EUSEC
EU SECURITY CERTIFICATION

D 1.3: AUDITING AND ASSESSMENT REQUIREMENTS

Overview of the research

Task Leader: Mikko Larikka, Nixu Corporation

D1.3 Auditing and assessment requirements
Guidelines, standards and normative references in scope of D1.3

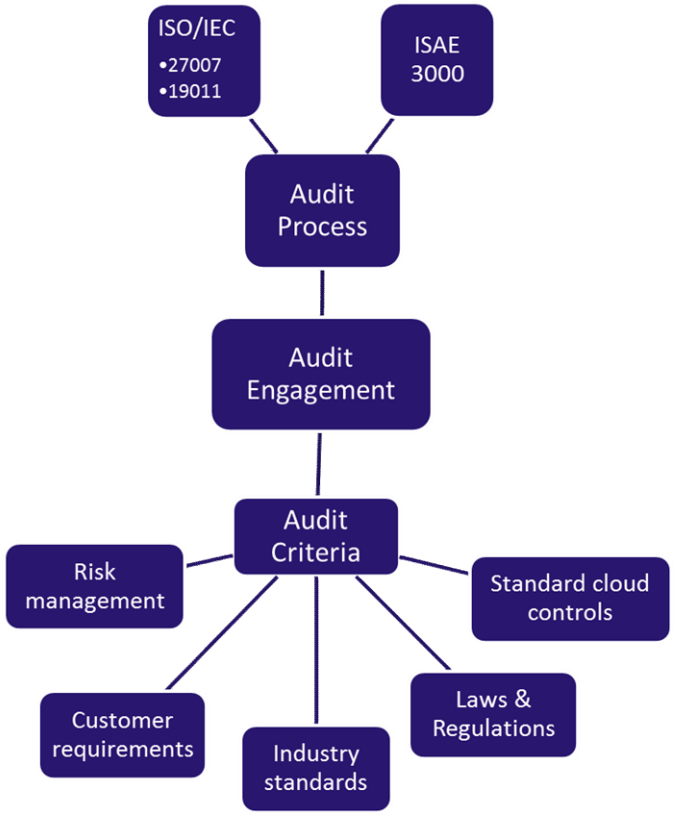
In the context of auditing of cloud service security requirements ad the control environment thereof, the following sources were studied:

- ISO Standards (27001 family, 17021, 17024, 19011)
- ISAE Standards (ISAE 3000 & ISAE 3402)
- SOC 2 (Trusted services criteria)
- German BSI C5 (Cloud security framework)
- CSA STAR Certification & CSA STAR Attestation frameworks
- French SecNumCloud (Cloud security framework)
- Ministry of Finance of the Slovak Republic (Auditing requirements)
- Slovenian Ministry of Public Administration (Auditing requirements)

D1.3 Auditing and assessment requirements
Research methodology

The auditing requirements were analyzed from the following perspectives:

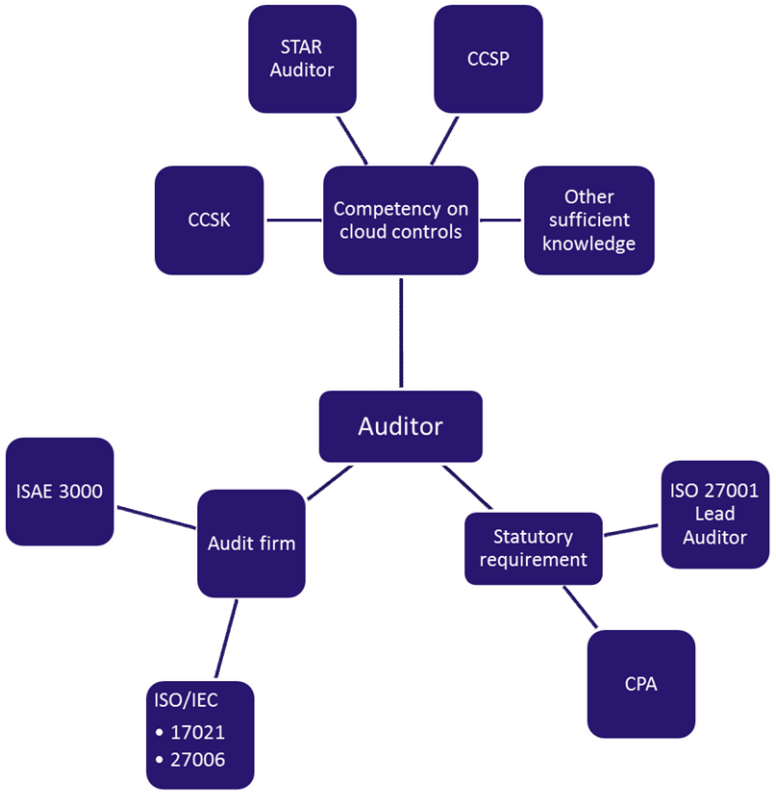
- **The auditor requirements** split into personal competency and accreditation requirements, and audit firm requirements
- **The process requirements** the auditing to be followed for auditing of cloud controls design and effectiveness
- What is considered as "**sufficient appropriate evidence**" and how it should be obtained



D1.3 Auditing and assessment requirements
General requirements for auditor (D1.3 chapter 3.2.1)

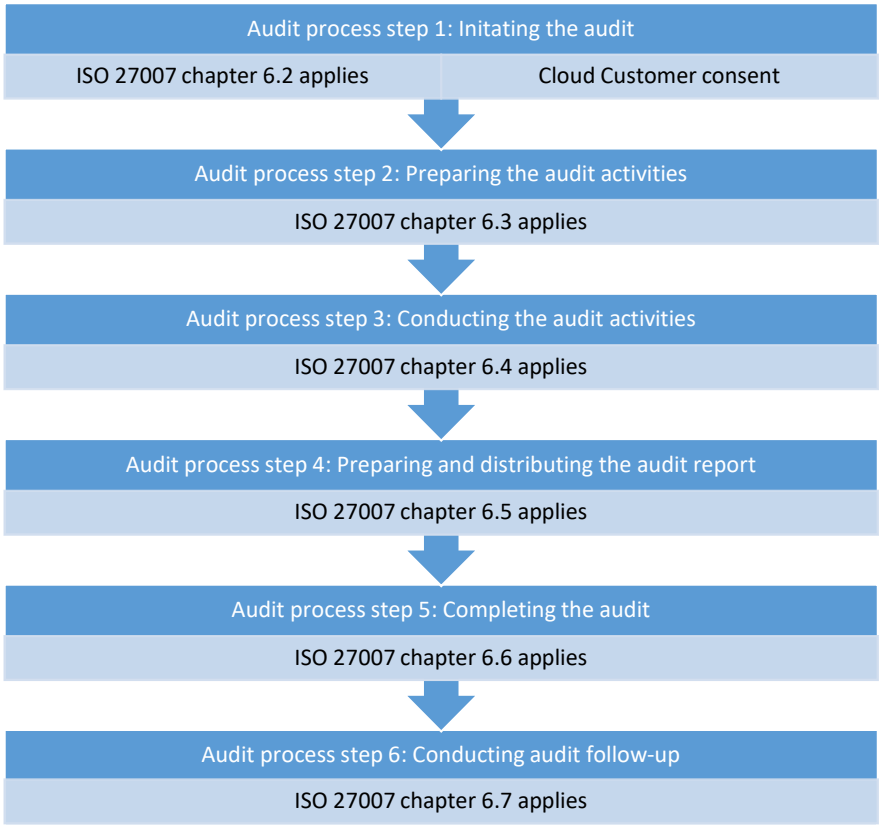
Meaningful to study auditor requirements narrow down to the two tracks:

- ISO/IEC 27006 and 27007, which are applied to companies and auditors providing auditing of cloud security management systems
- ISAE 3000 auditing standard to conduct either type 1 (design) or type 2 (operating effectiveness) assessment, resulting a SOC2 attestation
- Analysis:
  - Mutually same given the context
  - Both require the auditor to have **competency** on the target (industry) risk and control landscape
  - **Statutory requirement,** however**, is not interchangeable**



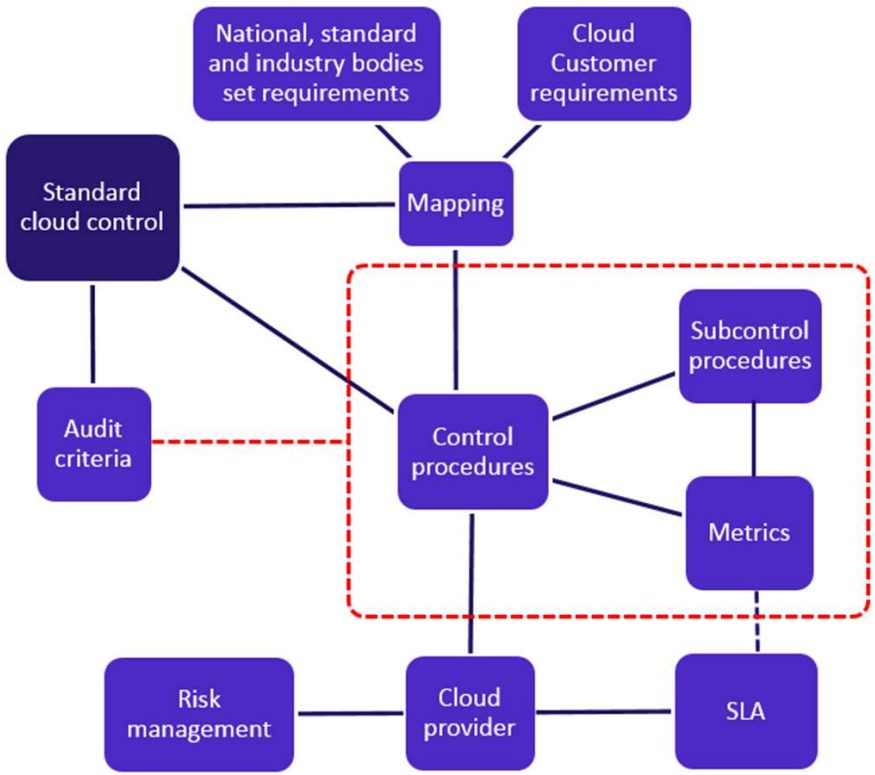
D1.3 Auditing and assessment requirements
Auditing Process Comparison of the ISAE 3000 and ISO/IEC 27007

- A comparison of the auditing processes between ISAE 3000 and ISO/IEC 27007 was conducted by using a ISO/IEC 27007 standard as the baseline. Each of the process steps were analyzed separately.
- Analysis:
  - The audit process at a practical level is the same between the two standards.
  - However, a difference can be found in audit process step 2: Preparing the audit activities where ISAE 3000 type 2 audit amends the ISO auditing requirement
  - **The main difference** is: in **ISAE** 3000 based auditing there must have (historical) evidence of the operating effectiveness throughout a specified period of time (e.g. 12 monhts)



D1.3 Auditing and assessment requirements
Multiparty recognition of the audit results

- Assuming a cloud service provider seeks for multiple certifications (e.g. PCI DSS, SOC2, ISO27001, and BSI C5):
- Statutory vice the auditing must be lead by QSA, CPA or ISO 27001 Lead Auditor
  - The lead auditor's competence and qualification requirement varies by the applied standard/framework and must be considered case by case.
- Audit plan (audit process step 2) must address the overlapping control requirements.
- In practice the auditee shall have “super” control procedures and/or documentation, and record of operation, for the auditing purposes, where the control procedures address all the mapped requirements, introducing e.g. necessary subcontrol procedures, where required
- In most cases building a control environment consuming **mapping data from CCMv3** and structuring information security management system **documentation and operations records according to ISO/IEC 27001 topics**, can be seen multiparty recognition friendly approach.



D1.3 Auditing and assessment requirements
Next steps

- Work continues by providing
  - Review support for control requirement mapping data (D1.2)
  - Contribution to **D1.4 Chapter 4 Multiparty recognition requirements** and
  - Contribution to **D2.1 Multiparty Recognition Framework for Cloud Security Certifications**.
  - Review support for **EU-SEC / WP4 / Common pilot plan**, as the auditee must identify and map the overlapping control requirements, and auditor shall provide guidance in structuring information security management system documentation and operations records according to ISO/IEC 27001 topics, in preparation for the auditing.
  - **Dissemination support** (WP6)