European Security Certification Framework

WP 4.2 Final

Rastislav Neczli, Samuel Belej

MINISTRY
OF FINANCE
OF THE SLOVAK REPUBLIC

Goal of D4.2.

- The scope of Pilot 1 was about applying, testing and validating the Multiparty Recognition Framework. Based on these goals, MF SR in the role of the auditee selected one representative service in the G-Cloud environment. We derived general rules for ISMS of other services provided in the government cloud.
- We applied the following principles:
  - Test the principles and mechanisms for the multiparty recognition framework, presented in D2.1 “Multiparty recognition framework for cloud security certifications”.
  - Assess the compliance of the MFSR with the requirements included in ISO 27001, ISO 27017, CSA CCM already collected in Task 1.2 and combined in EU-SEC Security Requirements Repository (D1.2).

PARTNERS INVOLVED

Auditee

MINISTRY
OF FINANCE
OF THE SLOVAK REPUBLIC

OFFICE OF THE DEPUTY PRIME MINISTER
OF THE SLOVAK REPUBLIC
FOR INVESTMENTS
AND INFORMATIZATION

MINISTRY
OF INTERIOR
OF THE SLOVAK REPUBLIC

Auditor

nixu
cybersecurity.

Situation at the beginning of the project

1. The government cloud architecture is originally built as a private cloud to provide services to public administration organizations;
2. After building the first phase of government cloud came a change in strategy and the government cloud could be opened up to other providers so public administrations could also use commercial cloud services;
3. Government cloud becomes hybrid cloud. For this purpose, MFSR will use the outputs of this project to verify cloud services that will be included in the G-Cloud service catalogue;
4. The timeline of building G-Cloud assumes that government services at all levels of IaaS, PaaS and SaaS will be available in 2020 and hybrid as well. This fact predetermined the way we could conduct the audit
5. IaaS services are currently available and therefore we decided to select one representative service for verification.

Validating the multiparty recognition framework

The evaluation phase of the MPRF-based audit includes following steps:

- ***Multiparty Recognition Request*** *is the provision and collection of inputs that will be fed to the framework, involving requests from the compliance schemes to initialize the multiparty recognition framework process.*
- ***Request Assessment and Acceptance*** *evaluates the request against the multiparty recognition framework's criteria such as comparability of the requirements and governance model, and principles such as relevancy and transparency. Approval of the request is required to initialize the correlation and gap analysis of the submitted compliance scheme.*

Life-Cycle Processes

- The following Life-Cycle processes were followed within the project:

1. The security requirements Correlation and Gap Analysis
   - Results and definition of the new requirements are performed using the EU-SEC requirements repository as the reference point.
   - An assumption was made that the auditee already had ISO 27001 certification. Auditee had built an ISO 27001 (Annex A) based SoA with required controls implemented and now targeted to implement and evaluate the ISO 27017 and national Slovak requirements to their Statement of Applicability.
2. An extended SoA was created. The extended SoA included controls from the targeted schemes ISO 27017 and Slovak national requirements.
   - The comparison and GAP analysis of selected requirements were conducted as required by MPRF.
   - During Gap analysis No Gap/partial Gap/Full Gap were identified.
   - If required, then in the GAP analysis additional compensating controls were created to fill all recognized GAPs.
   - Based on the GAP analysis phase in the pilot the final extended SoA was created.
3. Actual pilot audit was performed using the CSA CCM controls mapped through the repository or requirements to ISO 27017 and Slovak national requirements. Analysis was performed against those mappings.

CONCLUSION

- The audit pilot of the government cloud service was executed using the MPRF. The experience from the pilot audit indicates that the MPRF process can be followed to achieve mutual recognition between certification schemes. The two main findings were that for the auditee, on one hand the EU-SEC framework provides significant potential to reduce the effort and resources needed to achieve multiple certifications and on the other hand the auditors observed that the actual auditing process was not affected when using MPRF.

- Side output of the project is the decision of stakeholders in Slovakia use MPRF approach by extending onboarding methodology for cloud services within the Slovak G-Cloud.