EUSEC
EU SECURITY CERTIFICATION

# EUROPEAN SECURITY CERTIFICATION FRAMEWORK DELIVERABLE

## VERSION: 1.0

## PROJECT NUMBER: 731845

## PROJECT TITLE: EU-SEC

# D 1.3: AUDITING AND ASSESSMENT REQUIREMENTS

| DUE DATE: | DELIVERY DATE: |
|---|---|
| 31.10.2017 | 28.11.2017 |
| AUTHOR: | PARTNERS CONTRIBUTED: |
| Mikko Larikka, NIXU | NIXU, CSA, PwC, SI-MPA, MFSR, SixSq |
| DISSEMINATION LEVEL:* | NATURE OF THE DELIVERABLE:** |
| PU | R |
| INTERNAL REVIEWERS: | |
| SI-MPA, Fabasoft, CSA | |

*PU = Public, CO = Confidential

**R = Report, P = Prototype, D = Demonstrator, O = Other

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845

# EXECUTIVE SUMMARY

EU-SEC project contributes to enhanced mapping of laws, regulation and industry requirements to standard cloud controls. In this deliverable we study differences in professionally conducted audit and assessment engagements, and applied audit criteria.

It is not optimal for a cloud service provider to allow their customers to audit the IT operations directly. Instead, the cloud service provider may assign an independent audit and assessment firm to certify or attest on its information security management system and controls. Certification and attestation processes are governed with well-defined standards such as ISO/IEC 27000 and ISAE 3000.

After analysis of the standard, industry, law and regulation stated requirements selected to be in the scope of this deliverable, and in attempt to optimize cloud service providers' point of view, it may be optimal for an auditee to seek certification through ISO/IEC 27001, with ISAE 3000 specific amendments for the audit process. Benefits of this approach include but are not limited to standardized processes to maintain compliance, to handle non-conformities and to perform continuous certification.

A cloud service provider seeking for multiple accreditations may benefit from an EU-SEC designed multiparty audit and assessment engagement, to meet not one but several audit criteria with one engagement and this way, possibly lowering the "unit" cost of compliance for the cloud service provider. Therefore, we recommend building control environment in compliance with CCMv3 and structured according to ISO/IEC 27001 topics allowing to seek for ISO/IEC 27001 certification. This is in good alignment with most requirements, including ISAE 3000, and does not limit the cloud service provider from seeking an attestation on controls according to SOC 2, BSI C5 and/or SecNumCloud, requiring further efforts, however, to comply.

# ABBREVIATIONS

*Table* 1. *Abbreviations used in this document.*

| Abbreviation | Description |
|---|---|
| **(ISC)²** | (ISC)² is an international nonprofit membership association best known for its award-winning Certified Information Systems Security Professional (CISSP®) certification, with additional certification and education programs that holistically address security. |
| **ANSSI** | Agence nationale de la sécurité des systèmes d'information (eng. National Cybersecurity Agency of France) (https://www.ssi.gouv.fr/en/) |
| **BSI C5** | The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) Cloud Computing Compliance Controls Catalogue. (https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html) |
| **CCM** | Cloud Security Alliance Cloud Controls Matrix, a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance stated domains[1]. (https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview) |

[1] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, https://cloudsecurityalliance.org/download/security-guidance-for-critical-areas-of-focus-in-cloud-computing-v3/

| Abbreviation | Description |
|---|---|
| **CPA** | Certified Public Accountant (CPA) is the title of qualified accountants in numerous countries in the English-speaking world. A CPA is an accountant who has satisfied the educational, experience and examination requirements of his or her jurisdiction necessary to be certified as a public accountant. CPAs audit financial statements of both publicly and privately held companies. They serve as consultants in many areas, including tax, accounting, and financial planning. They are well-respected strategic business advisors and decision makers. CPAs work for public accounting firms — small, medium and large; and for companies in business and industry. Their roles range from accountants to Controllers, to Chief Financial Officers for Fortune 500 companies, and advisors to small neighborhood businesses. |
| **CSA** | Cloud Security Alliance (https://cloudsecurityalliance.org/) |
| **CSIRT** | Computer Security Incident Response Team, a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. (http://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?) |
| **D1.3** | EU-SEC deliverable of task 1.2 "Auditing and assessment requirements" |
| **DPA** | Data Protection Authority as defined in General Data Protection Regulation EU (2016/679) |
| **DPIA or PIA** | "Data Protection Impact Assessment" (DPIA) or "Privacy Impact Assessment" (PIA) - the process for building and demonstrating compliance. |
| **EU-SEC** | European Security Certification Framework (http://www.sec-cert.eu/) |
| **GDPR** | General Data Protection Regulation EU (2016/679) (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) |
| **IIA** | The Institute of Internal Auditors, an internal audit and risk management guidance-setting body. (https://na.theiia.org/about-us/Pages/About-The-Institute-of-Internal-Auditors.aspx) |

| Abbreviation | Description |
|---|---|
| **ISAE** | Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000) describes general requirements for the qualification and conduct of an auditor (e. g. professional judgment and skepticism) as well as for accepting, planning and carrying out an audit engagement i.e. it is a high-level auditing standard which provides the required high-level framework. |
| **ISMS** | Information Security Management System (See Terminology and Definitions – Management System) |
| **ISO** | International Organization for Standardization (https://www.iso.org/home.html) |
| **ISO/IEC 17021** | ISO/IEC 17021-1:2015 Requirements for bodies providing audit and certification of management systems (https://www.https://www.iso.org/standard/61651.html.org/standard/61651.html) |
| **ITRM** | The IT risk management (ITRM) (market) is a part of the growing category of integrated risk management (IRM) solutions. Through common functions, such as an asset inventory, requirements mapping, survey capabilities, workflow functions and data import, IRM automation addresses multiple segments. Within its coverage, Gartner has defined seven primary IRMS segments:<br>• Operational risk management (ORM)<br>• IT risk management<br>• Business continuity management (BCM) planning<br>• IT vendor risk management (VRM)<br>• Corporate compliance and oversight (CCO)<br>• Audit management (AM)<br>• Enterprise legal management (ELM) |
| **ISO/IEC 17024** | ISO/IEC 17024:2012 General requirements for bodies operating certification of persons (https://www.iso.org/standard/52993.html) |
| **ISO/IEC 19011** | ISO/IEC 19011:2011 Guidelines for auditing management systems (https://www.iso.org/standard/50675.html) |

| Abbreviation | Description |
|---|---|
| **ISO/IEC 27001** | ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements (https://www.iso.org/isoiec-27001-information-security.html) |
| **ISO/IEC 27006** | ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems (https://www.iso.org/standard/62313.html) |
| **ISO/IEC 27007** | ISO/IEC 27007:2011 Guidelines for information security management systems auditing (https://www.iso.org/standard/42506.html) |
| **MFSR** | Ministry of Finance of the Slovak Republic (http://www.finance.gov.sk/en/) |
| **SECNUMCLOUD** | Requirements Framework for Cloud Service Providers published by Agence nationale de la sécurité des systèmes d'information (eng. National Cybersecurity Agency of France) (https://www.ssi.gouv.fr/en/) (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.0_niveau_essentiel.pdf) |
| **SIA** | Slovenian Institute of Auditors (http://www.si-revizija.si/) |
| **SIEM** | Security information and event management products and/or services, which produce an operational view to information security status, enhancing log management and combining it with security event monitoring to enable centralized reporting (https://www.nixu.com/en/service/security-information-and-event-management-siem) |
| **SI-MPA** | Slovenian Ministry of Public Administration (http://www.mju.gov.si/en/) |
| **SOC 2** | Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (https://www.ssae-16.com/soc-2/) |
| **WP29** | The Article 29 Working Party (Art. 29 WP) is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. (https://en.wikipedia.org/wiki/Article_29_Data_Protection_Working_Party) |

# TABLE OF CONTENTS

## LIST OF TABLES



## LIST OF FIGURES

# TERMINOLOGY AND DEFINITIONS

*Table 2. Terms and definitions.*

| Term | Definition | Source |
|---|---|---|
| Accreditation | Accreditation assures users of the competence and impartiality of the body accredited. | http://www.iaf.nu/ |
| Assessment | Refers in this document to risk assessment, which overall process of *risk identification [ISO Guide 73:2009, definition 3.5.1], risk analysis [ISO Guide 73:2009, definition 3.6.1]* and *risk evaluation [ISO Guide 73:2009, definition 3.7.1].* | ISO Guide 73:2009, definition 3.4.1 |
| Attestation | An issue of a statement that conveys the assurance that the specified requirements have been fulfilled. Such an assurance does not, of itself, afford contractual or other legal guarantees. | ISO 17000:2004, 5.2 |
| Audit | Systematic, independent and documented process for obtaining *audit evidence* and evaluating it objectively to determine the extent to which the *audit criteria* are fulfilled | ISO/IEC 19011:2011, 3.1 |
| Audit conclusion | Outcome of an audit, after consideration of the audit objectives and the audit findings. | ISO 9000:2005, definition 3.9.5 |
| Audit criteria | Set of policies, procedures or requirements used as a reference against which *audit evidence* is compared | ISO/IEC 19011:2011, 3.2 |
| Audit evidence | Records, statements of fact or other information which are relevant to the *audit criteria* and verifiable. | ISO 9000:2005, definition 3.9.4 |
| Audit programme | Arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose. | ISO 9000:2005, definition 3.9.2 |
| Audit scope | Extent and boundaries of an audit | ISO 9000:2005, definition 3.9.12 |
| Auditee | Organization being audited. | ISO 9000:2005, definition 3.9.8 |
| Auditor | Person who conducts an audit. | ISO/IEC 19011:2011, definition 3.8 |
| Certification | The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements. | https://www.iso.org/certification.html |
| Competence | Ability to apply knowledge and skills to achieve intended results. | ISO/IEC 19011:2011, definition 3.17 |

| Term | Definition | Source |
|---|---|---|
| Conformity | Fulfilment of a requirement | ISO 9000:2005, definition 3.6.1 |
| Conformity Assessment | Conformity assessment involves a set of processes that a product, service or system meets the requirements of a standard. | https://www.iso.org/conformity-assessment.html |
| Continuous Auditing | An ongoing assessment process that aims to determine the fulfillment of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), conducted at a frequency requested by the purpose of audit. | EU-SEC D1.4 |
| Continuous Certification | An information system is said to be the state of continuous certification if it meets a predefined set of Service Qualitative Objectives (SQOs) and Service Level Objectives (SLOs), which have been verified through continuous auditing. | EU-SEC D1.4 |
| Information Security | Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.<br>Note: The terms “continuous” and “ongoing” in this context mean that security and privacy controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. | NIST SP 800-57 |
| Management system | System to establish policy and objectives to achieve those policies. | ISO 9000:2005, definition 3.2.2 |
| Nonconformity | Non-fulfilment of a requirement | ISO 9000:2005, definition 3.6.2 |
| Risk | Effect of uncertainty on objects | ISO Guide 73:2009, definition 3.9.2 |

# 1 INTRODUCTION

The European Security Certification Framework (EU-SEC) project strives to address the security, privacy and transparency challenges associated with the greater externalization of IT to Cloud services.

EU-SEC will create a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, privacy, governance, risks management and compliance in the Cloud. It will be tested and validated in pilots involving industrial partners.

This deliverable is part of work package 1 (WP1) with its main task to collect requirements for the design of efficient and effective security certification methods. Four different categories of requirements will be elicited:

1. Information security and privacy requirements,
2. Auditing requirements
3. Mutual / Multi party recognition requirements,
4. Continuous monitoring-based certification requirements.

This collection will result in a set of harmonized requirements.

## 1.1 OBJECTIVES AND SCOPE

This deliverable D1.3 Auditing and assessment requirements addresses objective 2 of the work package 1 (WP1) that has been defined in *EU-SEC project* as:

> *"Objective 2: Auditing requirements:*
>
> *These are requirements associated with auditing procedure, as the rules that tell you how an auditor should be executing an assessment and how the results should be reported. These requirements will be mainly collected from ISO/IEC 19011, ISO/IEC 27007, SOC 2 / ISAE 3402."*

## 1.2 WORK PACKAGE DEPENDENCIES

The requirements coming from standards and national legislation from the public sector and banking sector pilots are captured, analyzed and will be used in the EU-SEC framework and the pilots.

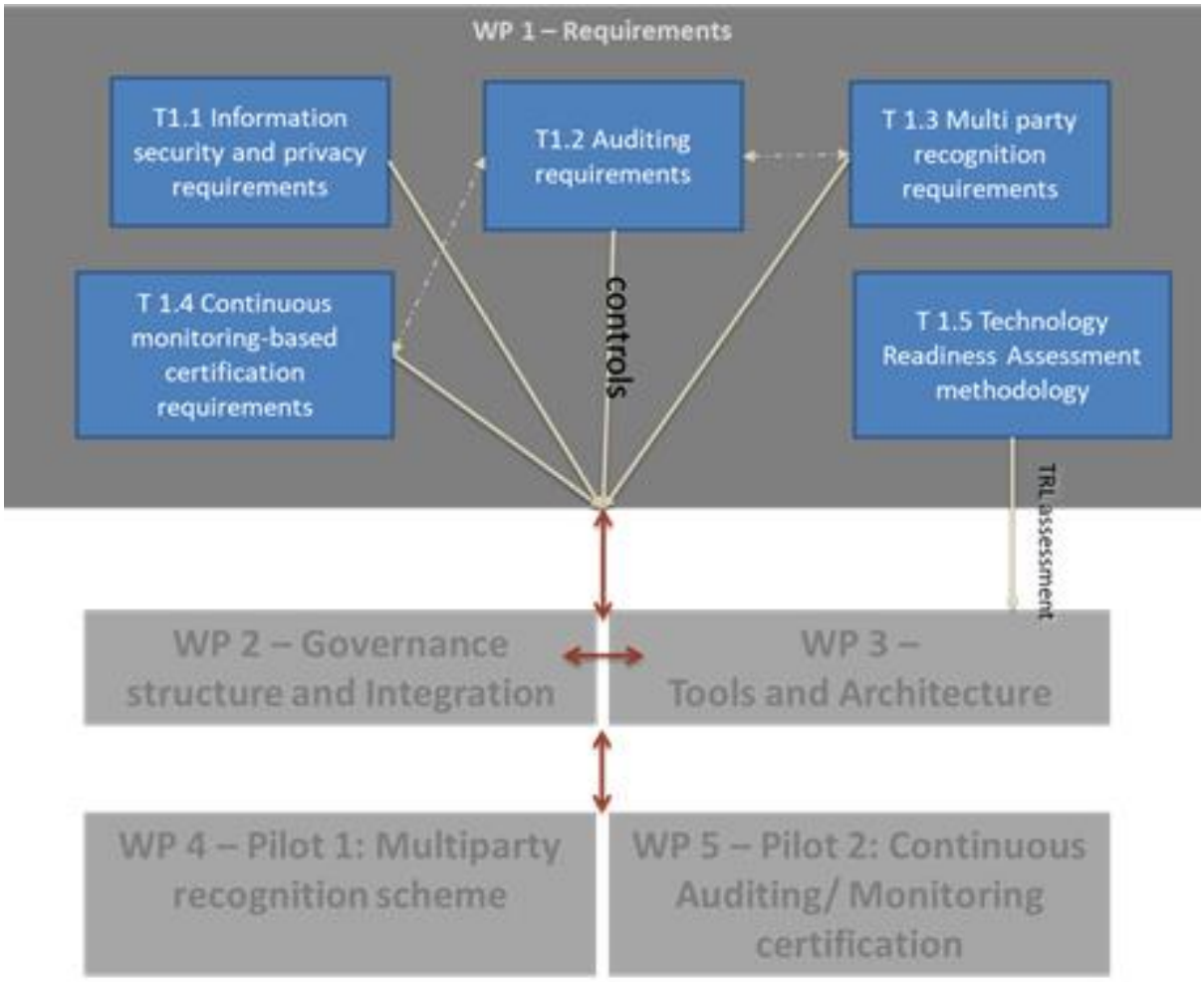



*Figure 1. Work package dependencies.*

# 2 PROJECT TASK OVERVIEW

## 2.1 METHODOLOGY

This deliverable collects requirements related to the execution of and reporting about an audit or assessment. The deliverable mainly focuses on the auditing requirements related to third-party-assessment-based certification, other important aspects that will be considered are the requirements itself. This deliverable also looks into the concept of "acceptable evidence" and will address the question on "what is meant to be considered as an acceptable evidence during an evaluation?"

The sources of guidelines, standards and normative references to be analyzed, have been selected for their applicability in Information Security Management Systems specifically. While there are hundreds of standards that can be used as cloud security controls, the standards here have been chosen for their holistic approach on information security. The standards within the scope of this study have been chosen for their global applicability and high-level strategic approach and have well-documented auditing and assessment requirements in place to provide a solid baseline for the requirements collection for this study.

The audit and assessment requirements are analyzed from perspective of:

- Bodies setting the requirements a cloud service must fulfil
- Auditors performing an independent assessment of standard cloud controls design and operation, compliance with national, standard and industry requirements.


*Figure 2. From multiple requirements to standard cloud controls.*

Specifically, the analysis is performed against established General Requirements For audit process defined in chapter 3.2.2. The outcome of this report may help to develop data architecture and tooling to support the audit and assessment process itself and more broadly, the design of efficient and effective security certification method.

## 2.2 AUDIT AND ASSESSMENT REQUIREMENT SOURCES IN SCOPE

Based on the methodology the following families of standards, normative and informative guidelines have been included for this study:

- ISO standards for auditing management systems (ISO/IEC 17021 and ISO/IEC 19011)
- ISO standards for auditing information security management systems (ISO/IEC 27006 and ISO/IEC 27007)
- International Auditing and Assurance Standards Board proposed International Standards for Assurance Engagements ISAE 3000 and ISAE 3402

Other sources for guidelines that have been reviewed, are:

- SOC 2 for Service Organizations: Trust Services Criteria - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

- Bundesamt für Sicherheit in der Informationstechnik (eng. German Federal Office for Information Security) Cloud Computing Compliance Controls Catalogue (BSI C5)
- SecNumCloud issued by Agence nationale de la sécurité des systèmes d'information (eng. National Cybersecurity Agency of France)
- Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR) Certification
- Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR) Attestation
- Audit and assessment requirements for the public procurement of government cloud services in Slovakia and Slovenia

The following subchapters describe each of these in more detail.

### *2.2.1 ISO STANDARDS*

ISO standard approach is that there is a set of standards for auditing Management Systems in general and then a particular applied set of standards for auditing Information Security Management Systems. The latter set refers to the former and requires having both sets at hand.

ISO/IEC 17021 sets requirements for bodies providing audit and certification of management systems. It covers principles (s.a. impartiality, competence, responsibility, openness, responsiveness to complaints), general requirements, structural requirements, resource requirements, information requirements, process requirements and management system requirements set to the auditing body.

ISO/IEC 27006 sets Requirements for bodies providing audit and certification of information security management systems and covers all particulars to be amended to ISO/IEC 17021 for the application to information security management systems.

ISO/IEC 19011 titled as "Guidelines for auditing management systems" provides guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits, as well as guidance on the evaluation of competence of individuals involved in the audit process, including the person managing the audit programme, auditors and audit teams. It is applicable to all organizations that need to conduct internal or external audits of management systems or manage an audit programme. The application of ISO/IEC 19011 to other types of audits is possible, provided that special consideration is given to the specific competence needed. This standard applies to the practitioners of the audit i.e. the individual auditors.

ISO/IEC 27007 titled as "Guidelines for information security management systems auditing" supplements the guidance included in ISO/IEC 19011 by providing guidance specific to managing an information security management system (ISMS) audit programme, on conducting the audits, and on the competence of ISMS auditors. This standard is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme. In particular the audit criteria must comply with ISO/IEC 27001.

### *2.2.2 ISAE STANDARDS*

Assurance Engagements Other than Audits or Reviews of Historical Financial Information (ISAE 3000) describes general requirements for the qualification and conduct of an auditor (e. g. professional judgment and skepticism) as well as for accepting, planning and carrying out an audit engagement i.e. it is a high-level auditing standard which provides the required high-level framework. Furthermore, the standard, which was issued by the International Auditing and Assurance Standards Board (IAASB), includes general requirements for audit criteria without specifying their content in more detail. The standard distinguishes between audits with "reasonable assurance" and audits with "limited assurance" and so-called "attestation engagements" are distinguished from so-called "direct engagements". ISAE 3000 addresses a number of important issues relating to practitioner (auditor) and subject of assurance (auditee) that are the code of conduct for external assurance on non-financial information.

ISAE 3000 is supported by the International Framework Ethics for Assurance Engagements (the IAASB Framework), which defines Professional Accountants and describes the elements and objectives of an assurance engagement and auditor firm thereof. The standard covers all aspects of an assurance engagement, including engagement acceptance, agreeing the terms of engagement, planning and performing the engagement, using the work of experts, obtaining evidence, considering subsequent events, documentation and preparing the external assurance report.

Assurance Reports on Controls at a Service Organization (ISAE 3402) was developed to provide an international assurance standard for allowing certified public accountants (CPAs) to issue a report for use by customer organizations and their auditors (customer auditors) on the controls at a cloud service provider that are likely to impact or be a part of the customer organization's system of internal control over financial reporting. The auditor shall not represent compliance with ISAE 3402 unless the auditor has complied with the requirements of ISAE 3000 as well.

Similar to ISAE 3000, ISAE 3402 states that an assurance engagement may be a "reasonable assurance" engagement or a "limited assurance" engagement; that an assurance engagement

may be either an "assertion-based" engagement or a "direct reporting" engagement; and, that the assurance conclusion for an assertion based engagement can be worded either in terms of the responsible party's assertion or directly in terms of the subject matter and the criteria. ISAE 3402, however, only deals with assertion-based engagements that convey reasonable assurance, with the assurance conclusion worded directly in terms of the subject matter and the criteria. It applies only when the cloud service provider is responsible for, or otherwise able to make an assertion about, the suitable design of controls.

Furthermore, the standard defines the guidelines concerning following themes:

- Ethical Requirements
- Management and Those Charged with Governance
- Acceptance and Continuance
- Assessing the Suitability of the Criteria
- Materiality
- Obtaining an Understanding of the Service Organization's System
- Obtaining Evidence Regarding the Description
- Obtaining Evidence Regarding Design of Controls
- Obtaining Evidence Regarding Operating Effectiveness of Controls
- The Work of an Internal Audit Function
- Subsequent Events
- Documentation
- Preparing the Service Auditor's Assurance Report

It should be noted that ISAE standards do not explicitly apply to information security management.

### *2.2.3 SOC 2*

Service Organization Control type 2 (SOC 2) reports, according to the specifications of the AICPA (American Institute of Certified Public Accountants), serve the purpose to understand the cloud service provider's internal control system with regard to each of the five pillars: security, availability, processing integrity, confidentiality and privacy. This information is necessary for cloud service customers own risk management, for example. Demand for SOC 2 reports is not typically coming from the cloud service customers' accounting or finance organizations or the auditors. Instead, demand is mainly driven by the cloud service customers' technology, risk management, operations and line-of-business organizations.

The Trust Services Criteria (updated in 2016) are classified into the following Trust Services Categories:

*Table 3. The Categories of Trust Services Criteria.*

| Category | Description |
|---|---|
| **Security** | The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements. |
| **Availability** | Information and systems are available for operation and use to meet the entity's objectives. |
| **Processing integrity** | System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives. |
| **Confidentiality** | Information designated as confidential is protected to meet the entity's objectives. |
| **Privacy** | Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives. |

Furthermore, the Trust Services Criteria are aligned to the 17 criteria (formerly known as principles) presented in "Internal Control — Integrated Framework", issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In addition to the 17 criteria, the Trust Services Criteria include additional criteria supplementing COSO principle 12: "The entity deploys control activities through policies that establish what is expected and procedures that put policies into action" (supplemental criteria). The supplemental criteria, which apply to the achievement of the entity's objectives relevant to the engagement, are organized as follows:

- Criteria applicable to all five of the Trust Service Categories, including supplemental criteria for:
  - Logical and physical access controls;
  - System operations;
  - Change management;
  - Risk mitigation; and
- Additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

For the security category, the common criteria constitute the complete set of criteria. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of

criteria consists of the common criteria and the criteria applicable to the specific trust services categories.

It is common practice for service organizations report on one or two Trust Services Principles in their first SOC 2 report – namely, Security and one other category, if required. This enables service organizations to strengthen their maturity in other areas so as to better position themselves to increase the scope of their reports in future audit periods, if necessary. The decision to add additional categories results from explicit requests received from user entities, or from changes in business risks, or from changes in the service organization's products and services.

### *2.2.4 BSI C5*

The objective of the C5 is to provide customers with better insights into a higher level of security and avoiding redundant audits. In a comprehensive catalogue which is publically available, the C5 provides a set of generally recognized requirements for secure cloud computing. Mainly, these were selected from established security standards and specified in more detail, where necessary. The C5 is designed to be suitable for an audit by a public accountant. The assurance engagement including the reporting shall be executed in accordance with the ISAE 3000 and based on the requirements (Criteria) as set forth in C5.

*Being subdivided into 17 sections (control areas), the C5 covers the entire spectrum of information technology (see Table 4). For each section, an objective is defined providing the cloud provider with a summarized target. The section-specific Criteria operationalize this objective and are to be fulfilled by controls. Table 4. The sections and objectives of BSI C5.*

| Section | Objective |
|---|---|
| **Organization of information security** | Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organization. |
| **Security policies and work instructions** | Providing policies and instructions with respect to the security claim and to support the business requirements. |
| **Personnel** | Making sure that employees, service providers and suppliers understand their tasks, are aware of their responsibility with regard to information security and that the assets of the organization are protected if the tasks are modified or completed. |

| Section | Objective |
|---|---|
| **Asset management** | Identifying the organization's own assets and responsible persons as well as ensuring an appropriate level of protection. |
| **Physical security** | Preventing unauthorized physical access and protection against theft, damage, loss and failure of operations. |
| **Safeguards for regular operations** | Assuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors. |
| **Identity and access management** | Securing the authorization and authentication of users of the cloud service provider (usually privileged user) and the cloud service customer in order to prevent unauthorized access. |
| **Cryptography and key management** | Using appropriate and effective cryptography in order to safeguard information security. |
| **Communication security** | Protecting information in networks and the corresponding information-processing systems. |
| **Portability and interoperability** | Providing the ability to securely operate the service on different IT platforms as well as the possibility of secure connections to different IT platforms and termination of the service |
| **Procurement, development and maintenance of information systems** | Complying with the security targets in case of new developments and procurement of information systems as well as changes. |
| **Control and monitoring of service providers and suppliers** | Protecting information that can be accessed by service providers and/or suppliers of the cloud service provider (subcontractors) and monitoring the services and security requirements agreed upon. |
| **Security incident management** | Assuring a consistent and comprehensive approach regarding the monitoring, recording, assessment, communication and escalation of security incidents. |
| **Business continuity management** | Strategic establishment and governance of a business continuity management (BCM). Planning, implementing and testing business continuity concepts as well as incorporating safeguards in order to ensure and maintain continuous operations. |

| Section | Objective |
|---|---|
| **Security check and verification** | Checking and verifying that the information security safeguards are implemented and carried out in accordance with the organization-wide policies and instructions. |
| **Compliance and data protection** | Preventing violations against statutory or contractual duties with respect to information security. |
| **Mobile device management** | Guaranteeing secure access to IT systems via mobile devices in the cloud service provider's responsibility to develop and operate the cloud service. |

Individual requirements are assigned to each section. The requirements specify general principles, procedures and measures for fulfilling the assigned objective. In this respect, a distinction is made between basic requirements and additional, optional requirements. The basic requirements are essential and the cloud service provider has to meet and at least comply with them. The cloud service customer can decide whether the basic requirements are sufficient or additional, optional requirements have to be met.

The subject of the audit includes the following two areas:

- The description of the internal control system related to the cloud services (system description) and
- The controls presented in the system description with reference to the individual requirements of the cloud service provider.

For a BSI C5 assurance report issued by a public accountant, a distinction is made between two types of audits and reporting:

- Type 1: The auditor has to assess whether the system description properly reflects the actual design and implementation of the internal control system related to the cloud services at the time of the audit and whether the controls presented have been designed appropriately.
- Type 2: As compared to type 1, the auditor performs additional audit activities with respect to the operating effectiveness of the controls (functional tests).

### *2.2.5 MINISTRY OF FINANCE OF THE SLOVAK REPUBLIC*

Ministry of Finance of the Slovak Republic acts as the Central Harmonization Unit for Public Internal Control. The quality and security of all cloud services must be audited by an

independent accredited auditor company prior purchase and integration to the government cloud. This is also required by regulation: ICT services must be technically tested prior integration to the government cloud. MFSR only requires an independent audit but does not set particular requirements to the auditing body or methodology.

### *CENTRAL CONTROL BODIES WITHIN THE SLOVAK REPUBLIC IN STATE ADMINISTRATION BODIES*

In accordance with the public interest in enhancing the efficiency, effectiveness and economic efficiency of public administration, a system of financial control is built up to ensure sufficient and effective control of the management not only of the state budget but also of the state property management through the Act no.357/2015 Coll. on Financial control and audit. Financial control in the Slovak Republic is currently divided into basic financial control (ex-ante control), administrative financial control (if the public administration provides or provided funds to legal or natural persons) and financial control on the spot (it is optional and evidence and facts can be verified on the spot).

Act no. 357/2015 Coll. on Financial control and audit further strengthened the internal auditor's independent status, increased the requirements for his expertise, increasing qualifications, while the existing current regulation no longer allows for the exemption from the provisions of the Internal Audit Service. Several principles of the COSO system and international auditing standards for the professional practice of internal auditors have been incorporated into the law.

**The Ministry of Finance of the Slovak Republic** and **The Government Audit Office** pursuant to Act no.357/2015 Coll. on Financial control and audit performs government audit and evaluates the quality of financial control exercises in public administration bodies. Government audit objectives are, for example:

- setting up financial management and internal control systems,
- management of funds, property and receivables,
- management of EU funds,
- compliance with obligations under generally binding legislation.

The Ministry of Finance of the Slovak Republic and The Government Audit Office within the government audit performance, as well as the internal audit of the administrator of the chapter of the state budget, are in addition to the objectives focused on economy, asset management, financial operations, etc. authorized to carry out an audit of information systems, i.e. verify and

evaluate the security and functionality of the information systems, the adequacy and completeness of the information contained in the information system.

**The Supreme Audit Office of the Slovak Republic**, as an independent state body for controlling the management of state budget funds, including the funds of the European Union and other funds from abroad provided for financing projects under international treaties, as well as controlling the management of assets to the extent stipulated by Act no. 39/1993 Coll. on the Supreme Audit Office of the Slovak Republic performs audit and control under INTOSAI international auditing standards.

**The Office of the Government of the Slovak Republic**, which at the governmental level performs control over fulfillment of the tasks related to the performance of the state administration, control of fulfillment of tasks from the resolution of the Government of the SR, control of the efficiency of the state administration and control of petitions and complaints pursuant to Act no. 10/1996 Coll. on Control in the State Administration, as amended.

*INTERNAL CONTROL BODIES IN STATE ADMINISTRATION BODIES*

In addition to the above-mentioned Central Audit Authorities, administrators of budget chapters control the management of budget appropriations of the budget chapter, for the control of the management of the budgets of the central authorities and the state funds is the responsibility of the competent minister or the head of the central body. These inspections have the character of an internal control and are part of the internal control system of the state administration body established under § 7 of Act no. 10/1996 Coll.

This system consists of the control activity of the heads of the state administration bodies, their senior staff, including professional and control departments focused on control of:

- fulfilling the tasks of state administration,
- handling petitions and complaints,
- compliance with generally binding legislation; and
- Measures issued on their basis and measures to remedy the deficiencies identified.

**Control of state administration in the specialized activities**

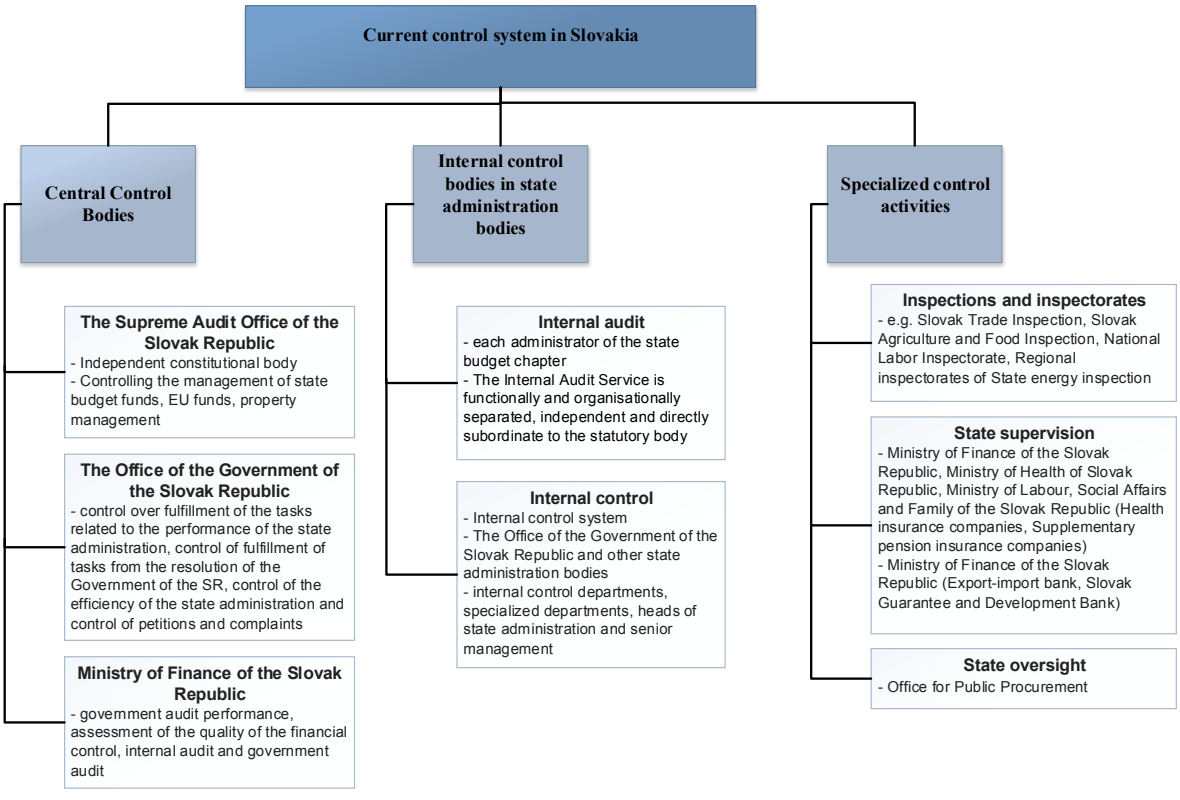
The control activity includes partially also the implementation of inspections by the inspection and supervisory bodies established by special acts in the area of state administration in specialized activities. This type of control also includes state supervision, which participate in the performance of the state administration with the control activity in the given area, defined by special laws.

**Audit of financial statements**

Independent auditing of public interest entities, accounting units that have statutory audit under the Act on Accounting, but also according to their own decision is governed by separate Act no 423/2015 Coll. on Statutory Audit. This Act transposes the Directive of the European Parliament and of the Council no. 2014/56 / EU amending Directive 2006/43 / EC on statutory audits of annual accounts and consolidated accounts and Regulation of the European Parliament and of the Council No. 537/2014 on specific requirements regarding the statutory audit of public interest entities and repealing Commission Decision 2005/909 / EC.

The Act regulates the status and activities of statutory auditors, audit firms, assistant statutory auditors, defines the statutory audit and the conditions under which it may be performed. It further regulates the work of the Slovak Chamber of Auditors, the Office for Supervision of Audit, as well as the scope of the Office for Supervision of Audit and its scope and the procedure for supervising statutory audit.

Statutory audit under this Act may be performed only by statutory auditors or audit firms registered in the Slovak Republic in the list of statutory auditors or the list of audit firms. All statutory audits performed under this Act are performed on the basis of the International Auditing Standards (ISA) issued by the IAASB.



### 2.2.6 SI-MPA – AUDITING SYSTEM IN SLOVENIA

Slovenian Ministry of Public Administration – SI-MPA - ensures that all services purchased by the administration have been audited for security using internationally recognized standards and applying them for case-by-case basis each time to cater the people, processes and technology concerned and to approve information systems supporting a specific working area / application. The Auditing Act (Official Gazette of the Republic of Slovenia, no. 65/08 and 63/13 - ZS-K) sets the basis of auditing in Slovenia. The expert areas related to auditing are:

- accounting,
- business finance,
- internal auditing,
- audit of information systems,
- tax examination and advice,
- valuation of companies, real estate and machines and equipment.

The auditing service my only be performed by an audit firm, and on behalf of the audit company only by persons authorized to carry out the tasks of a certified auditor who are in an employment relationship with an audit firm or have an agreement or agreement on business cooperation with an audit firm. The auditing process uses the hierarchy of the auditing rules, starting with the Auditing act, the international standards of auditing (IFAC - International Federation of Accountants), other legislation, basic audit principles, the code of professional ethics of external auditors and other rules, guidelines and good practice documents issued by the Slovenian Institute of Auditors (SIA, http://www.si-revizija.si/) or international organizations (IFAC, IAASB - International Auditing and Assurance Standards Board).

The SIA defines the auditing structure of information systems that is based on three levels of rules:

- First level includes the Auditing Act, other laws and regulations governing the auditing of information systems, international standards for auditing, control and assurance in the IT field (ITAF, ISACA - Information Technology Assurance Framework, Information Systems Audit and Control Association), and code of professional ethics of a certified information systems auditor
- Second level includes: international guidelines for auditing, control and assurance in the IT field, explanations and instructions from the Expert Council of the Slovenian Institute of Auditors

- Third level includes the methodological material manuals of the Slovenian Institute of Auditors, professional literature and published professional contributions, generally accepted principles for auditing information systems in foreign practice, and COBIT audit and assurance programs.

In accordance with the Slovenian Constitution the Court of Audit (http://www.rs-rs.si) of the Republic of Slovenia is the highest body for supervising state accounts, the state budget and all public spending in Slovenia. The Court of Audit performs the audit according to the laws (Court of Auditors Act and others) and international standards and guidelines (INTOSAI - International Organization of Supreme Audit Institutions, IFAC).

The Public Finance Act (Official Gazette of the Republic of Slovenia, No. 11/11 - official consolidated text, 14/13 - corr., 101/13, 55/15 - ZFisP and 96/15 - ZIPRS1617) defines the internal control of public finances for direct and indirect public budget users. The internal auditing ensures independent checking of financial management systems and controls, and advice the management to improve their efficiency. The internal audit is carried out by authorized (certified) internal auditors.

When the external audit firm (third party auditing) will perform the audit, the organizations of public administration must conclude a public procurement first to select the audit firm, before the audit process starts.

For the purpose of this deliverable, a general use case to audit an information system is used. In this case, the Auditing Act, the Hierarchy of the Rules for Auditing Information Systems and practice of the Slovenian Institute of Auditors (SIA) are used.

### *2.2.7 CSA STAR CERTIFICATION*

Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) Certification is a rigorous third-party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 information security management system standard together with the CSA Cloud Controls Matrix (CCM), a specified set of criteria that measures the capability levels of the cloud service.

The STAR Certification is based upon achieving ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix, that is, the controls set out in the CCM can be considered as additional controls in ISO 27001. To this end, no certificate for a CCM assessment is valid without an accompanying ISO 27001 certificate, with a scope that is equal to, or greater than, that of the STAR certification.

To be consistent with international standards, the STAR certification scheme is designed to comply with:

- ISO/IEC 17021:2011, Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ISO/IEC 27006:2011, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 19011, Guidelines for auditing management systems

A certification body conducting a CCM assessment must comply with ISO/IEC 27006. The requirements introduced hereby should be considered as supplemental to ISO/IEC 27006 and serve to outline the additional requirements for the assessment of the CCM.

**Audit Process and Requirements**

The CCM is audited against a management capability model, where a "Management Capability Score" is assigned to each of the control areas in the CCM (e.g., 16 controls areas for CCM v.3.0.1). This will indicate the capability of the management to ensure that each control is operating effectively in this area. Further guidance on how to audit using this model can be found at CSA's document "Auditing the Cloud Controls Matrix".

- Additional requirements with respect to the audits (e.g., duration, surveillance visits, etc.) and other parameters are as follows: Audit durations for conducting an ISO 27001 assessment combined with a CCM assessment will be a minimum of 1.5 times the duration required for an ISO 27001 assessment as defined in ISO/IEC 27006 (*Ref clause 9.1.3/9.1.4 ad Annex C in ISO/IEC 27006)*.
- There will be no reduction in the time that would usually be allocated to the assessment of ISO 27001 when conducting a combined ISO 27001 and CCM assessment. However, where there is overlap in the auditing requirements of ISO 27001 and the CCM, duplication of effort should be avoided. To make identifying areas of potential duplication easier, the corresponding areas of ISO 27001 have been referenced in the CCM.
- Sampling will be permitted in accordance with ISO 27001.
- A STAR certification certificate cannot be issued unless the organization has passed their ISO 27001 assessment.
- An assessment cycle will follow the assessment cycle for ISO 27001 (*Ref clause 9.2 /9.3 /9.4 in ISO/IEC 27006 )*
- For an organization simultaneously getting both ISO 27001 and STAR certification for the first time, there will be a two-part initial assessment covering all of the requirements

of ISO 27001 and the CCM followed by surveillance visits. Over a three-year period, the surveillance visits will cover the full range of ISO 27001 and the CCM. A recertification assessment will be conducted at the end of the cycle.

- For an organization adding STAR certification to an existing ISO 27001 certification, the full applicable control set will be audited on the first visit. This can be done on any type of visit provided that the time allocated to audit the CCM is an additional 50% of the time that would be required to conduct a recertification visit.

**Certification Body and Assessors Requirements**

A certification body conducting CCM assessments shall be accredited to ISO/IEC 27006 by an International Accreditation Forum (IAF) member accreditation body for delivery of ISO 27001 assessments. It shall comply with all the requirements of ISO/IEC 27006 as well as the requirements defined in the CSA document "Requirements for Bodies Providing STAR Certification".

With respect to auditors, the following requirements shall apply:

- All assessors must be able to present evidence of passing an accredited lead auditor course for ISO 27001 or be a qualified and experienced ISO 27001 assessor for an IAF member accredited ISO 27001 certification body (*Ref 7.2.1.3.1 c in ISO/IEC 27006)*.
- All assessors must have completed a BSI/CSA CCM course (*Ref 7.2.1.3.1 c* in 27006).
- All assessors must have a minimum of two years of experience working in information security (Ref 7.2.1.3.1 e in 27006).
- The 2 years' experience in information security is not necessary if the assessor has earned the CSA's Certificate in Cloud Security Knowledge (CCSK) or completed an alternative course that gives a similar level of knowledge in cloud computing or information security applications.

**Sufficient and Appropriate Evidence Requirements**

There must be reasonable evidence that a control has been in place and is effective. This would usually mean a control of some description would have been in place for three months. However, if evidence could be collected to demonstrate that the control was effective over a shorter period of time, this could be considered.

In some cases, a control may not be applicable and any exclusion of a control area must be properly justified as described in ISO 27001 (*Ref clause 4.2.1 g in ISO 27001*). Compensating controls are acceptable where one control in the CCM is rendered redundant by measures taken in other control areas.

**Reporting Requirements**

Following an assessment, an organization can choose to make their certification public on the STAR register. They can choose one of the following options:

- Disclose that they have been assessed against the CCM, but chose not to disclose any score
- Disclose a summary score, but not disclose the score for individual controls areas in the CCM
- Full disclosure of the scores for each control area

It will be the responsibility of the certification body to ascertain what level of disclosure the organization is prepared to make. Following the client's consent, certification bodies shall submit the scores to the CSA for listing on the CSA's STAR database through a mutually agreed data exchange program.

### *2.2.8 CSA STAR ATTESTATION*

Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix (CCM).

In fact, as a rigorous program based on the SOC 2 attestations standards or international equivalent (i.e. ISAE 3000), the STAR Attestation provides for robust reporting on the cloud service provider's description of its system and controls, including a description of the service auditor's tests of controls. The reports are intended to meet the needs of a broad range of users that need to understand cloud-specific control at a cloud service provider as it relates to security and the criteria in CCM. Similar to a traditional SOC 2 attestation there are two types of report:

- Type 1, report on management's description of a cloud service provider's system and the suitability of the design of controls ("point in time" assessment); and
- Type 2, report on management's description of a cloud service provider's system and the suitability of the design and operating effectiveness of controls ("over a period of time" assessment)

The Type 1 audit is used as a stepping stone to the more rigorous Type 2 audit. A CSA STAR Attestation Type 1 status demonstrates to cloud service customers the commitment to cloud

security through a thorough assessment of the policies and procedures in place to protect the Confidentiality, Integrity, and Availability of their data. A STAR Attestation obtained based on a SOC 2 Type 1 report is only valid for 6 months from the as-of date, i.e., an organization that received their STAR Attestation based on a SOC 2 Type 1 report is required to submit a SOC 2 Type 2 report to maintain uninterrupted STAR Attestation status. The validity period of a STAR Attestation is extended by grace period of 3 months on top of the basic validity period for report generation and delivery ("maximum validity period").

**Audit Process and Requirements**

Star Attestation is a SOC 2$^{SM}$ engagement that provides for rigorous third party independent assessments of cloud service providers, in which the criteria include:

- the applicable criteria in TSP section 100, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) (TSPC), and
- the control specifications included in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

In more detail, a SOC 2$^{SM}$ engagement is performed by a CPA in accordance with AT 101 and the AICPA Guide Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2$^{SM}$ Guide).

AT 101 provides a framework for performing and reporting on all attestation engagements. The SOC 2$^{SM}$ Guide provides performance and reporting guidance based on AT 101 for an examination of a cloud service organization's description of its system and the suitability of the design, and in type 2 engagements, the operating effectiveness of controls that are likely to be relevant to the security, availability, or processing integrity of a cloud service organization's system or the confidentiality or privacy of the information processed by the system. The TSPC provides criteria for evaluating and reporting on controls related to security, availability, processing integrity, confidentiality, and privacy.

SOC 2 reports are generally restricted use reports as they are intended for specified parties who are knowledgeable about the nature of the service provided by the service organization; how the service organization's system interacts with user entities, subservice organizations, and other parties; internal control and its limitations; the applicable trust services criteria, the risks that may prevent those criteria from being met, and how those controls address those risks; and complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria.

In addition, the CCM includes criteria that are equivalent to the criteria for the security principle in the TSPC plus certain additional criteria related to security.

**Certification Body and Assessors Requirements**

The STAR Attestation engagements must be performed by licensed CPAs. CPAs are governed by the rigorous requirements of the AICPA in addition to licensing requirements of their state of practice. The CSA's Certificate in Cloud Security Knowledge (CCSK) is an example of a very important component of the STAR Attestation Auditor's education.

Moreover, CPA services are subject to specific professional standards. Adherence to these standards is incumbent on CPAs under rules of the AICPA and individual state laws that have adopted these standards. For a greater overview over additional requirements with respect to related laws, ethics code, quality control policies and auditor required competencies, please refer to the CSA document "Guidelines for CPAs Providing CSA STAR Attestation".

**Reporting Requirements**

In a SOC 2$^{SM}$ report, the CPA expresses an opinion on the following:

- Whether the description of the cloud service organization's system is fairly presented, based on the description criteria
- Whether the controls are suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively.
- In type 2 reports, whether the controls were operating effectively to meet the applicable trust services and CCM criteria
- In engagements to report on the privacy principle, whether the service organization complied with the commitments in its statement of privacy practices.

Furthermore, the submission of information toward the completion of a STAR Attestation engagement will be determined by the management of the cloud service organization. In the spirit of transparency, CSA will explicitly note in the STAR Attestation entry if the engagement has been conducted by a CPA holding a CCSK certification or not. Because STAR Attestation does not require mandatory follow-up engagements, the "period of time" that the engagement covers, will be denoted on the STAR Registry along with the scope covered.

Further information about CSA guidelines regarding STAR Attestation is available at www.cloudsecurityalliance.org/star/attestation/.

### 2.2.9 SECNUMCLOUD

In this document we refer to Requirements Framework for cloud service Providers (SecNumCloud) "Essential" qualification level (formerly Secure Cloud). The provider must document and implement an audit program over three years defining the scope and frequency of audits in accordance with change management, policy, and the results of the risk assessment. The cloud service provider must engage with an Auditing provider of computer security [PASSI] qualified auditor firm to conduct annual audit. The audit plan must cover:

- Audit of the configuration of servers and network devices included in the scope of service. This audit is performed by sampling and should include all types of equipment and of servers in the service information system;
- The penetration test on external access to the service;
- If the service has internal development, auditing source code on the security features implemented

# 3 AUDIT AND ASSESSMENT REQUIREMENTS ANALYSIS

## 3.1 GENERAL AUDIT AND ASSESSMENT ENGAGEMENT

The attestation or assessment report is a conclusion of a journey of building cloud service provider's internal control environment to meet the requirements. Typically the journey starts with current state analysis, in which the current state of information security is evaluated and the observations are compared with the requirements, with ISO 27001 standard, for example. This is required in order to identify and prioritize key development needs, organized as designs of controls, and these are implemented and maintained by the IT operations, for example.

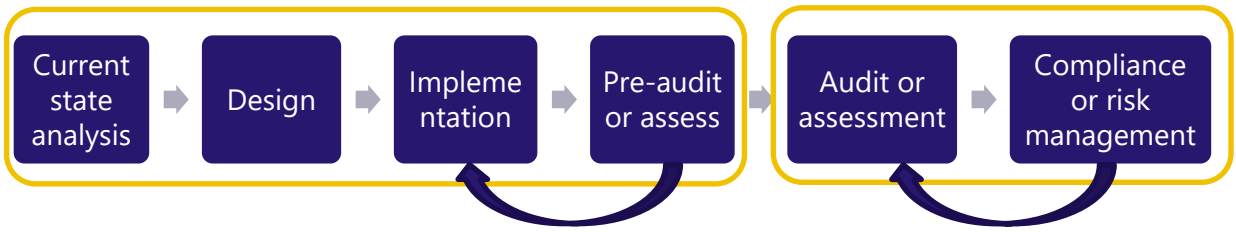



*Figure 3. General compliance service offering.*

Usually the biggest cloud service providers need to validate their compliance through an onsite assessment. Audit firms offer services, which are designed to be effective and to have as minimal effect on the cloud service providers everyday operations as possible, for example. The audit or assessment engagement outcome is a formal report on compliance or an attestation of compliance.

## 3.2 GENERAL REQUIREMENTS

### *3.2.1 FOR AUDITOR*

The requirements for an auditor, which audits a specific subset of information security management systems, viz. information security management systems of cloud service providers, can be based on ISO/IEC 27006 chapters from 4 to 7. For the audit and assessment services the following applies:

- The audit engagement must be led by ISO/IEC 27001 Lead Auditor or CPA and
- The auditors should have at least one of the following certificates:
    - Certificate of Cloud Security Knowledge (CCSK) by Cloud Security Alliance (CSA)
    - Certified STAR Auditor
    - Certified Cloud Security Professional (CCSP) certificate by (ISC)[2]
    - Other sufficient knowledge on cloud security, competence/qualification by professional judgement of certification body.
- General requirements: ISO/IEC 27006 chapter 5 requirements are applicable
- Structural requirements: ISO/IEC 27006 chapter 6 requirements are applicable
- Resource requirements: The requirements of ISO/IEC 27006 chapter 7 apply.

The figure below illustrates the aforementioned attributes of an auditor.

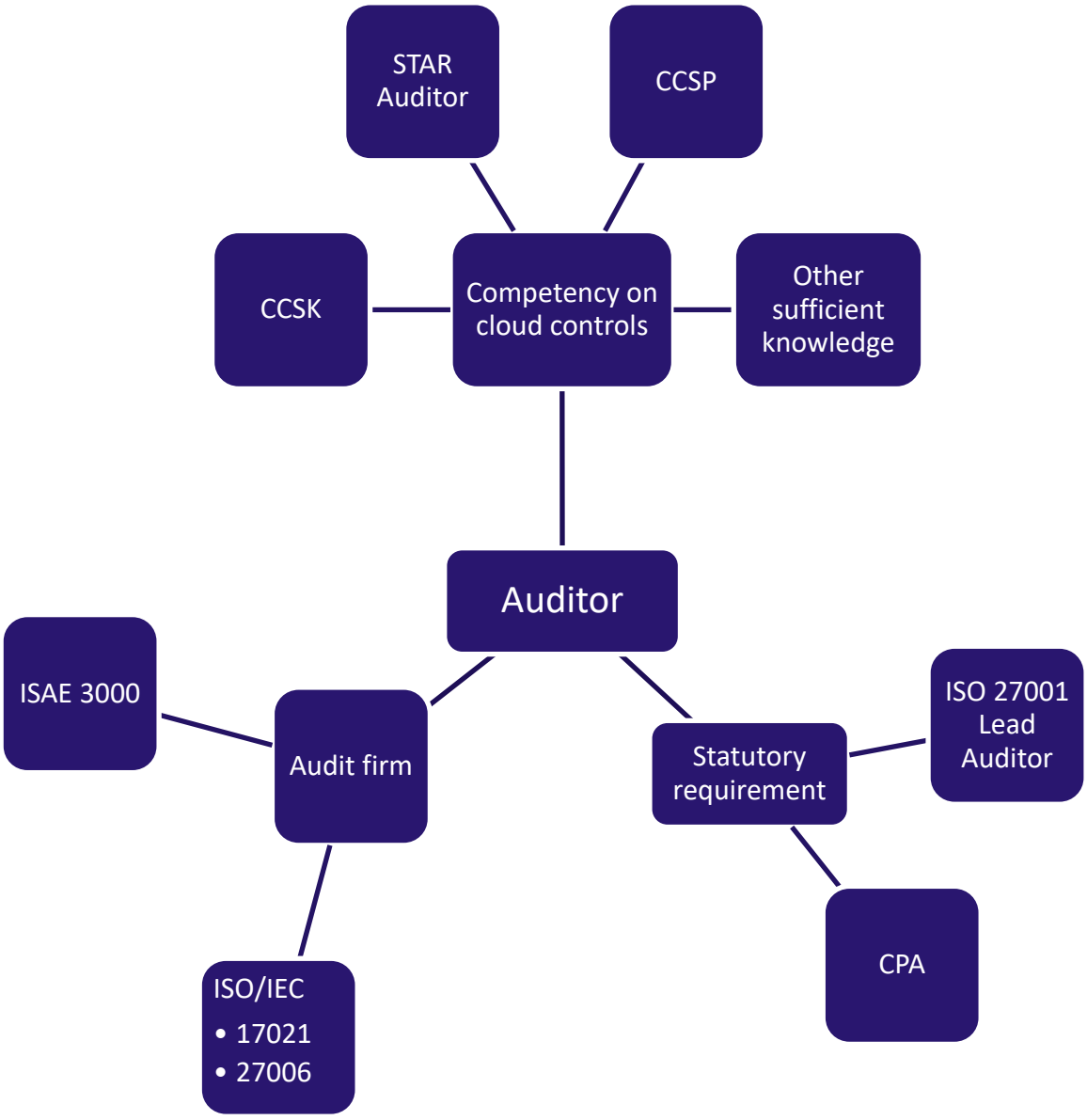



*Figure 4. The requirements for an auditor.*

The requirements for the auditor are based on ISO/IEC 27006 standard, which defines the requirements for bodies providing audit and certification of information security management systems. It should be noted that ISO/IEC 27006 is based on ISO/IEC 17021, to which information security management aspects are added.

The ISO/IEC 27006 as the baseline requirement for the auditor lies in the fact that among the assessed standards only ISO/IEC 27006 is targeted to auditors of information security management systems; the information security of a cloud service provider is built on the cloud service provider's information security management system. ISO/IEC 27006 defines the requirements for an auditor, which audits any information security management system.

### 3.2.2 FOR AUDIT PROCESS

The audit process for auditing a specific subset of information security managements systems, viz. information security management systems of cloud based service providers, can be based on the ISO/IEC 27007 chapter 6 (Performing an audit). This chapter relies heavily on ISO/IEC 19011 chapter 6 (Performing an audit).

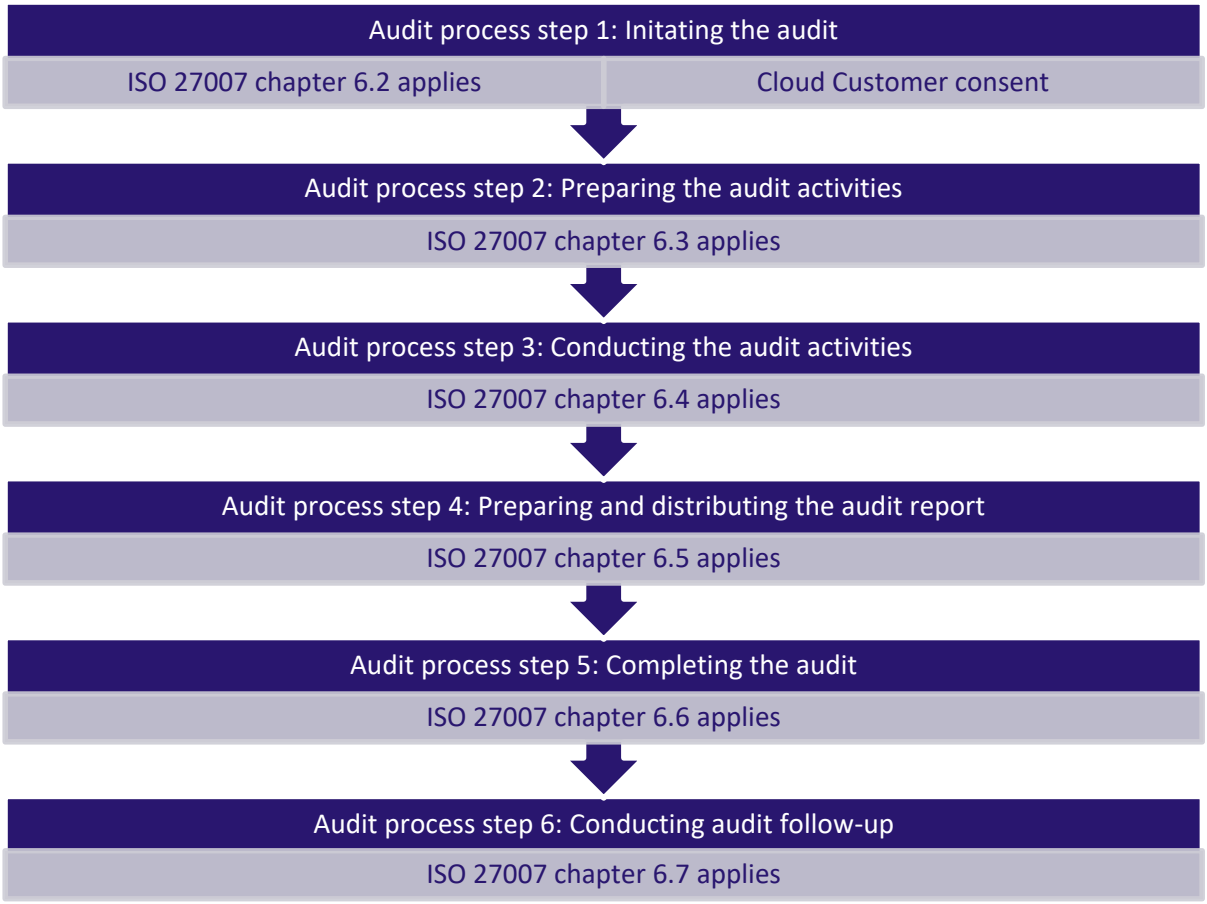



*Figure 5. Standard steps of an audit process with mapping to ISO/IEC 27007.*

For the assessment and audit of a specific subset of information security management systems of cloud service provider the following applies:

- Initiating the audit: ISO/IEC 27007 chapter 6.2 applies with the following addition:
  - To determine the feasibility of the audit, the auditee must have consent for the audit from auditee's customers. The consent can be either included in the contract or be a separately obtained consent.
- Preparing the audit activities: ISO/IEC 27007 chapter 6.3 applies.
- Conducting the audit activities: ISO/IEC 27007 chapter 6.4 applies.
- Preparing and distributing the audit report: ISO/IEC 27007 chapter 6.5 applies.

- Completing the audit: ISO/IEC 27007 chapter 6.6 applies.
- Conducting audit follow-up: ISO/IEC 27007 chapter 6.7 applies.

The aforementioned requirements are compliant with ISAE 3000 (see chapter 3.7). However a full alignment requires amending the audit process in steps 2 and 3: while ISO 27007 focuses on having the control in place, in terms of design and operation over one or more process cycles, ISAE 3000 requires the auditor to perform additional audit activities with respect to the operating effectiveness of the controls (functional tests), verifying the last 6 or 12 months of the control operation, for example. The figure below attempts to illustrate the audit engagement related attributes.

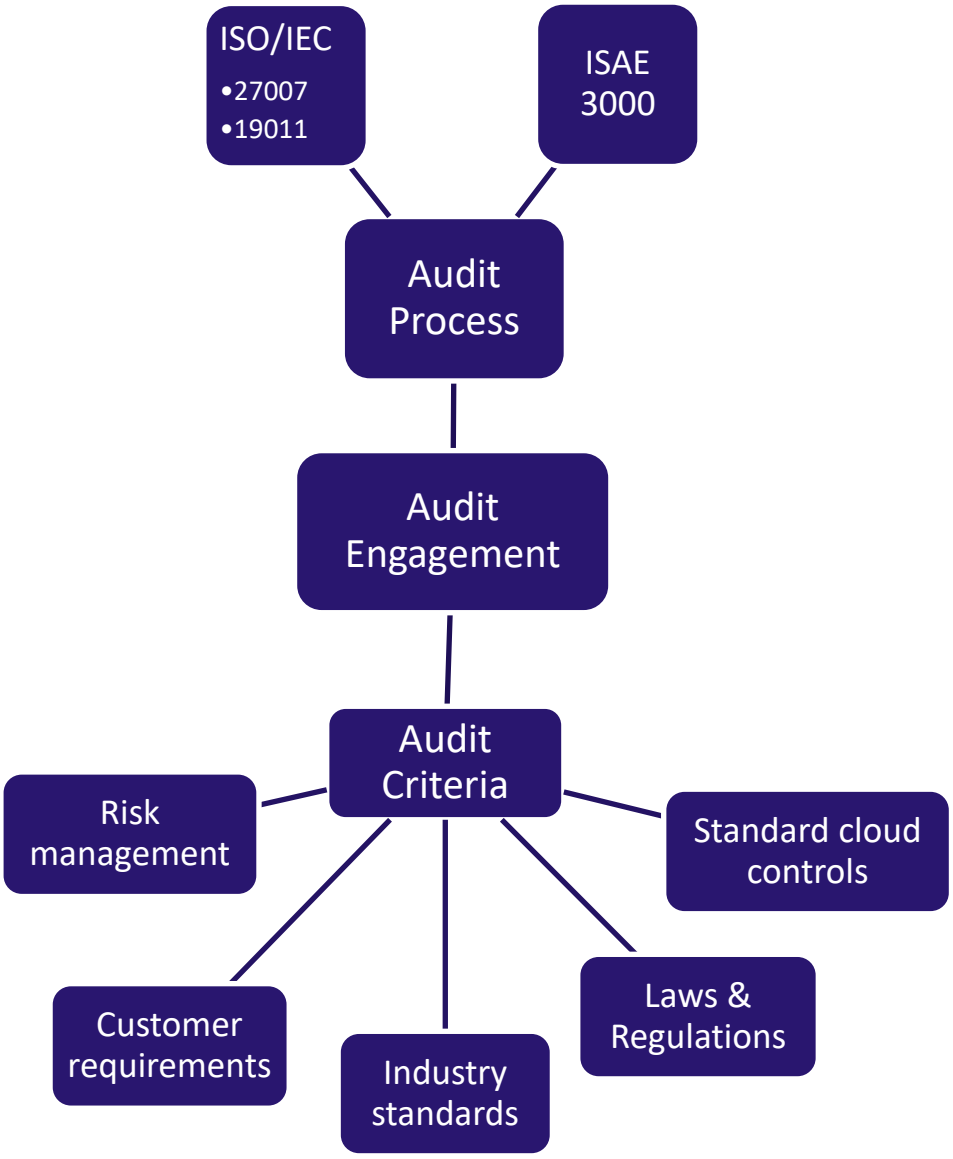



*Figure 6. Standard approach for auditing Information Security Management Systems.*

A cloud service provider seeking for multiple accreditations may not need to meet not one but several audit criteria, requiring several audit engagements respectively. Thus the "unit" cost of compliance per a control for the cloud service provider, can be high. If the cloud service provider is seeking for ISO/IEC 27001 certification, for example, this requires the internal control environment be structured according to ISO/IEC 27001 topics. While this is in good alignment with most audit criteria, SOC 2, BSI C5 and/or SecNumCloud, require new efforts to build the control environment according to these standards.

### *3.2.3 FOR AUDIT EFFORT*

The suggested audit effort should be calculated utilizing the guidance of ISO/IEC 27006 Annex C, which provides a procedure to determine audit time. For the first audit the adjustments for a cloud service Provider suggest a baseline of addition from 50% to 100% to the base table; the estimate is based on the following

- Many critical assets
- High amount of sensitive and confidential information
- Just established ISMS
- Complexity of IT


*Figure 7. Calculating suggested audit effort.*

### *3.2.4 FOR SUFFICIENT AND APPROPRIATE EVIDENCE*

The requirements for evidence quality and quantity for audits, which target a specific subset of information security management systems, viz. information security management systems of cloud service providers, are based on ISO/IEC 27007 Annex A.

As this annex is "... generic guidance on how to audit the ISMS processes, as required by ISO/IEC 27001, without regard to any specific ISMS requirements ..." and it provides the most comprehensive list of evidence items among the assessed standards, we take this as the

reference for collecting sufficient and appropriate evidence. For example, for the ISMS scope, policy and risk assessment approach, the annex groups the audit criteria, itemized list audit evidences and audit practice guide. While the annex is comprehensive, it is limited to non-technical controls and focuses mainly on information security management processes.

## 3.3 AUDITOR REQUIREMENTS COLLECTION

A cloud service customer relies upon the cloud service provider to support its one or more processes, and therefore an independent assessment is required to gain information on the cloud provider's capability to design, implement and operate information security safeguards for the cloud service. The cloud service must, for example, address numerous customer needs for risk control and compliance with various national, international and sector specific requirements.

Cloud service providers don't allow cloud service customers' auditors to interfere with their IT operations. Acceptable third parties, Independent Practitioners, are therefore required to perform the audit and assessment engagement on the design, implementation, operation and maintenance of safeguards.

The below tables collect requirements regarding the competence and statutory requirements of an auditor and requirements pertaining the auditor firm.

*Table 5. Competence requirements for an auditor.*

| Audit standard | Competency requirements | Ethical requirements | Competence maintenance |
|---|---|---|---|
| **ISO/IEC 27007** | The guidelines from ISO/IEC 19011:2011, Clause 7.2.3.2 apply.<br>(7.2.3.2 parts A.B.C etc.) | **7.2.2 Personal behavior**<br>"...Auditors should exhibit professional behavior during the performance of audit activities, including being:<br>—ethical, i.e. fair, truthful, sincere, honest and discreet;..."<br>"...—acting with fortitude, i.e. able to act responsibly and ethically, even though these actions may not always be popular and may sometimes result in disagreement or confrontation..." | ISO/IEC 19011:2011, 7.2 & 76 |

| Audit standard | Competency requirements | Ethical requirements | Competence maintenance |
|---|---|---|---|
| **ISAE 3000** | The engagement partner shall:<br>(a) Be a member of a firm that applies ISQC 1, or other professional requirements, or requirements in law or regulation, that are at least as demanding as ISQC 1; (Ref: Para. A60–A66)<br>(b) Have competence in assurance skills and techniques developed through extensive training and practical application; and (Ref: Para. A60)<br>(c) Have sufficient competence in the underlying subject matter and its measurement or evaluation to accept responsibility for the assurance conclusion. (Ref: Para. A67–A68) | 20. The practitioner shall comply with Parts A and B of the IESBA Code related to assurance engagements, or other professional requirements, or requirements imposed by law or regulation, that are at least as demanding. (Ref: Para. A30–A34, A60) | *ISQC1 1 - Relevant for the following texts:*<br>*ISQC 1: 9.*<br>-Introduction (ParaA30-A34)<br>-Quality Control (A60-66)<br>-Responsibilities of the Engagement Partner (A74)<br>-Firm Level Quality Control (3b, 31a)<br>-Engagement Quality Control - Review (Ref: Para. 36(b)): |
| **SOC 2** | The service auditor should have adequate training, proficiency, knowledge and experience to perform a SOC 2 engagement. The service auditor must be independent in mental attitude in all matters relating to the engagement. Note: The service auditor need not be independent of the users of the service organization. | See ISAE 3000 | Not defined |

| Audit standard | Competency requirements | Ethical requirements | Competence maintenance |
|---|---|---|---|
| **BSI C5** | According to the BSI's professional point of view, the assessment of C5 puts special demands on the qualification of the auditor due to the technical nature of the associated requirements. In addition to the general requirements for the auditor associated with the application of ISAE 3000 (Revised), the following supplementary requirements are imposed on the auditor respectively the audit team. At least half of the members of the audit team has more than 3 years of professional experience in accounting (auditing) and, in addition to this, at least one of the following professional examinations/certifications:<br>ISACA – CISA/ CISM/ CRISC<br>ISO/ IEC 27001 Lead auditor<br>CSA - CCSK<br>$(ISC)^2$ - CSSP | See ISAE 3000 | Not defined |

| Audit standard | Competency requirements | Ethical requirements | Competence maintenance |
|---|---|---|---|
| **SecNumCloud** | A qualification body has to have documented compliance with the Requirements Repository for Systems Security Audit Providers of information.<br>(Ref. 1.3.2) | The provider must have a built-in ethical charter rules.<br>(Ref. 7.2) | Not defined |
| **MFSR** | Certification scheme requirement. | Certification scheme requirement. | As per the certification scheme requirement. |
| **SI-MPA** | The audit company itself and the auditor must present the appropriate certifications and experience.<br>Auditing Act: SIA determines the expertise and experience needed to acquire the professional titles in auditing. SIA also organizes professional training, conducts tests of professional knowledge and issues a certificate of professional skills for obtaining professional titles in auditing. | As per ISO 19k standard.<br>SIA: Code of Professional Ethics of a Certified Information Systems Auditor | The auditor company to maintain. |

| Audit standard | Competency requirements | Ethical requirements | Competence maintenance |
|---|---|---|---|
| **CSA STAR CERTIFICATION** | All assessors must be able to present evidence of passing an accredited lead auditor course for ISO 27001 or be a qualified and experienced ISO 27001 assessor for an IAF member accredited ISO 27001 certification body<br>All assessors must have completed a BSI/CSA CCM course.<br>All assessors must have a minimum of two years of experience working in information security<br>The requirements of 3 are not necessary if the assessor has earned the CSA's Certificate in Cloud Security Knowledge (CCSK) or completed an alternative course that gives a similar level of knowledge in cloud computing or information security applications. | See ISO/IEC 27006 / 19011 | Not defined |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide / "Guidelines for CPAs Providing CSA STAR Attestation v2"*1 (Part 1, section 3) | See ISAE 3000 / SOC 2 Guide / "Guidelines for CPAs Providing CSA STAR Attestation v2"*2 (Part 1, section 3, 3.1.2) | "Guidelines for CPAs Providing CSA STAR Attestation v2"*1 (Part 2, section 1) |

*Table 6. Statutory requirements for an auditor.*

| Audit standard | Statutory requirements |
|---|---|
| **ISO/IEC 27007** | ISO 27001 Lead Auditor, must have professional experience in ISMS auditing |
| **ISAE 3000** | Certified Public Accountant i.e. the general requirements for the auditor associated with the application of ISAE 3000 (Revised) |
| **SOC 2** | Certified Public Accountant i.e. the general requirements for the auditor associated with the application of ISAE 3000 (Revised) |
| **BSI C5** | Certified Public Accountant i.e. the general requirements for the auditor associated with the application of ISAE 3000 (Revised) |
| **SecNumCloud** | PASSI qualified auditor firm. |
| **MFSR** | ISO 27001 Lead Auditor, must have professional experience in ISMS auditing |
| **SI-MPA** | ISO 27001 Lead Auditor, must have professional experience in ISMS auditing |
| **CSA STAR CERTIFICATION** | All assessors must be able to present evidence of passing an accredited lead auditor course for ISO 27001 or be a qualified and experienced ISO 27001 assessor for an IAF member accredited ISO 27001 certification body |
| **CSA STAR ATTESTATION** | Certified Public Accountant i.e. the general requirements for the auditor associated with the application of ISAE 3000 (Revised) |

Remarks: A clear distinction for auditor requirements can be made between studied ISO-based and ISAE-based frameworks. The obligatory requirement for ISO-based frameworks is ISO 27001 Lead Auditor certification while ISAE-based frameworks expect the auditor to be a Certified Public Accountant (CPA). This distinction is further elaborated at chapter 3.2.1.

*Table 7. Requirements for an auditor firm.*

| Audit standard | Company requirement |
|---|---|
| **ISO/IEC 27007** | A certification body conducting 27001 assessments shall be accredited to ISO/IEC 27006 by an International Accreditation Forum (IAF) member accreditation body for delivery of ISO 27001 assessments. |
| **ISAE 3000** | See ISAE 3000 / SOC 2 Guide |
| **SOC 2** | See ISAE 3000 / SOC 2 Guide |
| **BSI C5** | See ISAE 3000 / SOC 2 Guide |
| **SecNumCloud** | PASSI qualified auditor firm. |
| **MFSR** | In process of being defined. |
| **SI-MPA** | The audit company has to be accredited by a national accreditation body (ISO rule).<br>Auditing Act: The auditing service my only be performed by an audit firm, and on behalf of the audit company only by persons authorized to carry out the tasks of a certified auditor. |
| **CSA STAR CERTIFICATION** | A certification body conducting CCM assessments shall be accredited to ISO/IEC 27006 by an International Accreditation Forum (IAF) member accreditation body for delivery of ISO 27001 assessments.<br>A certification body shall comply with all the requirements of ISO/IEC 27006 as well as this document's requirements when conducting a CCM assessment.<br>This document adds greater clarity for areas specific to auditing the CCM, but does not relieve a certification body of its obligation to comply with ISO/IEC 27006 when conducting an assessment.<br>This document adds greater clarity for areas specific to auditing the CCM, but does not relieve a certification body of its obligation to comply with ISO/IEC 27006 when conducting an assessment. |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide |

Using an ISO accredited body as the audit firm allows the auditee to apply for a formal certification. An internationally recognized certification is often a valuable business enabler while adding transparency and trust between the cloud service customer and cloud service providers.

Certified Public Accountant performs an objective and transparent assessment of management systems impacting financial performance reporting on yearly basis. The end result is an attestation on controls, which is widely recognized and no further attestations by other parties are required. Extending this engagement with a team with competent (certified) persons to perform information security audit for cloud services the cloud service provider offers to cloud service customers, provides an objective and transparent assessment of information security safeguards as implemented and operated by the cloud service provider.

When the audit is conducted by an accredited audit and assessment service provider, the competence management inherently responsibility of the accrediting body and service provider thereof. The auditors are required e.g. to maintain a minimum level of qualifications and competence, among the studied standards most thoroughly described in ISO/IEC 27006:2015.

## 3.4 AUDIT PROCESS REQUIREMENTS COLLECTION

### *3.4.1 INITATING THE AUDIT*

Each of the standards require defining the target of assessment at this phase. In case of a cloud service, the audit process aims to verify that the audit objective, target and criteria are set.

*Table 8. Audit process step 1 requirements: Initiating the audit.*

| Audit standard | Audit objective | Audit scope | Source(s) of controls to be audited |
|---|---|---|---|
| **ISO/IEC 27007** | Organizational certification for a chosen ISO27k family standards. | Determined by the auditee. E.g. locations, sites, business processes etc. | ISO27k family of standards. |
| **ISAE 3000** | Promotion of corporate governance and transparency within financial markets in the European marketplace. | Leading standard for the definition of audit objectives. Provides a framework for all assurance engagements other than audits or reviews of historical financial information. Only provides the setting for an audit. A reference to other standards which include actual audit requirements (like SOC 2, CSA CCM, and BSI C5 etc.) needs to be established. | Dependent on the standard. |
| **SOC 2** | Provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls at the service organization. | "Common Criteria" and have to be included in the audit.<br>The criteria Availability, Processing Integrity, Confidentiality and Privacy can be included upon request. | N/A |

| Audit standard | Audit objective | Audit scope | Source(s) of controls to be audited |
|---|---|---|---|
| **BSI C5** | Issue a statement with reasonable assurance (audit opinion) as to whether controls are sufficiently designed (type I) and/or effectively enforced (type II) to assess the information security level of a cloud service provider. | Scope includes 17 control areas which address topics such as Asset Management, Physical Security or Communication Security<br>(see BSI C5 chapter 2.2) | •ISO/IEC 27001:2013<br>•CSA Cloud Controls Matrix 3.01 (CSA CCM)<br>•AICPA Trust Services Principles Criteria 2014 (TSP)<br>•ANSSI Référentiel Secure Cloud v2.0<br>•IDW<br>•ERS FAIT 5<br>•BSI IT-Grundschutz Catalogues, 14th version 2014<br>•BSI SaaS Sicherheitsprofile 2014 |
| **SecNumCloud** | The General Security Repository (RGS) defines a set of security rules that are imposed on administrative authorities in the security of their information systems. It also proposes good practices in the security of information systems that the administrative authorities are free to apply. | The service being considered as the government cloud service provider. | The General Security Repository (RGS) |

| Audit standard | Audit objective | Audit scope | Source(s) of controls to be audited |
|---|---|---|---|
| **MFSR** | To ensure services have been audited for security and quality prior integration to the government cloud. Regulation in place, where ICT service must be technically tested for security. | The service being considered for the government cloud integration. | Requirements collected from CSA CCM and ECSA (European cloud security audit) program, amended by few specific controls. |

| Audit standard | Audit objective | Audit scope | Source(s) of controls to be audited |
|---|---|---|---|
| **SI-MPA** | The audit objective for auditing information systems may be defined in the legislation or set by the organization of public administration on case by case basis. | Two scopes:<br>1) Standard approach in principal: defined each time to cater the people, processes and technology concerned<br>2) Information system supporting a specific working area / application<br>3) Example: SIA defines several types of auditing information systems:<br>4) audit of the entire IT environment (annual, external, internal),<br>5) audit of a particular area (e.g. security),<br>6) a special audit aimed at issuing opinions on the fulfillment of certain conditions and / or objectives,<br>7) Revision of the results of IT projects | Potential sources: legislation, standards (ISO 20k and 27k series).<br>SIA: legislation, auditing standards, ISACA standards and procedures, ISO standards, good practice. |

| Audit standard | Audit objective | Audit scope | Source(s) of controls to be audited |
|---|---|---|---|
| **CSA STAR Certification** | To leverage the requirements of the ISO/IEC 27001 management system standard together with the CSA Cloud Controls Matrix, a specified set of criteria that measures the capability levels of the cloud service, to ensure that the scope of the cloud service provider meets the consumer's needs and is service-level agreement (SLA) driven. | It is based upon achieving ISO/IEC 27001 and additionally the specified set of criteria outlined in the 16 control areas (CCM v.3.0.1.) of the Cloud Controls Matrix. | ISO 27001:2013<br>CCM v.3.0.1.<br>ISO/IEC 17021: 2011<br>ISO/IEC 27006 :2011<br>ISO/IEC 19011:2011 |
| **CSA STAR Attestation** | A CSA STAR Attestation (Type 1) status demonstrates to your customers the commitment to cloud security through a thorough assessment of the policies and procedures in place to protect the Confidentiality, Integrity, and Availability of their data. A Type 1 Attestation provides a solid foundation for a security program, but must be replaced with a Type 2 Attestation ("over a period of time" assessment) within 9 months. | The star attestation program is based on the combined requirements of the CCM and the TSPC.<br>For a cloud system to qualify for STAR attestation, its SOC 2 report scope must cover and the system must satisfy all CCM controls and the TSPC security principle, and must be evaluated to ensure it includes all activities related to the reported cloud system. | ISAE 3000 |

BSI C5, SOC 2 and CSA's STAR Attestation were found to be dependent on ISAE 3000 requirements while CSA's STAR Certification relies on ISO/IEC 27007/19011 guidelines. According to the analysis on the standards the best description for the scope of assessment for Cloud Service context was provided by BSI C5. BSI C5 uses ISAE 3402 as a baseline for defining the minimum scope based on the system description, which includes at least the following components where applicable:

- Type and scope of the provided cloud services,
- Principles, procedures and measures for providing (development and/or operation) cloud services, including the implemented controls,
- Description of the infrastructure, network and system components used for the development and operation of cloud services, including the geographical location of the data in use or at rest,
- Regulation for handling significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical IT systems,
- Roles and responsibilities of the cloud service provider and the customer, including the obligation to cooperate and required corresponding controls by the customer,
- Functions assigned or outsourced to subcontractors.

(Ref. BSI C5, 3.2.2)

### *3.4.2 PREPARING THE AUDIT ACTIVITIES*

The controls requiring assessment are defined at the initial phase of an audit. The controls in scope requiring the audit and assessment, are often defined case-by-case and are composed from multiple sources. The purpose of an audit and assessment process is to verify that the audit criteria are met as set by the respective standard. An audit plan captures these requirements and requirements for it have been collected in the tables below.

*Table 9. Audit process step 2: Preparing the audit activities: audit plan.*

| Audit standard | Is an audit plan required? | Which documents required prior audit? |
|---|---|---|
| **ISO/IEC 27007** | Yes, must follow ISO/IEC 27001 TOC, ISO/IEC 27007 guidelines and consider ISO/IEC 27006 ANNEX B and C guidelines for calculating suggested audit effort and procedures<br>(Ref: ISO/IEC 19011 Clause 6.3.22) | The guidelines from ISO/IEC 19011:2011, Clause 6.3.4, apply:<br>-Checklists<br>-Audit sampling plans<br>-Forms for recording information, such as supporting evidence, audit findings and records of meetings. |
| **ISAE 3000** | Yes, including:<br>- scope<br>- emphasis<br>- timing<br>- conduct | -Agreement on the terms of engagement |
| **SOC 2** | Planning of an audit is specified in the audit framework (see ISAE 3000) | Planning of an audit is specified in the audit framework (see ISAE 3000) |
| **BSI C5** | Planning of an audit is specified in the audit framework (see ISAE 3000) | Planning of an audit is specified in the audit framework (see ISAE 3000) |
| **SecNumCloud** | The provider must document and implement an audit program over three years defining the scope and frequency of audits in accordance with change management, policy, and the results of the risk assessment. | As per the three-year audit program the provider must have. |

| Audit standard | Is an audit plan required? | Which documents required prior audit? |
|---|---|---|
| **MFSR** | Yes, must follow ISO/IEC 27001 TOC, ISO/IEC 27007 guidelines and consider ISO/IEC 27006 ANNEX B and C guidelines for calculating suggested audit effort and procedures<br>(Ref: ISO/IEC 19011 Clause 6.3.22) | The guidelines from ISO/IEC 19011:2011, Clause 6.3.4, apply:<br>-Checklists<br>-Audit sampling plans<br>-Forms for recording information, such as supporting evidence, audit findings and records of meetings. |
| **SI-MPA** | Yes, must follow ISO/IEC 27001 TOC, ISO/IEC 27007 guidelines and consider ISO/IEC 27006 ANNEX B and C guidelines for calculating suggested audit effort and procedures.<br>(Ref: ISO/IEC 19011 Clause 6.3.22) | The guidelines from ISO/IEC 19011:2011, Clause 6.3.4, apply:<br>-Checklists<br>-Audit sampling plans<br>-Forms for recording information, such as supporting evidence, audit findings and records of meetings. |
| **CSA STAR CERTIFICATION** | Yes, must follow ISO/IEC 27001 TOC, ISO/IEC 27007 guidelines and consider ISO/IEC 27006 ANNEX B and C guidelines and requirements for bodies providing STAR certification for calculating suggested audit effort and procedures<br>(Ref: ISO/IEC 19011 Clause 6.3.22) | The guidelines from ISO/IEC 19011:2011, Clause 6.3.4, apply:<br>-Checklists<br>-Audit sampling plans<br>-Forms for recording information, such as supporting evidence, audit findings and records of meetings.<br>- Requirements for bodies providing STAR certification |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide / "Guidelines for CPAs Providing CSA STAR Attestation v2"*2 |

Remarks: BSI C5, SOC 2 and CSA's STAR Attestation were found to be dependent on ISAE 3000 requirements while CSA's STAR Certification and ISO/IEC 27001 relies on ISO/IEC 27006/17021 and ISO/IEC 27007/19011 provided guidelines. Both requirement "families" require mapping of the original requirements to the control environment the cloud provider has. However, a great match can be found from Cloud Controls Matrix (CCM v3) as the de facto industry standard in the market and is referenced by its national sisters such as German Cloud

Computing Compliance Controls Catalogue (C5 v1) and French SecNumCloud for example, and is also integral part of ISAE approach. In case of Trusted Service Criteria, the mapping of controls is a tedious process and has critical importance.

### *3.4.3 CONDUCTING THE AUDIT ACTIVITIES*

*Table 10. Audit process step 3: Conducting the audit activities: reviews.*

| Audit standard | Document reviews? | Interviews? | Observations/Process testing? | Technical testing? |
|---|---|---|---|---|
| **ISO/IEC 27007** | Yes | Yes | Yes | Yes (Conducted by auditor or auditee) |
| **ISAE 3000** | Yes | Yes | Yes | Yes |
| **SOC 2** | Yes | Yes | In general, a distinction is made between two different types of reports: type 1 ("design test") and type 2 ("functional/operating test"). | Yes |
| **BSI C5** | Yes | Yes | Yes | Yes |
| **SecNumCloud** | Professional judgement of the auditor | Professional judgement of the auditor | Professional judgement of the auditor | Yes |
| **MFSR** | Yes | Yes | As per the IIA | Yes, obligation by the regulation |
| **SI-MPA** | Professional judgement of the auditor. SI-MPA | Professional judgement of the auditor. SI-MPA | Preliminary report needs to be reviewed, the auditor has the last word. | Professional judgement of the auditor. SI-MPA obligated to support. |

| Audit standard | Document reviews? | Interviews? | Observations/Process testing? | Technical testing? |
|---|---|---|---|---|
| | obligated to support.<br>SIA: starting review of basic documentation, followed by the review of additional documentation | obligated to support.<br>SIA: The auditor conducts an informative meeting with the management.<br>During the process, there can be interviews with staff | SIA: the auditor presents the report to IT managers who can provide explanations | |
| **CSA STAR CERTIFICATION** | Yes (ISO/IEC 27006 /19011) | Yes (ISO/IEC 27006 /19011) | Yes (ISO/IEC 27006 /19011) | Yes (ISO/IEC 27006 /19011) |
| **CSA STAR ATTESTATION** | Yes, See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide |

Remarks: It can be concluded that all of the standards within the scope accept document reviews, interviews, observations/process testing and technical testing as acceptable evidence collection methods. No standard studied excluded any of the forementioned collection methods, while some mandatory obligations were in place.

*Table 11. Audit process step 3: Conducting the audit activities: non-technical evidence collection.*

| Audit standard | Collection method | Verification method | Acceptable evidence |
|---|---|---|---|
| **ISO/IEC 27007** | Verbal, observation, sampling etc. | Meeting notes | Professional judgement of the auditor |

| Audit standard | Collection method | Verification method | Acceptable evidence |
|---|---|---|---|
| | | Interviews | |
| **ISAE 3000** | **Ref. Paragraph 76 - Nature, Timing and Extent of Procedures:**<br>A combination of procedures is typically used to obtain either reasonable assurance or limited assurance.<br><br>Procedures may include: · Inspection;<br>· Observation;<br>· Confirmation;<br>· Re-calculation;<br>· Re-performance;<br>· Analytical procedures; and<br>· Inquiry | Inquiry, Observation, Inspection, Reperformance | Professional judgement of the auditor<br><br>**Ref. Paragraphs:**<br>**61 – 66 Sufficiency and Appropriateness of Evidence**<br><br>**50 – Evidence**<br><br>**A53 – Quantity and quality of evidence** |
| **SOC 2** | Same as ISAE 3000 | Same as ISAE 3000 | Same as ISAE 3000 |
| **BSI C5** | Same as ISAE 3000 | Same as ISAE 3000 | Same as ISAE 3000 |
| **SecNumCloud** | Professional judgement of the auditor | Professional judgement of the auditor | Professional judgement of the auditor |
| **MFSR** | Not defined yet | Not defined yet | Not defined yet |
| **SI-MPA** | Professional judgement of the auditor. Previous report is revisited. | Professional judgement of the auditor | Professional judgement of the auditor |
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 | See ISO/IEC 27006 / 19011 | See ISO/IEC 27006 / 19011 |

| Audit standard | Collection method | Verification method | Acceptable evidence |
|---|---|---|---|
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide 3000 | See ISAE 3000 / SOC 2 Guide |

Remarks: For non-technical evidence collection the acceptable methods found were verbal interviews, observation, sampling, confirmation, re-calculation, analytical procedures and inquiry where applicable with the corresponding control. For evidence verification and acceptability, professional judgement of auditor is applied. In order for the auitor to be able to professionally judge the evidence, a minimum competence and/or qualification has to be met as described at chapter 3.2.1.

*Table 12. Audit process step 3: Conducting the audit activities: technical evidence collection.*

| Audit standard | Collection method | Verification method | Acceptable evidence |
|---|---|---|---|
| **ISO/IEC 27007** | Not defined | Not defined | Not defined |
| **ISAE 3000** | **Ref. Paragraph 76: Nature, Timing and Extent of Procedures**<br><br>Procedures may include:<br>· Inspection;<br>· Observation;<br>· Confirmation;<br>· Re-calculation;<br>· Re-performance;<br>· Analytical procedures; and<br>· Inquiry | Inquiry, Observation, Inspection, Reperformance | Professional judgement of the auditor |
| **SOC 2** | Same as ISAE 3000 | Same as ISAE 3000 | Same as ISAE 3000 |

| Audit standard | Collection method | Verification method | Acceptable evidence |
|---|---|---|---|
| **BSI C5** | Same as ISAE 3000 | Same as ISAE 3000 | Same as ISAE 3000 |
| **SecNumCloud** | The provider must document and implement a policy to check technical compliance of the service with the requirements of this standard. The policy should define objectives, methods, frequencies, expected results and corrective action. | The auditor must be certified to perform technical security audits. | The auditor must be certified to perform technical security audits. |
| **MFSR** | CSIRT | CSIRT | CSIRT |
| **SI-MPA** | Auditor to decide. Previous report is revisited.<br>SIA: the auditor can request additional documentation, prepares and performs tests, performs interviews with staff, and performs other procedures in accordance with auditing standards. | Professional judgement of the auditor | Professional judgement of the auditor |
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 | See ISO/IEC 27006 / 19011 | See ISO/IEC 27006 / 19011 |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide |

Remarks: In conclusion, the description for sufficient and appropriate evidence as well as the verification method relies on the professional judgement of the auditor. In order to be able to professionally judge the trustworthiness of the collected evidence, the auditor must meet a minimum set of requirements for competence and qualification. The competence requirements for auditor vary between standards, the description is further elaborated at chapter 3.2.1.

### *3.4.4 PREPARING AND DISTRIBUTING THE AUDIT REPORT*

*Table 13. Audit process step 4: Preparing and distributing the audit report: report template.*

| Audit standard | Report format (template) |
|---|---|
| **ISO/IEC 27007** | Ref. 6.5 |
| **ISAE 3000** | No |
| **SOC 2** | No |
| **BSI C5** | Should be structured according to 3.4.2. |
| **SecNumCloud** | No |
| **MFSR** | In process of being defined |
| **SI-MPA** | Depends on the auditor company. |
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide |

Remarks: In preparation of the audit report, none of the studied standards had report format templates in place, however ISO27007, BSI C5 and CSA Certification and Attestation have defined guidelines on what the report has to include.

*Table 14. Audit process step 4: Preparing and distributing the audit report: report variants.*

| Audit standard | Management summary | Detailed technical report |
|---|---|---|
| **ISO/IEC 27007** | Yes | No |
| **ISAE 3000** | Yes | No |
| **SOC 2** | Yes | No |
| **BSI C5** | Yes | No |
| **SecNumCloud** | Yes | Yes |
| **MFSR** | In process of being defined | In process of being defined |
| **SI-MPA** | Yes | Yes, separate from the management report.<br>SIA: A final version of the report is presented to the client. The report can also contain recommendations. |
| **CSA STAR CERTIFICATION** | Yes | Yes[2] |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide |

Remarks: All of the studied standards require a management summary to be included in the audit report, while a separate detailed technical report was only required by a few of the standards/frameworks in scope (SecNumCloud, SI-MPA, CSA STAR Certification). MFSR's requirements were in the process of being defined at the time of the study, and CSA STAR required a technical report where obliged by ISAE 3000 / SOC 2.

[2] A technical audit report is produced that includes the client's performance as a maturity level in accordance to CCM maturity model and capability scoring per each of the control areas.

*Table 15. Audit process step 4: Preparing and distributing the audit report: conditional pass.*

| Audit standard | Pass/fail only? | Conditional pass subject to corrective actions allowed? |
|---|---|---|
| **ISO/IEC 27007** | No | Yes |
| **ISAE 3000** | N/A | N/A |
| **SOC 2** | No | AICPA Trust Service Principles and Criteria are structured into principles and criteria. Auditee's controls are mapped against criteria. If a criterion is not met because all control(s) mapped to a criterion failed, the auditor will issue a report with a qualified opinion. |
| **BSI C5** | No | BSI C5 is structured into control areas and requirements. Auditee's controls are mapped against C5 requirements. If a C5 requirement is not met because all auditee's control(s) mapped to a requirement failed, the auditor will issue a report with a qualified opinion. |
| **SecNumCloud** | No | Yes |
| **MFSR** | In process of being defined | In process of being defined |
| **SI-MPA** | No. | Yes |
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 / "Auditing the Cloud Controls Matrix"* | See ISO/IEC 27006 / 19011/ *A STAR certification certificate cannot be issued unless the organization has passed (is compliant) their ISO 27001 assessment. |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide |

Remarks: Providing audit finding in writing varies between the studied standards:

- A management summary is required to be provided at the end of audit for each of the standards with the exclusion of Slovakian Ministry of Finance's audit process which do not have a requirement of a summary in place or the requirement is in process of being defined.
- A detailed technical report was only required by CSA STAR Certification and Slovenian Ministry of Finance's Audit process, while MFSR's requirement was still being defined.
- An action plan to address nonconformities was required only by CSA's STAR Certification and SI-MPA's audit process.

*Table 16. Audit process step 4: Preparing and distributing the audit report: quality control.*

| Audit standard | Quality control review of the final audit report |
|---|---|
| **ISO/IEC 27007** | Ref. 6.5.2 |
| **ISAE 3000** | For those engagements, if any, for which a quality control review is required by law or regulation or for which the firm has determined that an engagement quality control review is required: (a) The engagement partner shall take responsibility for discussing significant matters arising during the engagement with the engagement quality control reviewer, and not date the assurance report until completion of that review; and<br>(b) The engagement quality control reviewer shall perform an objective evaluation of the significant judgments made by the engagement team, and the conclusions reached in formulating the assurance report. This evaluation shall involve: (Ref: Para. A75) (i) Discussion of significant matters with the engagement partner;<br>(ii) Review of the subject matter information and the proposed assurance report;<br>(iii) Review of selected engagement documentation relating to the significant judgments the engagement team made and the conclusions it reached; and<br>(iv) Evaluation of the conclusions reached in formulating the assurance report and consideration of whether the proposed assurance report is appropriate. |
| **SOC 2** | Same as ISAE 3000 |
| **BSI C5** | Same as ISAE 3000 |

| Audit standard | Quality control review of the final audit report |
|---|---|
| **SecNumCloud** | The auditor company is responsible for this. |
| **MFSR** | See ISO/IEC 27006 / 19011 |
| **SI-MPA** | The auditor company is responsible for this. |
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 |
| **CSA STAR ATTESTTION** | See ISAE 3000 / SOC 2 Guide / "Guidelines for CPAs Providing CSA STAR Attestation v2" (section 3, 3.1.3) |

Remarks: The quality control for the audit report is conducted by the audit company throughout the studied standards and frameworks. For ISO-based standards the quality control requirements are detailed at ISO/IEC 27006 and ISO/IEC 19011, while for ISAE-based frameworks the requirements are described at ISAE 3000 documentation. In conclusion, no significant differences were noticed between the two aforementioned types of standards.

*Table 17. Audit process step 4: Preparing and distributing the audit report: governing body.*

| Audit standard | Governing body | Are audit results reported to governing body? | Does the governing body monitor/accredit auditors? |
|---|---|---|---|
| **ISO/IEC 27007** | FINAS (Finland) | No | Yes – company level accreditation |
| **ISAE 3000** | IFAC | No | No, not a certification but an attestation |
| **SOC 2** | AICPA | No | No, not a certification but an attestation |
| **BSI C5** | BSI | No | No, not a certification but an attestation |
| **SecNumCloud** | ANSSI | No | Yes |

| Audit standard | Governing body | Are audit results reported to governing body? | Does the governing body monitor/accredit auditors? |
|---|---|---|---|
| **MFSR** | Standard accreditation bodies OK. Cloud brokers responsibility to validate. | No. Cloud brokers responsibility. | Yes |
| **SI-MPA** | Slovenian accreditation body<br>The Slovenian Institute of Auditors (SIA) based on Auditing Act<br>Agency for Public Oversight of Auditing | No. | Yes.<br>SIA: manages the register of audit firms and auditors, issues certificates of professional skills for obtaining professional titles in auditing.<br>Auditing Act: Supervision of the quality of auditing is carried out by the SIA and the Agency for Public Oversight of Auditing. |
| **CSA STAR CERTIFICATION** | CSA | Yes | Yes |
| **CSA STAR ATTESTATION** | CSA | Yes | Yes |

Remarks: The governing body for accreditation varies by the country where the assignment is conducted or by the origin of the certification body. The governing body monitors auditors where ever the audit results in a certification; for an attestation monitoring isn't conducted. Having an external monitoring body in place adds to the trust and transparency of the audit results.

### 3.4.5 COMPLETING THE AUDIT

*Table 18. Audit process step 5: Completing the audit: engagement documentation.*

| Audit standard | Engagement documentation (resources, budget, schedule) |
|---|---|
| **ISO/IEC 27007** | As part of the audit plan<br>Ref. 6.3.2 Preparing the audit plan:<br>The amount of detail provided in the audit plan should reflect the scope and complexity of the audit, as well as the effect of uncertainty on achieving the audit objectives. |
| **ISAE 3000** | **ISAE 3000 12:**<br>An audit plan needs to be established which should include:<br>• Terms of engagement<br>• Characteristics of subject matter and criteria<br>• Engagement process and possible sources of evidence<br>• Auditor's understanding of the entity and its environment<br>• Intended users and their needs<br>Personnel and expertise requirements |
| **SOC 2** | Same as ISAE 3000 |
| **BSI C5** | Same as ISAE 3000 |
| **SecNumCloud** | As part of the audit plan |
| **MFSR** | As part of the audit plan<br>Ref. 6.3.2 Preparing the audit plan:<br>The amount of detail provided in the audit plan should reflect the scope and complexity of the audit, as well as the effect of uncertainty on achieving the audit objectives. |

| Audit standard | Engagement documentation (resources, budget, schedule) |
|---|---|
| **SI-MPA** | Preliminary audit plan must be delivered comments, the auditor company then finalizes the audit plan and delivers it to the auditee (the next auditor will benefit from this). |
| **CSA STAR CERTIFICATION** | Audit plan (See ISO/IEC 27006 / 19011 / "Auditing the Cloud Controls Matrix") |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide / "Guidelines for CPAs Providing CSA STAR Attestation v2" (section 2, 2.1-2.3) |

Remarks: In conclusion, the audit plan should cover certain aspects of the engagement on the subjects of resourcing, budget and scheduling. The detailed requirements are covered in ISO/IEC 27007 and ISAE 3000 respectively. While

*Table 19. Audit process step 5: Completing the audit: evidence and report retention.*

| Audit standard | Evidence and report retention |
|---|---|
| **ISO/IEC 27007** | Certification lifecycle (max. 3yrs.) |
| **ISAE 3000** | The retention period for assurance engagements ordinarily is no shorter than five years from the date of the assurance report |
| **SOC 2** | The audit must be carried out and documented so that an expert third party can still understand after 10 years how the audit result was obtained. |
| **BSI C5** | Same as ISAE 3000 |
| **SecNumCloud** | As part of the audit program the provider is to establish, three year cycle. |
| **MFSR** | In process of being defined |
| **SI-MPA** | Depends case by case. |

| Audit standard | Evidence and report retention |
|---|---|
| CSA STAR CERTIFICATION | See ISO/IEC 27006 / 19011 |
| CSA STAR ATTESTATION | See ISAE 3000 / SOC 2 Guide |

Notes: The retention period for generated audit reports varies greatly between the studied requirements:

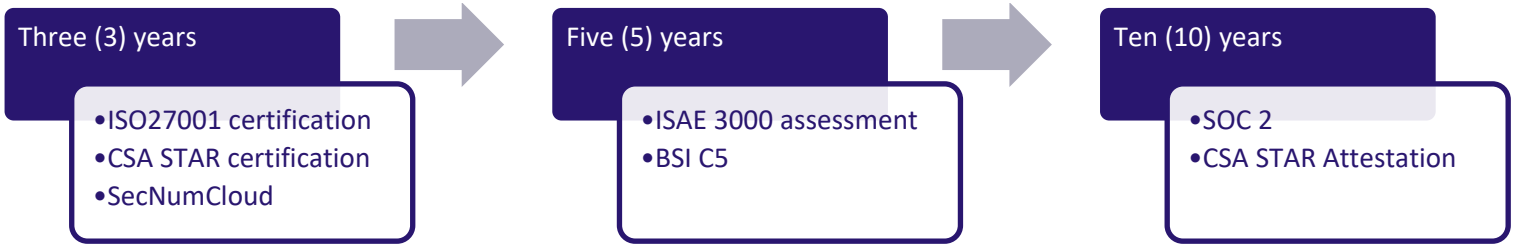



*Figure 8. Retention periods for generated audit reports.*

### 3.4.6 CONDUCTING AUDIT FOLLOW-UP

*Table 20. Audit process step 6: Conducting audit follow-up: auditee feedback.*

| Audit standard | Auditee feedback |
|---|---|
| ISO/IEC 27007 | The auditor company to decide. |
| ISAE 3000 | Not defined |
| SOC 2 | Not defined |
| BSI C5 | Not defined |

| Audit standard | Auditee feedback |
|---|---|
| **SecNumCloud** | Not defined |
| **MFSR** | The auditor company to decide. |
| **SI-MPA** | The auditor company to decide. |
| **CSA STAR CERTIFICATION** | Following an assessment, an organization can choose to make their certification public on the STAR register. They can choose one of the following options:<br>• Disclose that they have been assessed against the CCM, but chose not to disclose any score<br>• Disclose a summary score, but not disclose the score for individual controls areas in the CCM<br>• Full disclosure of the scores for each control area<br>It will be the responsibility of the certification body to ascertain what level of disclosure the organization is prepared to make.<br>Following the client's consent, certification bodies shall submit the scores to the CSA for listing on the CSA's STAR database through a mutually agreed data exchange program. |
| **CSA STAR ATTESTATION** | "Guidelines for CPAs Providing CSA STAR Attestation v2"*1 (Part 2, section 3) |

Remarks: Obligatory requirements for collecting auditee feedback were not found in any of the studied frameworks, hence auditee feedback is to be considered optional.

*Table 21. Audit process step 6: Conducting audit follow-up: non-conformity next steps (action plan).*

| Audit standard | Non-conformity next steps (action plan) |
|---|---|
| **ISO/IEC 27007** | All non-conformities must be addressed and will be re-audited. Depending on whether the non-conformity has been classified as major or minor. |

| Audit standard | Non-conformity next steps (action plan) |
|---|---|
| **ISAE 3000** | No |
| **SOC 2** | No |
| **BSI C5** | No |
| **SecNumCloud** | No |
| **MFSR** | In process of being defined |
| **SI-MPA** | Auditor defines deadline for creating an action plan, the top-management is responsible creating and implementing the plan. |
| **CSA STAR CERTIFICATION** | Yes |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide |

Remarks: In order to achieve compliance, ISO-based frameworks required the non-conformities to be addressed by maintenance audit according to action plan. ISAE-based frameworks within study did not have a requirement for addressing nonconformities.

# 3.5 SUFFICIENT AND APPROPRIATE EVIDENCE REQUIREMENTS COLLECTION

*Table 22. Requirements to obtain sufficient and appropriate evidence: general definition.*

| Audit standard | What is acceptable evidence? |
|---|---|
| **ISO/IEC 27007** | **ISO19011 6.4.6 Collecting and verifying information:**<br>During the audit, information relevant to the audit objectives, scope and criteria, including information relating to interfaces between functions, activities and processes, should be collected by means of appropriate sampling and should be verified. Only information that is verifiable should be accepted as audit evidence. |
| **ISAE 3000** | The practitioner should obtain sufficient appropriate evidence on which to base the conclusion. Sufficiency is the measure of the quantity of evidence. Appropriateness is the measure of the quality of evidence; that is, its relevance and its reliability. The practitioner considers the relationship between the cost of obtaining evidence and the usefulness of the information obtained. However, the matter of difficulty or expense involved is not in itself a valid basis for omitting an evidence-gathering procedure for which there is no alternative. The practitioner uses professional judgment and exercises professional skepticism in evaluating the quantity and quality of evidence, and thus its sufficiency and appropriateness, to support the assurance report.<br>**Sufficiency and Appropriateness of Evidence (Ref: Para. 12(i), 64) A146-154.** |
| **SOC 2** | Same as ISAE 3000 |
| **BSI C5** | Same as ISAE 3000 |
| **SecNumCloud** | The auditor company is responsible for this. |
| **MFSR** | In process of being defined. |
| **SI-MPA** | The auditor company is responsible for this. |

| Audit standard | What is acceptable evidence? |
|---|---|
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 / "Requirements for Bodies Providing STAR Certification"* |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide |

Remarks: In general, all of the frameworks studied had a requirement in place for evidence evaluation, with the exception of MFSR which was under process of being defined. The conclusion is that audit evidence has to be verifiable, sufficient and collected with appropriate methods.

*Table 23. Requirements to obtain sufficient and appropriate evidence for a control in scope.*

| Audit standard | Acceptable evidence for a control in scope | Non-conformity reporting | Non-conformity handling (risk based?) |
|---|---|---|---|
| **ISO/IEC 27007** | The guidelines from ISO/IEC 19011:2011, Clause 6.4.6, apply. | Any non-conformities are established. | All non-conformities must be addressed and will be re-audited. Depending on whether the non-conformity has been classified as major or minor. |
| **ISAE 3000** | Based on applied requirements catalogue<br><br>**Ref. Paragraph 42 - 49 – Criteria** | Based on applied requirements catalogue | Based on applied requirements catalogue |
| **SOC 2** | The requirements specified in the AICPA Trust Services Principles and Criteria. | Not defined | Not defined |

| Audit standard | Acceptable evidence for a control in scope | Non-conformity reporting | Non-conformity handling (risk based?) |
|---|---|---|---|
| **BSI C5** | The requirements specified in the BSI C5 catalogue. | If a deficiency was found, it must be specified when and with which measures the deficiency was identified. (BSI C5: 3.5.2) | In any case, it should be specified which measures for the future elimination of the deficiency and the date when these measures will be completed and/or implemented effectively.<br>(BSI C5: 3.5.2) |
| **SecNumCloud** | As per the certification the auditor (company) holds. | As per the certification the auditor (company) holds. | Risk based handling, top-management is responsible for the action plan |
| **MFSR** | In process of being defined | In process of being defined | In process of being defined |
| **SI-MPA** | As per the certification the auditor (company) holds. | The report is delivered for the top-management and on yearly basis to budget supervision office.<br>SIA: A final version of the report is presented to the client. The report can also contain recommendations. | Risk based handling, top-management is responsible for the action plan. |

| Audit standard | Acceptable evidence for a control in scope | Non-conformity reporting | Non-conformity handling (risk based?) |
|---|---|---|---|
| **CSA STAR CERTIFICATION** | See ISO/IEC 27006 / 19011 / "Auditing the Cloud Controls Matrix"[3] | See ISO/IEC 27006 / 19011 / "Auditing the Cloud Controls Matrix"[4] | See ISO/IEC 27006 / 19011 |
| **CSA STAR ATTESTATION** | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide | See ISAE 3000 / SOC 2 Guide |

Remarks: The audit evidence for each of the standards studied could be collected with similar methods: document reviews, interviews, observations/process testing and technical testing. While ISO27001 and ISAE 3000 accept the fore mentioned methods throughout the process, other standards such as SecNumCloud and SI-MPA's audit guidelines however give the auditor more freedom to decide which methods are adequate and sufficient in verifying the evidence.

[3] The CCM will be audited against a management capability model. Guidance on how to audit to this model can be found in the CSA's document 'Auditing the Cloud Controls Matrix'

[4] If a client has a major Non Conformance Report in the control area, the maximum possible score will be 6. An organization certified to ISO 27001 it is very unlikely that they would not achieve at least a bronze award (score between 3 and 6). The maturity level (No award up to Gold award) is not listed in the certificate but only in the auditing report.

# 3.6 ISO AUDIT APPROACH COMPATIBLITY AND ACCREDITATION

*Table 24. ISO audit approach compatibility.*

| Audit standard | Are audits conducted based on ISO/IEC 19011 + SFS-EN ISO/IEC 27007 guidelines seen as an acceptable audit procedure? Answers: fully, partially, no |
|---|---|
| **ISO/IEC 27007** | -- |
| **ISAE 3000** | No |
| **SOC 2** | No |
| **BSI C5** | No |
| **SecNumCloud** | Fully |
| **MFSR** | Partially |
| **SI-MPA** | Fully |
| **CSA STAR CERTIFICATION** | Fully |
| **CSA STAR ATTESTATION** | No |

Remarks: Of the studied frameworks, SecNumCloud, SI-MPA and CSA STAR Certification based their audit processes on ISO/IEC 19011 + SFS-EN ISO/IEC 27007 guidelines while MFSR's audit process was considered partially applicable.

*Table 25. National, international and industry certification bodies.*

| Audit standard | Please list national, international and industry certification bodies, if any? | Are these certification bodies complying with ISO/IEC 17021-1 + ISO/IEC 27006? |
|---|---|---|
| **ISO/IEC 27007** | E.g. in FIN 3 accredited companies: Nixu, KPMG and Inspecta. Internationally a large number of accredited certification bodies such as DNV etc. | Yes |
| **ISAE 3000** | N/A, not a certification but an attestation | N/A, not a certification but an attestation |
| **SOC 2** | N/A, not a certification but an attestation | N/A, not a certification but an attestation |
| **BSI C5** | N/A, not a certification but an attestation | N/A, not a certification but an attestation |
| **SecNumCloud** | ANSSI (National Agency for the Security of Information Systems) | No |
| **MFSR** | Slovak National Accreditation Service | Yes (Based on ISO) |
| **SI-MPA** | Slovenian accreditation body for the auditor companies. | Yes (Based on ISO) |
| **CSA STAR CERTIFICATION** | BSI, Coalfire ISO, DNV-GL, EY CertifyPoint, NIXU, Schellman, SGS, TUV Austria | Yes (compliance with 27006 is required) |
| **CSA STAR ATTESTATION** | N/A (w.r.t to attestation Deloitte, E&Y , KPMG, Schellman, Weaver)* | No |

Remarks: The ISO 27001 certification bodies are generally accredited nationally by local industry certification bodies, all of the accredited certification bodies have to be compliant with ISO/IEC 17021-1 + ISO/IEC 27006. For attestation-orientated ISAE-based schemes similar accreditation requirements was not reported.

# 3.7 COMPARISON OF THE ISAE 3402 AND ISO/IEC 27007

ISO/IEC 27007 "Guidelines for information security management systems auditing" and ISAE 3402 "Assurance reports on Controls at a Service Organization" are both used as supporting documents to describe the both normative requirements and best practices for ISMS evaluation processes. Companies providing these assessment services have different paths of accreditation. Therefore, we have compared these standards one-to-one to recognize the main differences. We compare first the structure, then users and finally domains of application of the standards.

## *3.7.1 STRUCTURE*

ISO/IEC 27007:2011 builds upon ISO/IEC 19011:2011 – "Guidelines for auditing management systems" - and ISAE 3402 "Assurance Reports on Controls at a Service Organization" builds upon ISAE 3000 "International Standard on Assurance Engagements" respectively. The objective for these documents is to provide guidelines for auditing and assessment process. On a high level both are similar comparing the table of contents and main topics addressed by these standards. Both ISO 27001 and ISAE-compliant information security management systems are required to have a process in place for continuous improvement in order to maintain the validity of certification. Maintenance audits are required annually at minimum for both frameworks.

## *3.7.2 USERS*

The most common user groups for ISO/IEC-family of standards are companies seeking formal ISO27001 certification or information security compliance assessments/attestations. ISO 27001-family of standards may also be used for informal self-assessments by organizations looking for ISO-compliance.

ISAE 3000 and 3402 are used by certified public accountants for similar assessments, however, giving more space for an auditee to choose, which security requirements are applicable for its internal control environment. Once those are defined, an auditor will utilize ISAE 3000 to provide attestation on the control environment itself as well as the operation of these controls.

### 3.7.3 SIMILARITIES AND DIFFERENCES IN APPLICATION

ISO 27000-family of standards focus on assessing information security management systems (ISMS) specifically while ISAE standards have been developed for assessing internal controls on a more general level. However, both are suitable for assessing information security (cloud) controls as well.

The main differences between ISO/IEC 27007:2011 and ISAE 3402 can be noted in the scoping phase of an audit and assessment engagement. ISO/IEC 27007 describes the requirements for the auditing process from planning to report itself while ISAE 3402 focuses on the requirements for the controls, although including guidelines for the auditing process as well. A notable difference can be found at the evidence evaluation and collection phase of the audit process. When applying for compliance against ISO 27001 controls, the auditee provides the auditor evidence representing a snapshot of current state of control objectives. ISAE 3000 on the other hand requires the auditee to provide evidence history from a longer period of time, six or twelve months back. However, ISO 27001 compliance requires evidence that the ISMS processes have been successfully conducted beyond planning while the timeframe is not specified.

Both standards aim to describe the normative requirements and informative guidelines in order to achieve the desired respective ISO compliance or attestation on controls. While the objective providing guidelines for the audit process is similar between the two standards, the main difference is that ISO27000 family focuses only on ISMS while with ISAE information security is just one of the possible applications. In theory, ISO27001 can be seen as a risk-based approach, where the scope is defined through risk assessment. ISAE framework on the other hand is used in context of fixed certification objectives and a set control framework Therefore it can be concluded that while both ISO 27001 and ISAE 3000 models itself can be used to provide proof of compliance against similar objectives in cloud security compliance (See chapter 4.2).

# 4 RECOMMENDATIONS

A cloud service customer counts on the cloud service provider's ability to provide service with equal or better controls in place compared to its own IT. While the audit and assessment engagements traditionally are seen as a manual process of verbal interviews, written observation, manual inspection, observation, confirmation, re-calculation, re-performance, analytical procedures and inquiries, in the IT age, many controls may have been automated and auditors could utilize IT tools in performance of the audits. In practice these IT methods and tools to support the audit process may be even required to collect appropriate and sufficient evidence for a cloud control implementation, operation and/or maintenance.

The following chapters attempt to present recommendations based on collected audit and assessment requirements from

- ISO standards for auditing management systems (ISO/IEC 17021 and ISO/IEC 19011)
- ISO standards for auditing information security management systems (ISO/IEC 27006 and ISO/IEC 27007)
- International Auditing and Assurance Standards Board proposed International Standards for Assurance Engagements ISAE 3000 and ISAE 3402

Other sources for guidelines that have been reviewed, are:

- SOC 2 for Service Organizations: Trust Services Criteria - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- Bundesamt für Sicherheit in der Informationstechnik (eng. German Federal Office for Information Security) Cloud Computing Compliance Controls Catalogue (BSI C5)
- SecNumCloud issued by Agence nationale de la sécurité des systèmes d'information (eng. National Cybersecurity Agency of France)
- Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR) Certification
- Cloud Security Alliance's Security, Trust & Assurance Registry (CSA STAR) Attestation
- Audit and assessment requirements for the public procurement of government cloud services in Slovakia and Slovenia

## 4.1 AUDIT AND ASSESSMENT PROVIDER

Cloud service providers don't usually allow Customers' auditors to interfere with their IT operations. An independent audit and assessment is therefore required. After analysis of the auditing and assessment requirements and in an attempt to optimize the cloud service providers' point of view, it may be optimal for an auditee to seek certification through ISO/IEC 27001, with ISAE 3000 specific amendments for the audit process. Benefits of this approach include but are not limited to standardized processes to maintain compliance, to handle non-conformities and to perform continuous certification. An internationally recognized certification is a valuable business enabler and adds transparency and trust between cloud service customers and the cloud service provider. In essence the general requirements for auditor stated in chapter 3.2.1 are recommended.

## 4.2 CONTROLS IN SCOPE

The controls in scope requiring the assessment, are in most cases defined case-by-case, risk-based and are composed from multiple sources. However, often match can be found with standards controls. EU-SEC project contributes to enhanced mapping of laws, regulation and industry requirements to standard cloud controls. A cloud service provider seeking for multiple certifications or attestations of compliance may achieve this via EU-SEC designed multiparty audit and assessment engagement, adding benefits of meeting not one but several audit criteria with one engagement and this way, possibly lowering the "unit" cost of compliance for the cloud service provider. Therefore, we recommend building control environment in compliance with CCMv3 and structured according to ISO/IEC 27001 topics to seek for ISO/IEC 27001 certification.

## 4.3 MULTIPARTY RECOGNITION

Running an internal control system related to the cloud services require comprehensive IT governance, risk and compliance processes and workflows. As the risk is "owned" by IT risk stakeholder both from cloud service provider and customer side, managing impacts on business outcomes, company and customer commitments is a complex task, which may result a massive spreadsheet exercise, leaving less time for the actual risk management work. IT Risk

Management (ITRM) solutions may provide the needed automation for common routine risk process workflows, policy management, control mapping and data, allowing reporting on controls to be based on data stored in a control and evidence database, for example. Such solutions may also integrate with vulnerability scan data, security configuration data and SIEM data (alerts), and provide vulnerability remediation workflow respectively. This data may provide a leverage for continuous audits and certification.

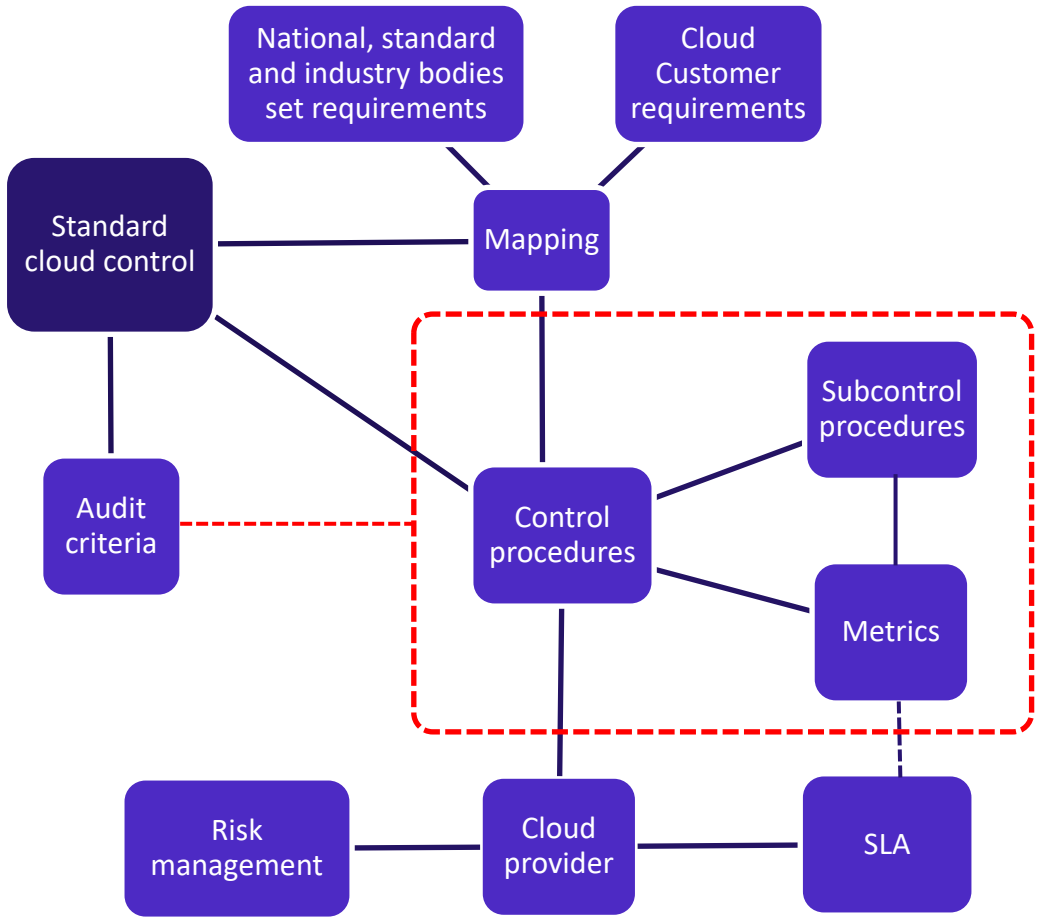



*Figure 9. Simple illustration of an audit criteria composition and integrated risk management.*

A cloud service provider seeking for multiple accreditations (e.g. PCI DSS, SOC2, ISO27001, and BSI C5) may benefit from an EU-SEC designed multiparty audit and assessment engagement to meet not one but several audit criteria with one engagement. This may possibly lower the "unit" cost of compliance for the cloud service provider. In the picture above the standard cloud control is the "EU-SEC requirements and controls repository", contain enhanced mapping of laws, regulation and industry requirements to standard cloud controls. This standard (EU-SEC)

cloud control repository can be seen as public reference point, but the audit criteria applied is an evaluation of the cloud provider specific internal control environment in respect to the mapped standards, laws, regulations and other could service customer requirements. Therefore this information is strictly confidential and illustrated with dotted red line in the figure above.

In most cases building control environment in compliance with CCMv3 and structured according to ISO/IEC 27001 topics, can be seen multiparty recognition friendly approach. This is a compliant approach as well, including ISAE 3000, and does not limit building control environment according to SOC 2, BSI C5 and/or SecNumCloud. However to comply with these latter mentioned standards specifically require extra efforts, because the audit must be restructured according to these control schemes.

The EU-SEC audit engagement must focus on the cloud service provider's (auditee's) internal control environment and it's mapping to EU-SEC standard cloud control repository, taking into account any of the (mapped) requirements applying to it and deriving the actual audit criteria per a standard cloud control (individually), practically speaking case-by-case basis until a general consensus of the implementation and operation of the safeguard is achieved. Ideally the composed audit criteria (be it technical or non-technical) is formulated in a such manner, which fulfills all requirements mapped to the control in question, and the audit itself can implicitly conclude all mapped requirements "compliant" or "non-compliant" or "n/a", for example.

## 4.4 EU-SEC CONSENSUS AUDIT REQUIREMENTS

*Table 26. EU-SEC audit recommendations for audit requirements.*

| Topic | Requirement |
|---|---|
| **Auditor** | For the audit or assessment of specific subset of information security management systems of cloud service provider the following applies:<br>o General Requirements For auditor (Chapter 3.2.1)<br>o Auditor team lead must have three or more years of professional experience in ISMS auditing (Ref. BSI C5) |

| Topic | Requirement |
|---|---|
| **Audit scope** | Minimum scope is based on the system description, which includes at least the following components where applicable:<br>• Type and scope of the provided cloud services,<br>• Principles, procedures and measures for providing (development and/or operation) cloud services, including the implemented controls,<br>• Description of the infrastructure, network and system components used for the development and operation of cloud services, including the geographical location of the data in use or at rest,<br>• Regulation for handling significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical IT systems,<br>• Roles and responsibilities of the cloud service provider and cloud service customers, including the obligation to cooperate and required corresponding controls by the cloud service customer,<br>• Functions assigned or outsourced to subcontractors.<br>(Ref. BSI C5, 3.2.2) |
| **Audit criteria** | A cloud service provider, seeking for multiple accreditations, may achieve this via EU-SEC designed multiparty audit and assessment engagement, adding benefits of meeting not one but several audit criteria with one engagement and this way, possibly lowering the "unit" cost of compliance for the cloud service provider. Therefore, we recommend building control environment in compliance with CCMv3 and structured according to ISO/IEC 27001 topics to seek for ISO/IEC 27001 certification. |
| **Sufficient and appropriate evidence** | ISO/IEC 27007 AND ISO/IEC 19011 guidelines apply. Endorse **Fehler! Verweisquelle konnte nicht gefunden werden.** at the cloud service provider side (Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**). |
| **Written report** | • Management summary is provided at the end of audit<br>• Management summary and audit report are to be retained for the duration of two certification lifecycles (6 years)<br>• ISO/IEC 27007 AND ISO/IEC 19011 guidelines for report ToC apply |

Remarks:

- ISO/IEC 27001 based ISMS by design gather all regulations, laws, and other external/internal requirements and defines controls with risk based approach to satisfy the all of them. A compliant ISO/IEC 27001 ISMS is thus a dynamic machine, which takes care of itself.
- Information Security audit does not assess the business risk of the cloud service provider going out of business, exposing the cloud service customers to information availability risk.

# REFERENCES

General Data Protection Regulation EU (2016/679) (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679) (Referenced 21.8.2017)

ISAE 3402 (http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf) (Referenced 25.8.2017)

ISO/IEC 17024:2012 General requirements for bodies operating certification of persons, July 2012

ISO/IEC 19011:2011, Guidelines for auditing management systems, November 2011

ISO/IEC 27001:2013, Information security standard, September 2013

ISO/IEC 27006:2015, Requirements for bodies providing audit and certification of information security management systems, October 2015

ISO/IEC 27007:2011, Guidelines for information security management systems auditing, October 2017

SecNumCloud (https://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.0_niveau_essentiel.pdf) (Referenced 21.8.2017)

BSI Compliance Controls Catalogue (C5) (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/ComplianceControlsCatalogue.pdf;jsessionid=CC804E3B3EAF5EE632A81AB5E18296E8.1_cid369?__blob=publicationFile&v=4) (Referenced 21.8.2017)