA CCM. The EU-SEC working groups will perform these activities under the supervision of the EU-SEC governance body. The standard owner will participate in this process as part of the stakeholders group, and will provide guidance on the requirements comparison works (e.g., mappings and gap analysis methodology used).

Process #4

The mutual recognition activities between the requirements of the national standard and CSA CCM have been concluded and archived at the EU-SEC repository after successful completion of the previous process. In step #4, the stakeholders group and owners of the two standards will review and validate the multiparty recognition results and potentially endorse them.

In practical terms, validation translates into the standard owner's agreement with the soundness of the multiparty recognition results. Hence, in order to acquire the national standard's certification, the CSP would only have to be compliant with those requirements or "deltas" of the national standard that are not met within CSA STAR.

Possible corrections to the established results that are agreed between the two parties will be provided back to the EU-SEC working groups for another round of comparison and better refinement of the final results.

Process #5

The standard owner will ensure the proper formulation of the multiparty recognition results and their archive to the EU-SEC repository.

In addition, the standard owner will be able to access the EU-SEC repository and retrieve those multiparty recognition results that would allow the identification of missing requirements in its own standard against the CSA CCM (and also against other renowned international or national standards), hence having the opportunity for the evolution and alignment of its own standards to new technological and security requirements.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EUSEC
EU SECURITY CERTIFICATION

A GUIDE FOR AUDITORS

Implementing Multi-Party Recognition for Cloud Security Certifications

This project has received funding from the European Union's HORIZON Framework Programme
for research, technological development and demonstration under grant agreement no 731845.

The multi-party recognition framework (MPRF) developed by EU-SEC aims to minimise the burden of becoming accredited to multiple cloud security certifications. It does this by providing a unified set of systematic and consistent activities towards achieving certification.

MPRF: an overview of the actors

The actors listed below all play important roles in the MPRF process. This section focuses on auditors. Guidelines are also available for standard owners and auditees.

Governance Body
The EU-SEC Governance Body is a trusted party that qualifies external auditors to perform audits and establishes rules for recognition of external auditors. It also deals with complaints from stakeholders.

Standard owners
Owners or custodians of a proposed standard or framework. This can include owners of regulatory and industry sector standards.

Authorised auditors
Accredited assessment bodies that have been approved by the EU-SEC Governance Board

Auditees
Cloud Service Providers who are looking for a way to improve the effectiveness and cost efficiency of their cloud certification process.

Stakeholders Group
The stakeholders group includes the individual bodies of standard owners and EU regulators/agencies (e.g., EC, ENISA, EDPB). The role of the group is to provide guidance and eventually endorse the requirements comparison results of the MPRF’s working groups.

Why should auditors work with the MPRF?

Auditors are a significant part of MPRF. They are responsible for conducting the audits which are made possible by mutual recognition of different certification schemes. For a certification body employing auditors, MPRF creates new possibilities. First, it creates distinct advantages over competitors when compared to traditional audits. The advantage of the MPRF process over conventional siloed approach is efficiency: The time and effort required to audit is significantly reduced when the number of audited controls can be reduced as a result of mutual recognition. This streamlines the auditing process since only the Delta between multiple certification schemes must be audited compared to multiple full audits.

For an auditor, the workload of a single audit is lowered when existing controls can be used for reference, which makes the auditing of requirements and controls much faster.

This is especially true for audit services for Cloud Service Providers. CSPs have to comply to many standards and audit schemes, so it is of special interest to streamline efforts and compare requirements, results and evidence for different schemes. By implementing MPRF, it is possible to significantly reduce efforts involved in applying for an additional scheme by recognizing the requirements and evidences already audited for another scheme.

This project has received funding from the European Union’s HORIZON Framework Programme
for research, technological development and demonstration under grant agreement no 731845.

MPRF is also a valuable tool for learning. For example, learning the differences, gaps and similarities of multiple certification schemes is made easier by utilising the requirements repository. Auditors are provided with access to the EU-SEC requirements repository which allows them to adopt information about the overlap between requirements from different certification schemes. This might also make the effort of achieving new accreditations easier and more tempting, since the certification body could then more easily expand their market offering in MPRF by providing the additional certifications that are available in MPRF.

How can auditors engage with MPRF operational and governance processes?

By looking at the RACI-matrix in Table 2, we can see that auditors play a consultative role in each of the steps of MPRF. This ensures continuous interaction between auditors and the governance structure. Interaction also takes place via the change and complaint management processes.

The output of the process is the set of requirements and controls that are used to achieve mutual recognition between two certification schemes. While the output is mainly used by the auditees, it has a significant effect on auditors too, since the auditors conduct the actual audits based on the output of the process. Therefore, it is important that auditors are involved in the MPRF processes to have the possibility of influencing the output.

Table 2: Auditors' roles and responsibilities mapped to multiparty recognition activities

Multiparty Recognition Party Process		**Activities**				
		#1	**#2**	**#3**	**#4**	**#5**
Roles	EU-SEC Governing Body	R	AR	R	R	AR
	Standard Owners	AR	C	AR	AR	R
	Authorized Owners	AR	C	C	C	CI
	Auditees (the Cloud Service Providers)	-	-	C	C	CI

Process #1

- **Request access to requirements repository:** The MPRF gives auditors the opportunity to understand the relationship between information security, privacy and auditing requirements defined by various compliance schemes such as BSI C5, CSA STAR, ISO or ISAE 3000. This opportunity is offered by the provision of access to the EU-SEC repository, where the certification schemes' requirements comparison results and respective subsidiary guidelines are archived and made available.

- **(optional) Participate in the Open Certification Framework (OCF) Working Group[7]:** The OCF WG is comprised and led by subject matter experts from the cloud security standardisation and certification community. The objective of the WG within the scope of EU-SEC will be the identification of new trends, standards, best practices and legal and regulatory requirements (e.g. EU Cybersecurity Act) in cloud security certification and their integration within certification solutions (i.e. self-assessment, third-party certification and attestation, and continuous auditing) already existing within the EU-SEC Framework and the CSA OCF.

- **(optional) Participate in the Cloud Control Matrix (CCM) Working Group[8]:** The CCM working group is responsible for performing requirements comparison analysis between cloud security standards. It is comprised of cloud security experts (cloud security practitioners, auditors, etc.) coming directly from the relevant industry. Its core activities fall under the MPRF's processes 3 and 4, where requirements comparison mappings, gap analysis and their validation are performed respectively.

Auditors will play a significant role in both working groups as the core components of the EU-SEC framework governance organisation.

Process #2

- **Support standard's eligibility evaluation:** Auditors have a consulting role in this process for providing support and clarification whenever this is required with respect to the evaluation of a certification scheme against the MPRF's eligibility criteria and requirements for such a scheme to be accepted and included in the MPRF process.

Process #3

- **Support analysis of requirements comparison:** In this process a certification standard is to be compared with other standards in the MPRF's repository of requirements. The process will be run either automatically by the MPRF (i.e., a certification scheme publicly available is automatically included to the framework) or after a request is placed by a scheme owner.

[7] Working Group - Open Certification Framework

[8] Working Group - Cloud Controls Matrix

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Auditors have a consulting role especially in the comparison work by providing their valuable experience gained from practice in the field. Auditors have the knowledge and experience of interpreting and assessing security requirements during an actual audit. The comparison work involves mappings, gap analysis and compensating controls' formulation between the security, privacy and auditing requirements as defined within the compared schemes. Auditors have an opportunity to affect the mapping between standards, which will potentially affect their own work, and therefore auditor's involvement is desired.

Process #4

- **Validate results of requirements comparison:** The auditors' role in this activity is working collaboratively with other MPRF stakeholders (e.g., governance body, scheme owners) for validating the soundness of the requirements comparison methodology and results.

This MPRF process encourages the establishment of mutual agreements between the involved parties, such as auditors and certification bodies to recognize full or partial equivalences that are found between the certification and/or attestation they govern and other certification schemes.

Process #5

- **Acquire access to MPRF-based auditing guidelines:** Auditors are given access to the MPRF's requirements repository, where the final requirements comparison results between the evaluated certification schemes are archived.

The content of EU-SEC repository will present auditors valuable information with respect to:

- ○ "How to" guidelines, such as this guideline, for understanding and using the identified differences (deltas) between two standards' security requirements to prepare and conduct an MPRF-based audit.
- ○ An integrated auditing scheme comprised of the "union" of the auditing criteria and requirements of the two compared certification schemes (i.e., both schemes' auditing criteria and requirements must be considered for an MPRF-based audit).

For more details see Annex B: **Auditor guidance – Case example.**

Finally, the MPRF, through the requirements repository, will enable auditors and audit firms to present and provide a more attractive compliance assessment portfolio to auditees (CSPs), in means of cost/time-effectiveness, efficiency, and as well as of increased transparency of the audit process.
The MPRF's operational processes interact with the framework's governance processes, namely, change and complaint management processes (as also shown in EU-SEC D2.1 deliverable).

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

Governance - Complaint Management Process (CoMP)

- **Submit a complaint:** Through the MPRF's complaints management process, auditors are able to submit a complaint. The complaint could for example refer to operational or governance related objections that an auditor may have with regards to the MPRF's processing methodology and outputs. For instance, objections could refer to the MPRF's security and auditing requirements comparison results and provided guidelines, etc.

Governance – Change Management Process (ChaMP)

- **Request for change of MPRF output results:** Auditors can place requests for change to the MPRF's comparison results and output products archived at the MPRF repository. For instance, auditors can provide additional input with respect to established MPRF-based auditing guidelines involving two standards, which may result such guidelines being reassessed and updated accordingly. Therefore, the governance body acts as a valuable link between the auditors and scheme owners to ensure that proper interpretation between standards can be established and if problems occur, they can be resolved.

PROCESS #N	PROCESS NAME	AUDITOR ACITIVITY
#1	Multiparty Recognition Request	Request access to requirements repository Request to join the MPRF's stakeholders group
#2	Request Assessment and Acceptance	Support standard's eligibility evaluation
#3	Requirements Comparison Analysis	Support analysis of requirements comparison
#4	Comparison Results Validation	Validate results of requirements comparison
#5	Results Output and Dissemination	Acquire access to MPRF-based auditing guidelines
COMP	Complaint management process	Submit a complaint
CHAMP	Complaint management process	Request for change of MPRF output results

Figure 4: *Auditor involvement in MPRF processes*

NOTE: Include further reading advice… maybe in a box. If you are interested to learn more into detail about:

[1] Security and privacy requirements and controls then read D1.2 (link to EU-SEC website)

[2] ISO/IEC 27001 0.1

[3] D2.1 MULTIPARTY RECOGNITION FRAMEWORK FOR CLOUD SECURITY CERTIFICATIONS

ANNEX B: AUDITOR GUIDANCE – CASE EXAMPLE

For illustrative purposes, we present a case example of how auditors should act in each phase of the MPRF audit, including the applicable requirements for auditors in MPRF-based audits. After reading, the auditor should be able to understand the auditing process in MPRF and understand the general auditing and auditor requirements.

MPRF-based audit in multiple certification scheme scenarios

The audit process for simultaneous multiple audits follows the same audit process as a single audit. As for traditional audits, the scope has to be identified and the auditee must prepare their organisation's ISMS or control environment against the requirements set out in the required certification schemes. Thus, when using the MPRF they can use mappings created between targeted certification schemes. For the auditee, the MPRF provides a tool can be used to select those requirements and controls required by both certification schemes and create deltas from those which are required by only one of those certification schemes. Then by using both directly mapped requirements and deltas the auditee can built up an advanced ISMS and Statement of Applicability (SoA) based on the requirements of both certification schemes.

After the auditee is confident that they have adequately prepared themselves against the targeted certification schemes they can call for an accredited certification body and their auditors to perform the actual audit process. The MPRF audit process follows the common audit process steps (e.g. ISO/IEC 27007 or similar). The auditee and auditor will agree the initiation phase to be done; in which the certification schemes and SCOPE are validated and common understanding of the readiness of the auditee ISMS environment is done. Compared to a traditional audit, the auditor has to acknowledge all certifications schemes to be applied, SCOPE and ISMS preparation has to be made using an MPRF-based approach.

The main difference for the auditor then comes from the preparation for the audit activities. In this phase the auditor uses the MPRF and control repository to plan the actual audit in such a manner that all targeted audits can be done during one audit process. The auditor uses the MPRF mappings to identify those requirements and controls required by all targeted certifications. Secondly the auditor uses the MPRF to create deltas from those requirements and controls required only by one of those certification schemes. By combining both mutual and individual requirements, the auditor can prepare to perform several certification scheme audits in one audit process. Such a method will save time compared to carrying out several independent audit processes. It should be noted that the auditor still has to have detailed knowledge of all audited certification schemes and their requirements. Even if the controls used are directly mapped between the audited certification schemes there might be some existing differences to what is actually required (e.g. if both audited certification schemes require the adequate legislation to be identified and followed, there might be actual differences between the required legislations in both of the certifications). The auditor has to collect the required evidence carefully for both certification schemes during the audit activities. Also, there might be differences in details of the controls required by the certification schemes (e.g. log retention time required might differ, in such scenarios highly restrictive should be used to fulfil the requirements of both certification schemes). Collection of the evidence should

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

be planned during the preparation phase in such way that requirements for the evidence is fulfilled in both certification schemes.

If the preparation of the audit activities was performed carefully using the MPRF, the phase of conducting the audit activities is done like a traditional audit. The method of collecting and storing evidence is based on the requirements set by both targeted certification schemes. Evidence and other information collected during the audit process can be used to validate the compliance against all targeted certification schemes. Nonconformities are handled as required by all targeted certification schemes.

After the actual audit activities, the reports, completion of the audit and follow-ups are done as defined in the certification schemes. At this point there is no existing report template which would suit for all certification schemes and due to this restriction, it might be that a separate report must be done on each targeted certification scheme. However, this should be easy if the preparation and collection of the evidence was done as required by certification schemes and MPRF.

Let’s break down the requirements:

General auditing requirements

Auditing requirements for audits based on the multiparty recognition framework are defined in the EU-SEC project’s deliverable “D1.3 Auditing and assessment requirements” . The deliverable concludes that both ISO 27000 -family and ISAE 3000 -standards can be equally used to provide the compliance assessment for cloud service security requirements since the standard families have a lot in common. In detail, the documents defining auditing principles and processes are the following: ISO/IEC 27006 and ISO/IEC 27007 for ISO 27001 audits and ISAE 3000 for ISAE 3402 audits.

Auditor requirements

As stated above, the ISAE 3000, ISO 27006 and ISO 27007 standards specify the mainstream auditing requirements in the context of cloud service security control environment’s compliance assessment. These standards provide both normative requirements and best practices for evaluation processes, for example. The key difference is that companies providing certification services on ISO, shall be accredited as the certification body by a member of the national accreditation organisation, whereas in order to issue Third Party Attestation Reports according to ISAE 3000 the audit firm needs to be registered as an accounting firm according to the respective national provisions.

When looking at the requirements for audit teams and auditors, the following were concluded in deliverable D1.3:

“The team executing the auditing engagement in the multiparty recognition context shall meet all the auditing competence requirements dictated by each of the compliance scheme(s) in the scope of the engagement”

In order to meet these requirements, the auditing

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

team shall have sufficient knowledge of the cloud service industry, risks and control landscape. The knowledge shall be demonstrated, e.g. by holding relevant certifications (e.g. CCSK, CCSP, ISO 27001 Lead Auditor) or other relevant training. However, sufficient knowledge and auditor firm requirements may vary depending on the standard in question, so the results of "Auditing requirements analysis" in MPRF's operational process ultimately defines the requirements for an auditor. Consult the governance body for additional guidance if needed.

Audit process

The auditing requirements and auditing process were tested and validated in the project's pilot exercises which are summarized in the EU-SEC project deliverable "D4.5 Consolidation and analysis – The pilot results" . One of the main findings in all the pilots was that the auditing process remains the same when MPRF is used. That is simply because the MPRF processes are executed beforehand and the audit is conducted based on the output of MPRF. Thus, the only difference between a regular and an MPRF-based audit are the audited requirements which are reduced based on the delta between certification schemes.

To understand how this all works, we will go through a fictional case where the compliance process of a CSP is described from the perspective of an auditor. At the beginning, when a CSP seeks to get certified against a specific standard, the MPRF operational processes commence. The auditor's role is to provide consultancy on the operational processes. It shall be noted that auditors, by definition, shall not provide consultancy during an audit, but during the MPRF processes it may be required. Auditors shall only provide assistance in matters that require auditor's competence, such as giving a professional opinion on certain control mappings, but any other kind of consultancy that would guide the auditee is strictly prohibited to ensure impartiality.

The following figure illustrates the auditing process used in MPRF-based audits. The auditing process, as illustrated in the figure, is identical with ISO-based audit process defined by ISO/IEC 27007 and is also compliant with ISAE 3000.

[10] D4.5CONSOLIDATION AND ANALYSIS–THE PILOT RESULTS

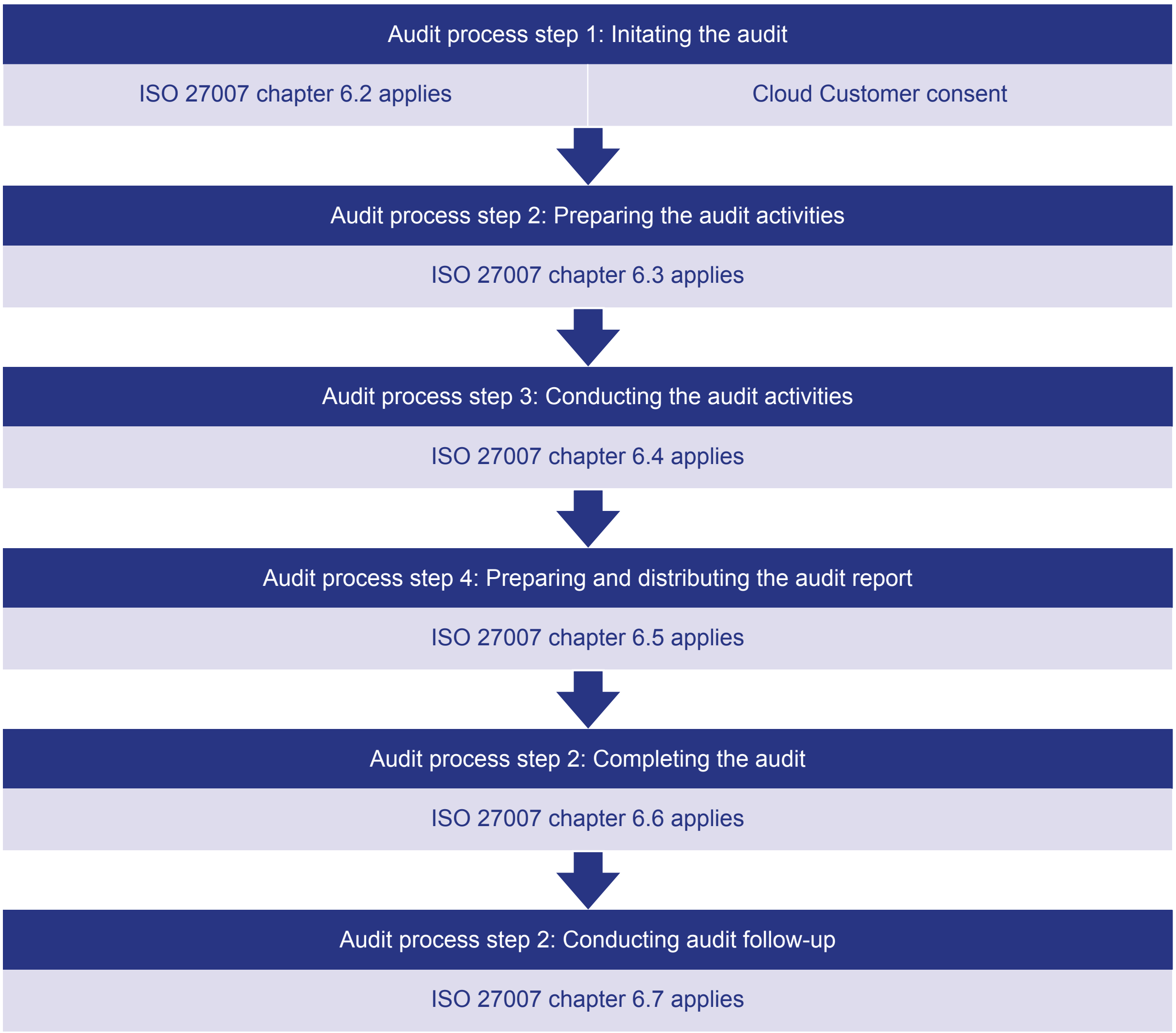
Audit process step 1: Initating the audit
ISO 27007 chapter 6.2 applies
Cloud Customer consent
Audit process step 2: Preparing the audit activities
ISO 27007 chapter 6.3 applies
Audit process step 3: Conducting the audit activities
ISO 27007 chapter 6.4 applies
Audit process step 4: Preparing and distributing the audit report
ISO 27007 chapter 6.5 applies
Audit process step 2: Completing the audit
ISO 27007 chapter 6.6 applies
Audit process step 2: Conducting audit follow-up
ISO 27007 chapter 6.7 applies

Figure 5: *Standard steps of an audit process with mapping to ISO/IEC 27007.*

The MPRF operational processes produce an output which ultimately defines the delta between multiple certifications. The delta defines the reduced audit criteria that should be used in the audit, which ultimately is the goal of MPRF. Other than that, the audit process in MPRF-based audits should follow the default processes.

In our example case, the CSP is responsible for implementing and creating their documentation based on the output of MPRF. Therefore, in our fictional case of an ISO-based audit, the auditee would create a new Statement of Applicability and other required documentation based on the defined delta. Then, the auditee's control(s) mapped to the security requirement of the EU-SEC requirement repository (for the multiparty recognition), would be tested against evidence demonstrating the operating effectiveness throughout a specified period of time, whenever possible.

When planning the audit, it must be noted that the audit plan in the multiparty context shall meet the requirements set by each of the compliance scheme(s) in the scope of the engagement. Otherwise the planning activities go in-line with the normal approach used in a regular audit involving a single standard. The auditing is conducted as defined in this document and in the figure above. For detailed descriptions, see deliverable D1.3 of the EU-SEC project. As stated, ISO/IEC 27007 chapter 6.4 applies for conducting audit activities. Respectively, standard procedures apply for audit close-out (ISO/IEC 27007 chapter 6.6), audit report distribution (ISO/IEC 27007 chapter 6.5) and follow-up (ISO/IEC 27007 chapter 6.7).

When handling nonconformities, the approach must be selected based on the audited standard. In ISO-based audits the auditee must address the nonconformities with an action plan set in place at the time of the audit completion. In ISAE-based audits no such requirements for follow-up actions are set. However, the auditor must report the issues found in the attestation report. Sometimes the auditor may face an issue where the auditee is compliant with a requirement from standard a, while still failing to comply with the same requirement from standard b. These situations could occur due to inconsistencies in the mapping or due to auditor's interpretation. To resolve the issue, it shall be reported by the auditor and shared with the connected standards and evaluated for their impacts. The conclusion of the non- conformity's severity shall be consolidated (feedback loop) and addressed accordingly. This provides the MPRF framework valuable feedback and supports the auditor in challenging situations.

Finally, when the audit is finished and the auditee has passed the audit, the standard certification/attestation process is finished, and the certification/attestation is granted by the auditor company according to industry standards based on the approach.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

EUSEC
EU SECURITY CERTIFICATION

A GUIDE FOR AUDITEES

Implementing Multi-Party Recognition for Cloud Security Certifications

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

The multi-party recognition framework (MPRF) developed by EU-SEC aims to minimise the burden of becoming accredited to multiple cloud security certifications. It does this by providing a unified set of systematic and consistent activities towards achieving certification.

MPRF: an overview of the actors

The actors listed below all play important roles in the MPRF process. This section focuses on auditees. Guidelines are also available for standard owners and auditors.

Governance Body
The EU-SEC Governance Body is a trusted party that qualifies external auditors to perform audits and establishes rules for recognition of external auditors. It also deals with complaints from stakeholders.

Standard owners
Owners or custodians of a proposed standard or framework. This can include owners of regulatory and industry sector standards.

Authorised auditors
Accredited assessment bodies that have been approved by the EU-SEC Governance Board

Auditees
Cloud Service Providers (CSPs) who are looking for a way to improve the effectiveness and cost efficiency of their cloud certification process.

Stakeholders Group – The stakeholders group includes the individual bodies of standard owners and EU regulators/agencies (e.g., EC, ENISA, EDPB). The role of the group is to provide guidance and eventually endorse the requirements comparison results of the MPRF's working groups.

This guide is designed to assist organizations wishing to obtain multi-party recognition and compliance with a variety of different quality standards, code of conducts and cyber security certification schemes.

Why should auditees work with the MPRF?

Cloud service providers are under considerable pressure to comply with several international, national, and sector specific standards and requirements. Such a proliferation of standards and requirements demands more resources be spent, increases compliance acquisition costs, and potentially also creates room for security vulnerabilities. The MPRF aims at tackling the former challenges by enabling its processes to compare two compliance schemes and output a minimum set of complementary security requirements. A CSP only needs to use this minimum set of requirements in addition to the existing certification during a third-party audit – not only reducing the overall auditing effort and costs but also the CSP's security surface exposure.

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

How can auditees prepare for the MPRF process?

1. Carefully collect all the requirements needed for the target scheme(s);

2. Using the EU-SEC Repository of Requirements, find the corresponding controls and compensating controls for each requirement collected in step 1;

   In many cases, different requirements will have overlapping controls. When that happens, note should be kept of which requirement that control is covering

3. Build your Statement of Applicability (SoA) based on the final list of controls from step 2. Make sure you do this step as thoroughly as possible, indicating which requirements are covered by each control, and whether the controls are implemented or not (with justification and/or evidence of implementation);

4. Contact an auditor with the aim of performing a MPRF-based audit. If the auditing company is not familiar with the Multi-Party Recognition Framework, then the auditor can refer to the MPRF guidelines for auditors and contact the EU-SEC governance body for additional assistance with the process. ";

5. Upon agreement from both parties, all the necessary legal and contractual documents shall be signed;

6. The auditor will send out a questionnaire and guidance checklist, to assess your readiness to engage with the MPRF-based audit;

7. When all documents are ready, the CSP should inform the auditor that the auditing process can start. This will not deviate from current standard audits;

   This also means that you should be prepared for the final auditor's assessment, where additional requirements, evidence and/or clarifications might be asked before stating compliance to the desired schemes.

This project has received funding from the European Union’s HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.