EU-SEC The European Security Certification Framework

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

EU-SEC D4.4 Fabasoft & PwC Pilot on Framework Verification

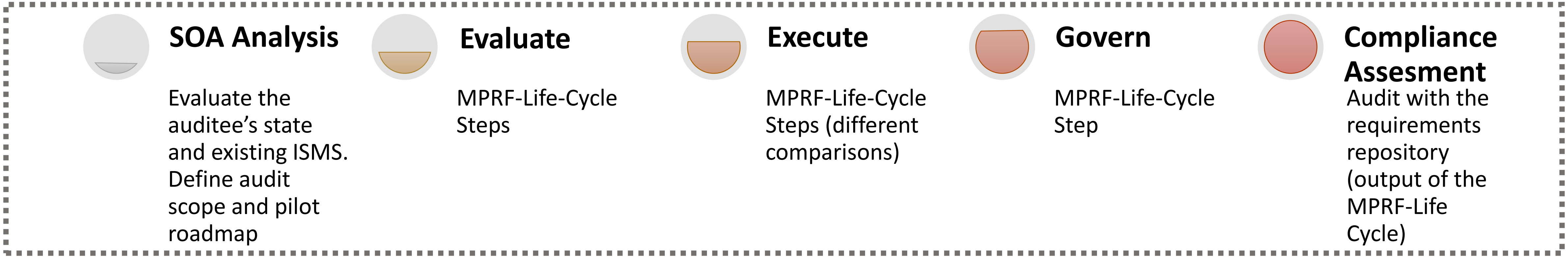
Fabasoft®

pwc

Assumptions & Approach

I. **Assumption:** Fabasoft ha a Star attestation and therefore is compliant to all 136 CCM requirements.
   - The CSA CCM is a superset of other compliance schemes (such as SOC 2 TSCs).

II. **Assumption**: Fabasoft strives (in theory) for a BSI C5 attestation.
   - In reality, Fabasoft already is compliant to BSI C5 2016.



SOA Analysis

Evaluate the auditee’s state and existing ISMS. Define audit scope and pilot roadmap

Evaluate

MPRF-Life-Cycle Steps

Execute

MPRF-Life-Cycle Steps (different comparisons)

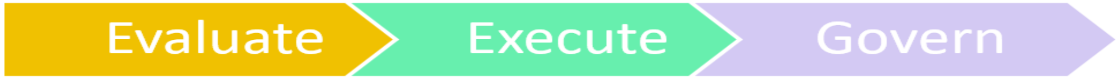
Govern

MPRF-Life-Cycle Step

Compliance Assesment

Audit with the requirements repository (output of the MPRF-Life Cycle)

Multiparty recognition framework lifecycle:



Multiparty Recogniction Life-Cycle

- The exploited schemes were already included and mapped in the Framework
  - PwC needed to double check
  - in some cases (approximately 5%) PwC came up with revised interpretations and mapping argumentations
- Verification of mappings and closing of gaps
  - An auditor will always cross-check the work of the auditing party of the scheme used as the baseline, if the auditing party is not the current auditor itself.
- As both schemes are based upon ISAE 3000, PwC accepts evidences produced for STAR Attestation, when using it for BSI C5
  - when looking at requirements with “no gap”
  - Auditors need to decide case-by-case by considering the individual context
- Identified inconsistencies were discussed with the Governing Body to provide the auditee a sound solution to advance with the audit
  - the complaint management process would process these activities and the repository would be updated

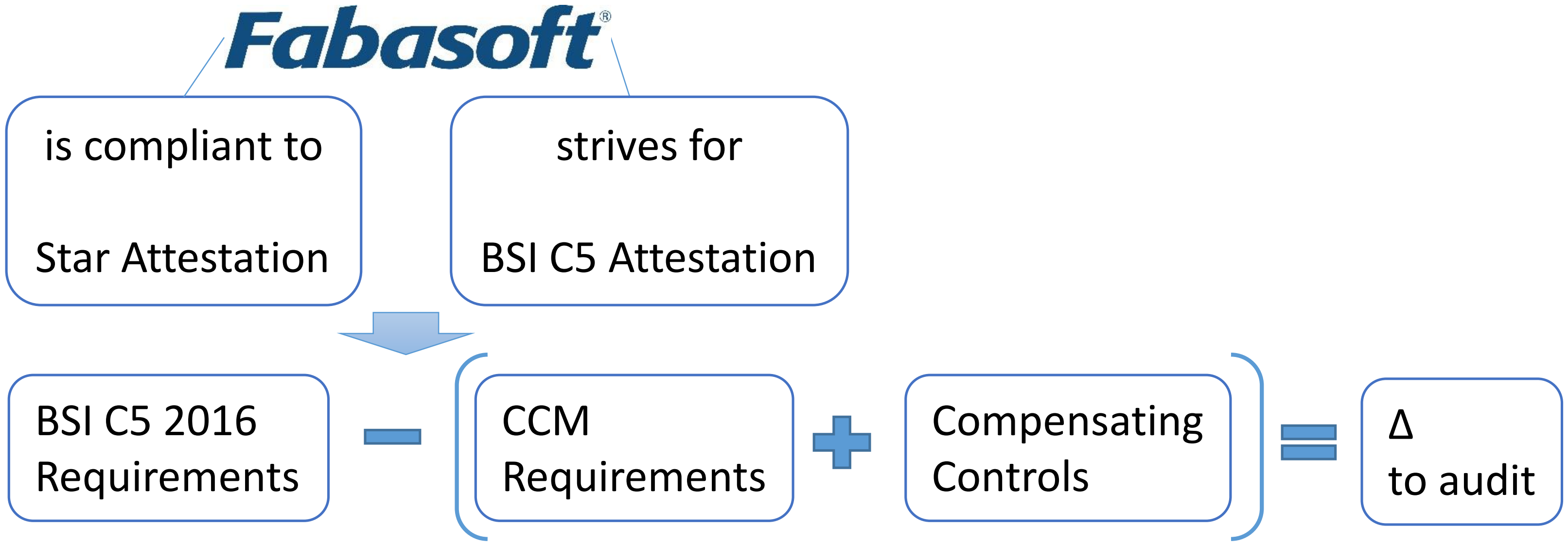
Results (Compliance Assessment)

- Fabasoft was able to subsequently narrow down the list of requirements for the pilot audit scope.

- The preliminary math for deriving the Delta was:

  114 (BSI C5) – 83 (EU-SEC no gaps) – 8 (PwC revised to no-gaps) + 4 (PwC revised to partial gaps) = 27 requirements

- In the pilot, the participants were able to reduce the (T4.4)-Repository to 27 requirements.



Fabasoft

is compliant to

Star Attestation

strives for

BSI C5 Attestation

BSI C5 2016 Requirements − (CCM Requirements + Compensating Controls) = Δ to audit

Recommendations

- Operational Applicability
  - the Framework already works well in its current form
  - further efforts not need to focus on improving the quality of the requirements interpretation & mapping process and the usability of the MPRF
- Requirements Interpretation & Mapping
  - an "appropriate experts group" either accepts or rejects requests for changes
  - this task is upcoming project work to be done in D2.5
- Usability of the Framework
  - the EU-SEC Framework should focus on guidelines to apply the tool for involved stakeholders: scheme owners, auditors and auditees. Because if auditees understand the benefits and ask the auditors to perform an MPRF-based audit, they create a market demand and therefore accelerate the market adoption of the framework.