EU-SEC The European Security Certification Framework

EU-SEC working package 4 (WP4) T4.3/D4.3

EU-SEC D4.3 SixSq audit report

- **SixSq** is an SME that provides cloud neutral solutions allowing companies and institutions to benefit from cloud computing while avoiding lock-in. Its smart cloud-in-a-box appliance, NuvlaBox, is a simple plug & play edge solution which brings customers a private cloud at an affordable price as well as playing an intrinsic part of smart city and IoT strategies. SixSq's smart multi-cloud and edge management platform, Nuvla, offers application deployment from a single, simple dashboard. Nuvla is powered by SlipStream, the company's cloud management platform which allows users to deploy any application in any cloud or edge, and it will also serve the EU-SEC project with the management portal for the repository of evidence. As SixSq matures, it will address larger and more sensitive markets.

Audit Scope

SixSq develops and provides cloud-based software and services to both private and public organizations. Consequently, the company's ISMS applies to the following areas:

- *Development of Software and Products,*
- *Operations of Services.*

The development and operations areas cover the following products and services:

- *Nuvla,*
- *SlipStream, and*
- *NuvlaBox (all versions),*

as well as the supporting infrastructure required to develop, operate, and support them.

Objectives

- ***"test the process and core activities of multiparty recognition framework"***, by doing a practical review and assessment of the framework's theoretical model and readiness of the EU-SEC repository, within the audit's scope and the auditee's goal for compliance with ISO 27017;
- ***"assess SixSq's compliance with the requirements of ISO 27001 and ISO 27017"***, through a standard audit process, which considers the MPRF as a trustworthy baseline for the mutual recognition between ISO 27001 and ISO 27017;
- ***"test the tools developed within WP3, to assess their readiness within the audit process"***, which consists on testing the Evidence Store. This is to be done by gathering evidence to support the audit, storing it and finally testing the evidence management capabilities of the Evidence Store via the Nuvla Web Interface.

Conclusions

- In general, the auditing experience indicates that for this specific use case, the use of the MPRF might not bring a significant added value since ISO 27001 and ISO 27017 have a big overlap, and the actual difference between both can be more easily fulfilled by implementing the native ISO requirements rather than relying on the EU-SEC repository.
- There is an obvious upside of using the EU-SEC framework and tools, in the sense that it allows the auditee to exponentially decrease the future effort for acquiring other certifications.
- It is also clear that the use of the framework does not affect the overall auditing process, which makes its adoption more appealing for both auditees and auditors.

Recommendations

- improve the overall MPRF documentation and guidelines, in terms of definitions, usability and applicability
- a database application should be built in order to improve the usability and efficiency of the repository. The application should provide a simple interface to extract new required requirements and controls from it when acquiring new certifications. It should assist the auditee when creating deltas and compensating controls
- further evaluate and improve the mapping of the requirements. This should be done according to a defined change management process. Follow the continuous improvement process of the Multiparty Recognition Database (mappings)
- build a story board as part of the EU-SEC dissemination plans and framework usage manuals, explaining what's the motivation for using the framework, in which circumstances it should be used, and how