EU-SEC The European Security Certification Framework

EU-SEC working package 4 (WP4) T4.1/D4.1

EU-SEC D4.1 SI-MPA audit report

Introduction

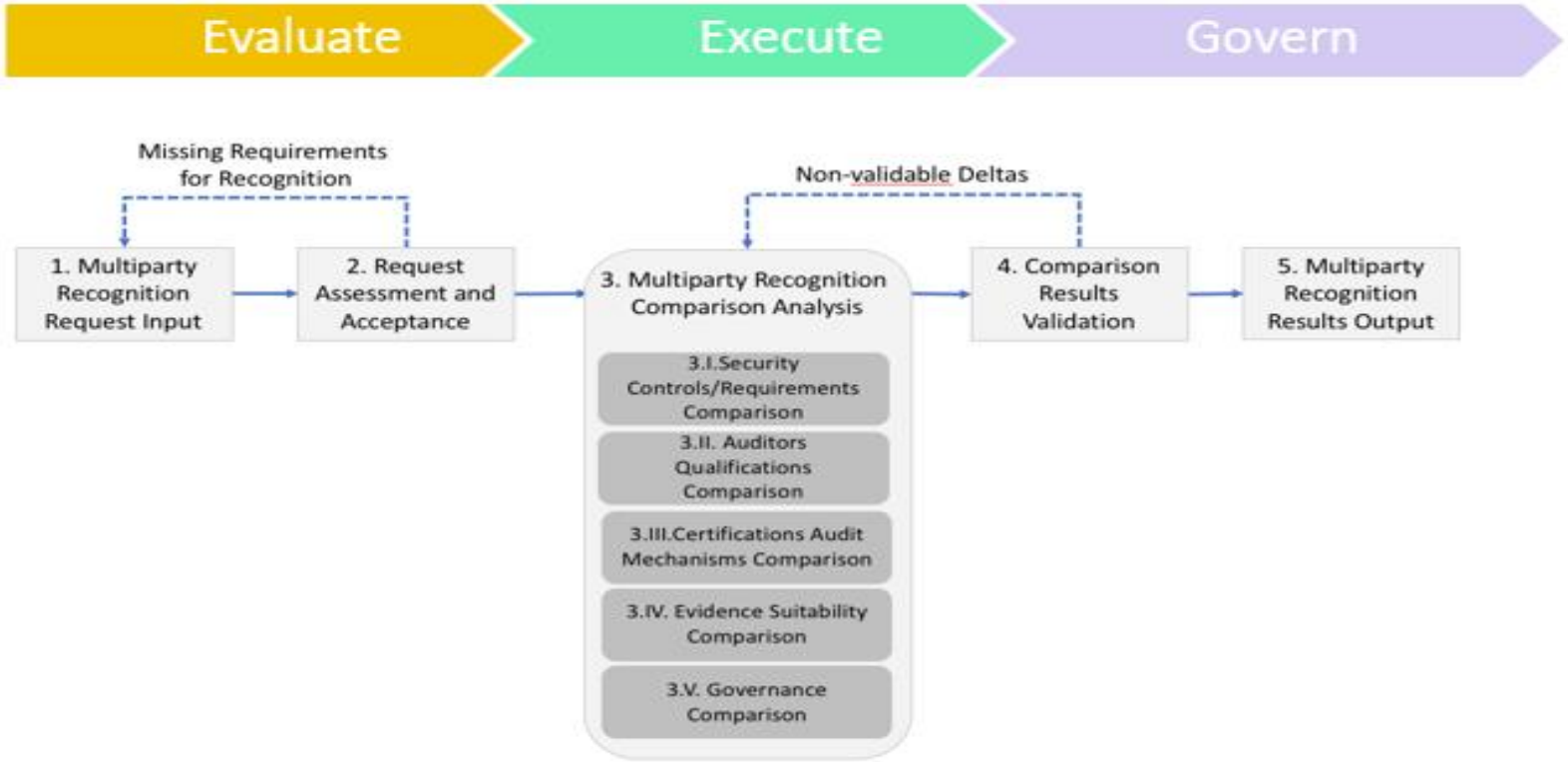
- The deliverable (D4.1) present an execution of audit pilot in the Slovenian Government Cloud (SGC is governmental ICT infrastructure managed by the Ministry of Public Administration, dedicated to offer cloud computing services to citizens, businesses entities and government administration).
- The ministry's SGC has already obtained the ISO 27001 certificate for the ISMS of the core business process.
- This deliverable D4.1 is part of the EU-SEC working package 4 (WP4) which main goal is to test and evaluate the core activities of the Multiparty Recognition Framework (MPRF) defined in the document D2.1.
- The testing and evaluation of the activates of MPRF is done through a table top exercise as well as a real-life ISO-based audit involving the Ministry of Public Administration of the Republic of Slovenia (SI-MPA), as an auditee, and NIXU Corporation (NIXU) as an auditor.

Scope and objectives

- **The objectives:** a) Testing the MPRF process and its core activities

  b) Assess the suitability of the MPRF to satisfy the needs of the auditee via the simulation of a real-life audit

- **The scope:** Evaluate and Execute phase of the MPRF



Methodology

- **Objective 1**: Testing the process and the core activities of multiparty recognition framework theoretical model and readiness of the EU-SEC repository, within the audit's scope:

  a) Evaluate phase (Multiparty recognition request input, Request Assessment and Acceptance, Comparison Results Validation)

  b) Multiparty Recognition Comparison Analysis phase (Security controls / requirements comparison, Auditors' qualifications comparison, Certifications audit mechanism comparison, Evidence Suitability comparison, Governance comparison).

- **Objective 2**: Assess the compliance of the auditee ISMS through a standard audit process to the selected requirements from ISO 27017 and Slovenian national requirements (definition of the scope of audit, definition of applicable controls SoA + Extended SoA, sampling, audit execution and reporting).

ISO based audit (MPRF Validation Approach)

REPUBLIC OF SLOVENIA
MINISTRY OF PUBLIC ADMINISTRATION

Control Set for ISO 27001

EUSEC
EU SECURITY CERTIFICATION

Multiparty Recognition Framework

EU-SEC Requirements Repository

Mapping Validation

EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK
D4.1 SI-MPA AUDIT REPORT
0.5
PROJECT NUMBER: 731845
PROJECT TITLE: EU-SEC

nixu

Requirements:
ISO 27001
ISO 27017
ISO 27018
CSA CCM
SI National

CCM CAIQ v3.0.1

Obstacles in the audit process

- Lack of understanding the scope of audit
- The preparation of certain reports was delayed
- Certain products that have not yet been completed have gone to the preliminary examinations
- The deadlines for the submission of deliverables are extended
- The essential content and the conclusions of the auditor were in a lag
- Distance from the auditor and the auditee
- Problems were with untranslated documentation
- Language barrier (English, Finnish, Slovenian)

Conclusions

- Audit pilot use case shows that MPRF theoretical model could be executed in real-life situation, what is done by evaluating the compliance of SI-MPA ISO 27001 ISMS to additional cloud specific security requirements, coming from ISO 27017 and Slovenian national requirements.
- By using the EU-SEC repository in adherence to MPRF process, we found almost 80% less security requirements that were needed to be used in an audit. This shows that MPRF reduces the workload of the audit process and increases its efficiency.
- Security controls comparison between ISO 27001, ISO 27017 and Slovenian national requirements were compared through already working CSA CCM, which gives EU-SEC MPRF higher level of trust and usability.
- By the execution of the audit we had to provide a number of evidences in many forms. Due the limited number of requirements in scope, evidence comparison does not provide full picture on how the collection and comparison would work in real-life, and how to achieve full trust to evidences collected by auditors of different audit organisations.
- Auditee and auditor had difficulties understanding the concepts and process structure of MPRF. This could be explained by the nature of this EU-SEC innovative project and the audit pilot use case, where new approach to audit process and MPRF has to be tested and perfected in the real case.

Recommendations

- MPFR theoretical model needs to be explained in more operational level, with supporting documentation, manuals and guidelines, which would help the auditee to be prepared for MPRF audit and auditor to execute the audit.
- Existing EU-SEC Requirements and controls repository is built as an Excel spreadsheet which is difficult to handle where one or many requirements are mapped to one or many controls and becomes non-transparent. Repository should be built in a database with simple interface for adding and mapping new requirements, which will significantly improve usability and efficiency of the repository.
- Through the security controls comparison, the differences and inconsistency in mapping execution were discovered. This finding shows on different subjective opinions when mappings of ISO 27001 and ISO 27017 to CCM were performed. Further verification is recommended to raise the maturity level of EU-SEC Requirements and controls repository.