Antti Hentula

EVIDENCE IN CLOUD SECURITY COMPLIANCE – TOWARDS A META-EVALUATION FRAMEWORK

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2019

ABSTRACT

Hentula, Antti
Evidence in cloud security – Towards a meta-evaluation framework
Jyväskylä: University of Jyväskylä, 2019, 77 p.
Cyber Security, Master's Thesis
Supervisor: Soliman, Wael

Recently the trend of outsourcing IT services into cloud environments as opposed to traditional locally administrated services has been on the rise. This transition allows enables great cost savings through service flexibility for the customer. As a byproduct, the need for the cloud security customers to assure that the service being considered or used meets the needs to provide appropriate security to protect customer data presents formerly inexistent compliance challenges.

To provide transparency and trust between cloud security customer and service provider, several new standards and frameworks have emerged to provide trust by assuring a set of safeguards demanded by a respective standard are in place. The standards provide a set of controls, requirements that must be met to receive an official certification or a third-party attestation. The compliance against the controls must be verified by providing evidence to an auditor. This is followed by the auditor's decision of whether the requirements are in place or not.

The problem with a host of existing standards and frameworks suitable for auditing cloud security is that the process of evidence evaluation is not described in detail or at all. As of now, the evidence evaluation in many standards is left to the professional judgement of the auditor. Auditors are fallible to human errors, such as biased decision-making, in the absence of standardized guidelines. The objective for the master's thesis is to study the quality requirements for scientific evidence and find out if the qualities are applicable and transferable over to cloud security audit evidence evaluation.

The discovered applicable qualities will be conceptualized into a checklist, a meta-evaluation tool to assist both the auditor and the auditee in the evaluation decision-making process. The conclusions may assist the auditee in providing the auditor quality evidence and the auditor will be able to review the evidence from sufficiency and appropriateness points of view. In other words, the objective is to study what the professional judgement of the auditor should consist of; what qualities must cloud security compliance assessment evidence consist of.

Keywords: Audit, assurance, evidence evaluation, frameworks, cloud security, compliance, information security management systems

TIIVISTELMÄ

Hentula, Antti
Evidence in cloud security – Towards a meta-evaluation framework
Jyväskylä: Jyväskylän Yliopisto, 2019, 77 s.
Tietojenkäsittelytiede (Kyberturvallisuus), pro gradu -tutkielma
Ohjaaja: Soliman, Wael

IT-palveluiden ulkoistamisen trendinä on ollut viime aikoina julkisten pilvipalveluiden käyttöönotto perinteisen, paikallisen "on premise"-kapasiteetin kehittämisen sijaan. Muutos tarjoaa mahdollisuuden merkittäviin kustannussäästöihin pilvipalveluiden joustavuuden ansiosta. Samalla pilvipalveluiden asiakkaat ovat alkaneet vaatimaan palveluntarjoajia todentamaan, miten kilpailutettava tai hankittu palvelu ylläpitää riittävää tietoturvallisuustasoa asiakasdatan suojaamiseksi uusien vaatimuksenmukaisuushaasteiden edessä.

Läpinäkyvyyden ja luottamuksen luomiseksi pilvipalveluntarjoajien ja asiakkaiden välille, on kehitetty uusia turvallisuusstandardeja ja viitekehyksiä, jotka tarjoavat työkaluja palvelun tietoturvatason todentamiseksi. Standardit sisältävät sarjan vaatimuksia ja kontrolleja, jotka täyttämällä palvelu voi hakea virallista sertifiointia tai kolmannen osapuolen lausuntoa palvelun turvallisuustasosta. Vaatimuksenmukaisuus todennetaan parhaiten ulkopuolisen auditoijan toimesta, jonka tehtävänä on arvioida auditoitavan toimittamaa todistusainestoa. Todistusaineiston perusteella auditoija muodostaa päätöksen arvioitavan järjestelmän vaatimuksenmukaisuudesta.

Useiden pilvispesifisten standardien ja viitekehysten ongelmana on, että itse todistusaineiston arviointiprosessia ja todistusaineistolle asetettuja laatuvaatimuksia on kuvattu vain pintapuolisesti tai ei ollenkaan. Monet standardit jättävät todistusaineiston arvioinnin auditoijan oletetun ammattitaidon varaan. Tämän pro gradu-tutkielman tavoitteena on tutkia narratiivistyyppisen järjestelmällisen kirjallisuuskatsauksen keinoin poikkitieteellisesti todistusaineiston, eli evidenssin määritelmää ja kartoittaa, mitä laatuominaisuuksia pilvipalveluiden tietoturvallisuuden todentamiseen liittyvään evidenssiin tulee sisältyä.

Lisäksi tavoitteena on luoda hahmotelma pilvipalveluiden evidenssin arvioinnin tukena käytettävästä työkalusta, jonka avulla auditoitava voi tuottaa auditoijalle laadukasta todistusaineistoa tai auditoija pystyy arvioimaan esitetyn todistusaineiston kelpoisuutta. Toisin sanoen, tavoitteena on tutkia, mitä ammattitaitoinen tietojärjestelmätarkastaja haluaa todistusaineiston sisältävän todennettaessa pilvipalvelun tietoturvallisuutta.

Asiasanat: Auditointi, todentaminen, todistusaineiston arviointi, viitekehykset, pilvipalveluiden turvallisuus, vaatimuksenmukaisuus, tietoturvallisuuden johtamisjärjestelmät

FIGURES

Figure 1: Key stages in a systematic review (Modified from Jesson, Matheson & Lacey. 2011, p. 104) 10
Figure 2: Security responsibilities in different types of cloud services. (ENISA, Cloud Standards and Security, 2014, p. 2) 30
Figure 3: Gantz (2013) The Basics of IT Audit: Purposes, Processes, and Practical Information (p. 32) 39
Figure 4: Gantz (2013) p. 183 42
Figure 5: Gott, R. & Duggan, S. (2011), p. 4 44
Figure 6: Gray & Manson (2000) p. 155 46
Figure 7: Relationship of Risk of material Misstatement to Suffciency (Quantity) of Audit Evidence required (Zuca, 2013, p. 702. originally from Puncel, L 2009.) 50
Figure 8: Relationship of Appropriateness (Quality) to sufficiency (Quantity) of audit Evidence Required (Zuca, 2013, p. 702. originally from Puncel, L 2009.) . 50

TABLES

Table 1: Online material collection, search words 14
Table 2: Abbreviations and key terminology 25
Table 3: Cloud security responsibilities (Modified from Salazar, 2016, p. 4) 31
Table 4: Modified from Gantz (2013), p. 33 40
Table 5: Modified from Gantz (2013) p. 157 43
Table 6: Evidence evaluation checklist concept 59
Table 7:Evidence identifier list example 59
Table 8: CSA CCM requirement IAM-04: Identity & Access Management, Policies and Procedures 60
Table 9: Evidence evaluation checklist in practice, administrative requirement. 61
Table 10: CSA CCM requirement IVS-01: Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection 62
Table 11: Evidence evaluation checklist in practice, technical requirement. 63
Table 12: CSA CCM requirement DCS-09, Datacenter Security / User Access . 64
Table 13: Evidence evaluation checklist in practice, physical requirement. 65

TABLE OF CONTENTS

ABSTRACT 2

TIIVISTELMÄ 3

FIGURES 4

TABLES 4

TABLE OF CONTENTS 5

1 INTRODUCTION 7

2 RESEARCH FRAMEWORK 9
- 2.1 Research problems 11
- 2.2 Research question 12
- 2.3 Material collection 13
- 2.4 The need for evidence evaluation in cloud security compliance 15
- 2.5 Previous related research 17

3 CLOUD COMPUTING AND SECURITY COMPLIANCE 20
- 3.1 Abbreviations and key terminology 23
- 3.2 Cloud computing security certification schemes 25
- 3.3 Cloud-specific security objectives 28
- 3.4 Audit and assurance process 31
- 3.5 Audit evidence 34

4 EVIDENCE COLLECTION PROCESS IN CLOUD COMPLIANCE 37
- 4.1 Types/domains of requirements and controls 39
- 4.2 Evidence types and collection methods 42

5 EVIDENCE DEFINITION IN SCIENTIFIC RESEARCH 44
- 5.1 The scope of the cross-scientific review for definition of evidence 44
- 5.2 Evidence and its evaluation in scientific research 46
- 5.3 The effect of cognitive bias on evaluation process 55

6 QUALITY APPRAISAL OF THE DISCOVERIES 58
- 6.1 Evidence evaluation checklist concept 58
- 6.2 Evaluation checklist for an administrative requirement 60
- 6.3 Evaluation checklist for a technical requirement 62
- 6.4 Evaluation checklist for a physical requirement 64
- 6.5 The results of conceptualization and discussion 66

7 CONCLUSIONS 68

REFERENCES..70

8 APPENDIX 1 SUMMARY OF REVIEWED TEXTS..75

1 INTRODUCTION

Recently the trend of outsourcing information technology-dependent services into cloud environments as opposed to traditional locally administrated services has been on the rise. As a byproduct for the phenomenon, the need for cloud computing platform and service users to assure that the service being considered is capable to provide appropriate security measures to protect valuable customer data has posed a new problem.

To provide transparency and trust between cloud service shareholders, service provider, customer and end user, several standards and frameworks are in use globally, with ISO27001/27017 being the *de facto* for cloud security. Additionally, there has been an emergence of several other universally applicable cloud security frameworks, such as the Cloud Security Alliance's Cloud Controls Matrix, and national standards for cloud security, such as the Finnish *PiTuKri*. The standards provide a set of controls, requirements that must be met in order to achieve an official certification or attestation. The compliance is verified by providing evidence on how the assessed system meets the requirements, presented to an external auditor. This is followed by the auditor's decision of whether the requirements are satisfied. If all requirements are met, the auditor can then award the auditee a certificate of compliance[1]. This process includes the main research problem of this study.

The issue with many of existing standards and frameworks suitable for auditing cloud security is that the process of evidence evaluation is not described in detail or at all. As of now, the evidence evaluation in many current standards is up to the professional judgement of the auditor. This means that it is the auditor's responsibility to provide an educated opinion of whether the evidence is sufficient and appropriate. However, even if the evidence is evaluated valid, it may still result in either compliance or non-compliance against the control it is being reviewed for. Also, in absence of an evidence evaluation process or a guideline, the auditor's opinion may be affected by the auditor's bias that will

[1] Even though the standards are commonly implemented, many of the implementing organizations choose to not apply for a certification but rather use the standards as "best-practice" tools.

inevitably influence the audit outcome and quality. However, it should be noted that an unfitting structured guideline might also result in flawed judgement.

The objective for this master's thesis is to provide an exploratory overview into evidence requirements for cloud auditing and assurance, the research will be carried out as a narrative systematic literature review. The conclusions may help both the auditor and the auditee to streamline the assurance process by cutting out time wasted on processing insufficient evidence. The auditee will be able to provide the auditor with quality evidence and understand what the auditor is looking for in the evidence quality-wise. In other words, the objective is to study what the professional judgement of the auditor should consist of.

In order to support the discovered common nominators, the quality requirements for evidence, a proposal for an evidence evaluation tool will be drafted. The tool will not be an end-all solution for evaluating evidence in all cloud-related security audits, but rather a concept or a proposal, a first step towards understanding the evidence evaluation process for cloud security compliance. The outcome could be a primer for further research on the subject or even useful as-is in the absence of other purpose-built guidelines or tools.

2 RESEARCH FRAMEWORK

The objective of the research is to provide an answer to the research question:" *What quality requirements can be applied on cloud security audit evidence?"*. In other words, what qualities make up the "professional judgement" by an auditor. The research problems will be answered by studying the objectives on what does an auditor look for in evidence to be able to provide an educated opinion on the sufficiency and appropriateness of the evidence. The research is qualitative in nature and the selected research method after considering several options is *systematic literature review* for its suitability on the type of material collection required for this study.

I postulate that even in the absence of information security and cloud computing, there are various models and methods could be applied in cloud security evidence evaluation as such (or with certain necessarily modifications). The research requires a general understanding of information security and cloud security frameworks including the security requirements, the auditor's evidence collection methodology and the evidence review mindset.

To understand the auditor's decision-making process, the concepts of evidence must be studied from multiple points of view and from various fields and disciplines of scientific research. The goal is to provide an exploratory overview into cloud security evidence evaluation rather than a prescriptive set of criteria. Furthermore, the research is focused on *evaluation of collected evidence*, however the evidence collection method selection is briefly covered to provide an understanding on the complete audit process on a general level.

The study collects and concludes evidence requirements from multiple disciplines to gain an understanding on security evidence requirements applicable in cloud security auditing. The systematic literature review research method was found to be fitting for the purpose of this research. According to Jesson, Matheson and Lacey (2011, p. 104), systematic reviews provide a systematic, transparent means for gathering, synthesizing and appraising the findings of studies on a particular topic or question. Additionally, the aim is to minimize the bias associated with single studies and non-systematic reviews. According to the authors, the output of the study is a research article that identifies relevant studies, appraises their quality, and summarizes their results using scientific methodology. The systematic review method includes identifying and sifting through all the relevant studies and evaluating each according to predefined criteria (Jesson, Matheson and Lacey, p. 105). In essence, this is what distinguishes a systematic review from a traditional review[2]. The steps of the research process are presented in the following figure:

[2] As opposed to systematic review, a traditional review has less academic rigor and formal methodology, making it less helpful for policy development. (Jesson, Matheson and Lacey, 2011, p.73)

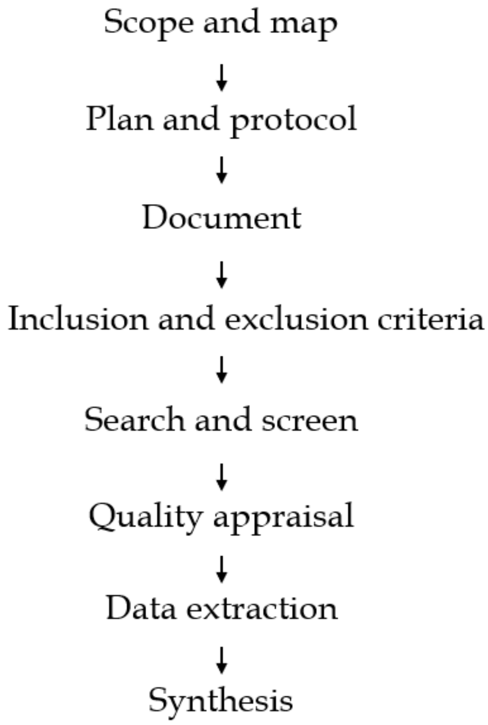


Figure 1: Key stages in a systematic review (Modified from Jesson, Matheson & Lacey. 2011, p. 104)

The aforementioned steps are conducted in this research as follows: The scope and map-phase are specified to answer the research question, presented in subchapter 2.2. The emphasis of the research question is in cloud security, all of the findings in this study will be synthesized to answer the question on specifically cloud computing's point of view. The planning phase is detailed in chapter 2, including the plan for material collection, analysis and quality appraisal of the discoveries. The findings are documented as the research processes and relevant discoveries are detailed in dedicated chapters. The general process of the search and screen phase is detailed in subchapter 2. The search and screen phase are focused on the data analysis of existing evidence definitions, as well as evidence requirements and evaluation methods in cloud computing and beyond.

Furthermore, according to Templier & Paré (2015, p. 133), systematic literature reviews (SLR) can be split into four different types, narrative, developmental, cumulative and aggregative. As the general objective of narrative-type systematic literature reviews is to map the current state of knowledge and identify gaps in prior research, this type was found best fitting for this study. According to the authors, narrative systematic literature review allows researchers to gather studies that focus on thematically dissimilar concepts and findings, as well as combining both conceptual and empirical studies with varying methods and designs. Most importantly, as stated by Templier & Paré (p. 118), narrative reviews often serve as an appropriate starting point for future inquiries and research developments and help researchers to determine and refine research questions or hypotheses. This study follows the aforementioned approach in pursuing a primer or a starting point on future research on security audit evidence quality.

Another approach on SLR research, presented by Okoli & Schabram, (2010, p. 7) is aimed specifically for information systems research, that also in concluded of 8 steps as Jesson, Matheson & Lacey's model, although with slightly different terminology. However, Okoli & Schrabram cover the steps in greater detail, that were used in concretizing the steps for this study. Jesson & Matheson & Lacey (2011, p. 105) recognize a checklist as a valid tool for assessing the methodological quality of a systematic review. As the relevant literature has been identified and reviewed, the discoveries will be tested in a checklist concept in order to evaluate the applicability and the concepts will then be compared. For example, repeated patterns, categories and properties will summarized to construct an exploratory evaluation checklist; a meta-analysis tool proposal to answer the research question. The created checklist in chapter 6 concept also covers the data extraction and synthesis phases by summarizing the discoveries and providing a tool for quality appraisal through cloud security-specific use cases to tie the research outcome into the research question and problem.

2.1 Research problems

The research problems of this study are based on the observation that while several cloud computing-specific security auditing frameworks answer to the cloud service customers trust management needs, the meta-evaluation process[3] for the frameworks hasn't been well studied or documented. As the core requirement for trust management for security may be fulfilled through audits and assessments, the frameworks, especially cloud specific, do not include guidelines or reference quality assurance processes for evaluating the evidence in the audit process. Flick (2011, p. 82) emphasizes is his publication on research methodology that before deciding on the research problem, it should be assessed that existing knowledge about the problem is sufficiently available and if the problem can be studied empirically. The iterated final research problem applies for both of these prerequisites. The problem isn't simple or self-explanatory, so the research problem has hereby been split into two main problems:

1) Common security certification schemes do provide well-thought requirements and controls, but the evidence evaluation is left to professional judgement of the auditor.

[3] According to Stufflebeam (2011, p.99), good evaluation requires that evaluation efforts are evaluated. This process is often referred to as meta-evaluation.

2) Auditors and auditees do not have often tools for evaluating the sufficiency of evidence, especially for cloud computing environment, but must rely on common sense and unsuitable guidelines from beyond cloud security in absence of a purpose-built evidence quality assessment tool.

As discussed in the previous subchapter, the problems are approached through systematic literature review methodology. In systematic literature review, as for several other types of qualitative research methods, the priority is given to the data and the field being studied over theoretical assumptions. The theories are instead being discovered and formulated by conducting research within the field and rely on the empirical data collected in the process.

In performing this type of qualitative research, the theory cannot be hypothesized or assumed in detail before extensive data collection and analysis. The chosen approach is suitable for this specific research case because as the research problems are set, no suitable theory is directly available for cloud security evidence evaluation. According to Flick (p. 55), in case the research emphasis and focus is on the interpretation of data, the question of which method to use collecting data becomes minor. Thus, the research problems are to be solved by collecting relevant data by reviewing both scientific and professional literature and publications on the subject, the material collection process in further detailed in subchapter 2.3.

2.2 Research question

According to Flick (2011, p. 84), for the success of any study, it is important to limit the chosen research problem to a research question that is manageable. The elements of the question defined to be able to formulate a manageable research question with a reasonable scope. These elements are described and reasoned in this subchapter. Also, in order to be able to answer to the research question through systematic literature review methodology, the research question has been iterated and narrowed down to a clear and concise form. This iteration was done by answering to the key research guideline questions by Flick. The guideline requirements that the research must meet are relevance, clarity, background knowledge, feasibility, scope, quality, neutrality and ethics. No restrictions were noticed in answering to these demands by conducting the research with the finalized research question. (Flick 2011, p. 99) To keep the scope reasonable and the findings reportable, the finalized research question has been set as follows:

- *What quality requirements can be applied on cloud security audit evidence?*

The answer to the research question research will be found through extensive cross-scientific research on the topics of evidence in general, evidence

> qualities, evaluation and sufficiency parameters. Common cloud computing-specific security auditing frameworks will be reviewed to gain an understanding into cloud-specific security management and auditing mindset. Scientific and professional material will then be compared in order to find similarities. If overlapping qualities are found, the universal qualities will be used to create a theory that. The universal qualities will then be reviewed against requirements from a selected cloud security framework in order to test the applicability in cloud security auditing.

In case an answer can be found by using systematic literature review methodology, the research will be beneficial for an organization as an auditee planning for an external security audit on a cloud-based information system , as knowing how to create compliant processes and to document them correctly will improve the chances of passing the audit and getting ultimately certified. The findings may also be beneficial for an independent internal auditor or an external third-party auditor in assessing cloud security as the evidence may often be difficult to judge in absence of quality guidelines from the security framework.

2.3 Material collection

This subchapter describes the research material collection processes and methods used in the research. According to Templier & Paré (2015, p. 118), in narrative-type systematic literature review the material should cover a representative set of the literature by including a sample that is illustrative of the larger population. Therefore, the research material consists of three main types of References, in order of significance: (1) Scientific research papers and publications (2) Literature and articles on auditing, evidence evaluation, cloud computing, security management systems and (3) Cloud computing-specific security compliance frameworks suitable for auditing. As cloud computing is still relatively new technology, no publication release time limit was set on the subject; all suitable publications on the subject were accepted. The material search was conducted in both libraries at the University of Jyväskylä and the University of Helsinki and online. The online material search was limited on free sources only, through the University of Jyväskylä's online library database, JYKDOK. Common search engines such as Google Scholar were also used. As per Okoli's and Schabram's (2010, p. 15) SRL-models step two, "protocol and training" requires, the study has to follow a strict protocol that is "a plan that describes the conduct of a proposed systematic literature review". The protocol of this study follows the guidelines and principles set in this chapter. For the online material collection from the aforementioned sources, the following key search terms were used:

- Scientific evidence
- Evidence evaluation
- Evidence quality

- Auditing
- Assurance process
- Security auditing
- Cloud security standard
- Cloud security framework
- Evidence collection
- Meta-evaluation

Okoli's and Schabram's SLR-process' step four is practical screen. By following the protocol and conducting searches with the predefined criterion, the practicality of the selected materials and search terminology scope can be screened. The search online with the selected search words yielded the following amount of results:

Search word	JYKDOK	Google Scholar
Scientific evidence	952	~3 350 000
Evidence evaluation	951	~2 650 000
Auditing	626	~1 040 000
Assurance process	204	~2 650 000
Security auditing	118	~481 000
Cloud security standard	58	~1 700 000
Cloud security framework	198	~1 290 000
Meta-evaluation	2470	~19 900

Table 1: Online material collection, search words

The listed keywords were also used in combinations and variations such as "audit process" and "security auditing frameworks". The selected research method, systematic literature review is based on the assumption that all relevant studies are included in the review (Jesson, Matheson & Lacey, 2013, p. 105). In this case, as the subject of cloud computing security is relatively new and recognizing the fact that information technology produces new research constantly, including all of the research would be impossible with taking the amount of found References into consideration. Therefore, countless References found with the key search terms were skimmed, and only relevant, applicable and free-of-charge material was accepted. In judging the sufficiency of the material, applicability in cloud computing context was emphasized.

As the research includes also cloud security framework reviews, the emphasis was respectively on frameworks that were available completely free of charge, such as CSA CCM and PiTuKri. No restrictions were set for the reviewed cloud security frameworks, as they were few in number by the time of conducting the research. However, some of the security frameworks, such as the ISO/IEC standards mentioned in this research were available through purchase only, so references to such examples were kept to minimum if only previews were available for free. As the evidence for the cloud security frameworks available at the time of conducting this study consists of qualitative-type information and information collection methods, in the context of this study quantitative evidence evaluation research will be excluded.

The theoretical background of the research was brought together by combining the fore mentioned theoretical, scientific research sources with practical sources such as security frameworks in order to provide a link from the discoveries into a practical application concept. The research was conducted on literature and published material only, leaving out interviews and other empirical References. This decision was based on the research problem 2: "*Auditors and auditees do not have often tools for evaluating the sufficiency of evidence, especially for cloud computing environment, but have to rely on common sense and unsuitable guidelines from beyond cloud security in absence of a purpose-built evidence quality assessment tool.*" As a few professional auditors and compliance specialists both on private and public sectors were casually approached through the researcher's professional connections with the research topic, the answer was common: There are no thorough or purpose-built guidelines available, the evidence qualities are evaluated case-by-case.

The reason for excluding auditor interviews in this research is further detailed in Westhausen's publication on cognitive biases in internal auditing (2019, pp. 45-47). The author claims that auditors are prone to cognitive biases, caused by information asymmetries among other causes, which may affect the auditor's decision making. Lack of evidence evaluation guidelines in cloud security frameworks can be seen as a cause of information asymmetry as the auditors are forced to formulate their personal mindsets on professional judgement of audit evidence. It was thus decided that the research would have to be carried out based on published articles, with the main focus in peer-reviewed scientific material to avoid these personal cognitive biases. Cognitive bias in auditing is further discussed in subchapter 5.4. It was acknowledged that the chosen approach would most likely yield different, a more theoretical than practical outcome, however the emerged theory would be briefly tested in the form of a concept tool. The material collection process was found to be suitable for this type of research resulting in prototype-phase tool proposals. This research could be seen as a precursor for an in-depth research resulting in a finished evaluation tool.

2.4 The need for evidence evaluation in cloud security compliance

A way to view information systems, including cloud platforms security compliance is through trust management. Thampi, Bhargava & Atrey (2014) have presented a several definitions for trust in their book Managing trust in cyberspace that are as follows:

- *It is the percentage in which one party meets the behavior as expected by the other*

- *It is the degree in which the first party behaves exactly as it was expected from the second party. If the degree is high, it represents a higher trust on the first party by the second one.*
- *It is represented in the form of a trust model. It can also be referred to as confidence.*
- *It is generally a binary relationship between two entities. It is established between two entities based on certain common attributes over which the confidence is analyzed and measured.*

It can be reasoned from the recent rapid appearance of cloud computing security frameworks and certification schemes that there indeed is a need in trust management between cloud customers and vendors. According to Gul, ur Rehman and Islam (2011, p. 147), data confidentiality, integrity, authentication and availability are the major concerns in cloud adoption. This can again be summarized in the search for a secure cloud computing platform in which the organizations and other potential cloud service customers can trust to keep their valuable data 's confidentiality, integrity and availability maintained by an external entity that is the cloud service provider. From the cloud service provider's point of view, attaining a certification or an attestation from an independent third party of the security posture of the cloud service offered again servers as a key tool in managing the trust between the vendor and the customer. Attaining this key tool that is a certification or 3rd party attestation however is a process that requires certain internal trust management as well, that becomes evident in the compliance requirement evidence evaluation.

As cloud security auditing and assurance processes includes evidence collection for both technical and non-technical controls (Anantha, 2002, p. 2) the required evidence types can vary from policy documents to network scan samples or vulnerability assessment tool outputs. Therefore, all collected evidence must be evaluated separately and the type of evidence dictates which evaluation metrics are applicable respectively. For example, when reviewing an auditee's security policy an auditor must take into consideration whether the documentation is up to date or outdated, while when reviewing a network packet capture sample, the sufficiency of the sample size must be evaluated. Usually, these kind of evaluation checklists or requirements are not included in the standards and schemes themselves. Hence the sufficiency and appropriateness of provided or collected evidence is up to the auditor to evaluate.

A relevant modern phenomenon in information security auditing is the emergence of audit automation; technical solutions to collect real-time evidence from IT infrastructure against select control objectives. This allows for compliance information on demand at any time. The automation is usually conducted with software that acquires evidence from selected References. The applicable References for this are often security information and event management system's (SIEM) logs and selected logs from the cloud services, such as AWS's or Azure's management interfaces.

For example, a full scope of ISO/IEC 27001:2013 information security framework includes over 130 technical and non-technical control objectives, which means a huge work effort for both the auditor and the auditee. Montesino etc. (2011. p. 3) state in their research that 37 of the controls in ISO/IEC 27001:2013 can be automated, which can be a great time saver. The audit automation provide evidence on technical controls only, which often are the most time-consuming for the auditor to collect manually, as opposed to document reviews etc. provided by the auditee. However, even though with the latest technology the evidence collection process can be automated partially, the final evaluation of the sufficiency of the evidence is still the auditor's responsibility.

According to ENISA's whitepaper on cloud standards and security (2014, p. 12) Cloud Services are often more common than traditional legacy IT deployments. Due to this increase in popularity, implementing a cloud-specific security framework is getting more and more crucial for cloud service providers and customers. At the same time, the concept of evidence for compliance should become an increasingly interesting objective for scientific research as it has been widely neglected so far in IT-related research, however remotely applicable research on meta-evaluation has been published, however these studies have been aimed at scientific research rather than professional auditing.

Evidence evaluation in general can be seen as meta-evaluation, in other words evaluating the quality of the evidence itself that is used for evaluating an objective, such as the information collected during a security audit. Therefore, an evidence evaluation framework for any type of auditing is in essence a meta-evaluation framework. Caracelli & Cooksy (2013, p. 97) recognize the issue of the lack of common criteria in qualitative studies in general. According to the authors, even though there is an abundance of checklists for evaluation, little work has been done to evaluate the checklists themselves. Also pointed out by the authors, the challenge with the checklists is how the quality criteria from different research traditions can be operationalized.

In the context of this study, the fore mentioned issue is apparent; in information systems and cloud security auditing, the frameworks are built on reviewing information from a broad spectrum of different domains ranging from administrative to technical subject matters. Caracelli and Cooksy (p. 102) summarize the issue as follows: "Transparent criteria and methods are a necessary condition for being considered in evidence-based reviews whether in a qualitative synthesis or as part of expanding the frame of reference in evidence reviews emphasizing quantitative designs.

2.5 Previous related research

The definition of evidence regarding compliance in information security management frameworks has not been widely studied scientifically so far, especially in cloud security context. However, cloud security as well as information security auditing in general has been researched from various administrative and technical viewpoints since the emergence of cloud computing. Takabi etc. (2010) have researched the Security and Privacy challenges in Cloud Computing with a very generalist approach, resulting in 18 different issues an organization must manage when operating in cloud environment.

Out of the eighteen mentioned findings, five are unique to Cloud Security. The unique findings were Outsourcing Data and Applications, Extensibility and Shared Responsibility, Service-Level Agreements, Heterogeneity in clouds, Virtualization and Hypervisors and *Compliance and Regulations*. According to the research, Compliance and Regulations in cloud can raise multiple jurisdiction issues with regard to protection requirements and enforcement mechanisms as cloud services must be accessible from anywhere and at any time. (Takabi etc., 2010. p. 26)

Siponen and Willison (2009) have conducted a study on the problems and solutions concerning information security management standards. Cloud-specific security management frameworks didn't exist at the time, and anyway Siponen and Willison (2009) focused on the information security management standards. They recognized that the standards were validated by appeal to common practice and authority, and that this validation was not a sound basis for important international information security guidelines. In other words, appeal to common practice was found to be fallible and not paying attention to specific needs of a system. These conclusions (by Siponen & Willison 2009) seem to apply in cloud-specific standards as they lack specific guidelines, such as evidence quality requirements.

Anantha (2002) has stated in his research article that the main challenge in information security audit effectively.is that the audit process involves collecting in depth technical evidence. The findings then should be translated into vulnerabilities and actual business impacts that can be communicated to non-technical management. The conclusion can be seen applicable in cloud security as well.

While the structure and processes as well as different details of auditing have been scientifically researched in different contexts for decades, the first information technology security audit researches can be found from as far as 2005. It was in the year 2005 that the first version of ISO/IEC 27001 standard *"Information technology – Security techniques – Information security management systems – Requirements"* was published and was one of the first widely-adopted information security standards, still being the most commonly applied today. Auditing and audit evidence-related research however can be found from decades back, mostly from scientific topics outside of information technology.

According to European Cyber Security Organization, currently there are eight (8) standards and certification schemes focusing specifically on cloud service providers. (*ECSO State of the art syllabus, 2.2, July 2017 p. 9*)
The standards and schemes mentioned are the following:

- Cloud Security Alliance Cloud Controls Matrix
- Code of Practice for Cloud Service Providers
- EuroCloud StarAudit Certification
- ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services)

- ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- TüV Rheinland Cloud Security Certification
- ANSSI SecNumCloud
- Cloud Computing Compliance Controls Catalogue (C5)

The security controls studied and/or referred to in chapters 3 and 6 are derived from the above-mentioned standards excluding ANSSI SecNumCloud and Cloud Computing Compliance Controls Catalogue (C5). The exclusion was made with global applicability in mind, SecNumCloud and C5 are based at least partially in their countries of origin's local legislation and/or the Reference materials were not available in English.

In addition to the aforementioned cloud security frameworks this study includes the PiTuKri (Pilviturvallisuuden auditointikriteeristö), a cloud security-specific auditing criterion published by the Finnish National Communications Security Authority (NCSA-FI) in May 2019. While not globally applicable as PiTuKri has been built from Finnish cloud service customer's point of view, the framework has been built on various other universally accepted standards, such as ISO/IEC 27017 and CSA CCM, adding the European General Data Protection Regulation's requirements in the framework. PiTuKri also was the latest cloud security framework that had been published by the time of writing this study, so it makes for an interesting reference point in comparison to the longer running and more established frameworks such as the CSA CCM.

3 CLOUD COMPUTING AND SECURITY COMPLIANCE

The key concepts defined in this chapter for the research are cloud computing security compliance, Security audit and assurance process, evidence collection methods, evidence evaluation and evidence requirements. In order to understand the terms and definitions, the concept of c*ompliance* must be understood. According to Ratsula (2016, p. 67), compliance covers all rules and regulations an organization must comply with. In addition to legally mandatory regulation, an organization can define its own compliance goals according to its values. Carstensen, Morgenthal and Golden (2012, p. 259) explain that typical activities performed by a compliance function include the following:

- Developing and administering policies and procedures to comply with legal and regulatory requirements.;
- Developing and administering training programmes for employees and contractors covering regulatory requirements;
- Assisting employees ongoing legal and regulatory requirements;
- Monitoring of systems for adherence and breach of organizational policies;
- Assisting (and possibly leading) any investigations and breaches of legal and regulatory requirements;
- Reporting and engaging with executives on the compliance posture of the organization;
- Liaising with regulators in relation to regulatory matters.

In addition, as stated in the book, compliance may also be responsible for the coordination of activities related to the collection of evidence and other materials required in the event of an investigation.

Ratsula (2016, p. 12) also states that the main principle of organizational compliance is to ensure that the organization operates according to laws and regulations. It is no longer acceptable that the operating procedures cover only the minimum legal requirements, but the organization has to follow also moral and ethical requirements set by external entities. Every organization has compliance risks regardless of size and industry. A non-compliance or a compliance breach in general means that the organization operates against set expectations and requirements. (p. 13) Even though moral and ethical questions make up a big part of organizational compliance, these qualities are difficult to measure, thus this study is focused in compliance through third-party security frameworks.

According to Fitzgerald (2012, p. 8) compliance is supposed to ensure that due diligence has been exercised within an organization to meet the government regulations for security practices. Additionally, Fitzgerald states that there are several ways to achieve compliance as the regulators have created the requirements often in high level. Although the lower level implementations on how the solutions must be conducted in detailed platforms to achieve compliance can be very specific and not stated in the requirement itself. Cloud security is a good example of such low-level detailed security objective; as mentioned in subtitle 2.3.2, cloud security includes several unique security objectives not found in other security domains.

Looking back into Ratsula's publication (p. 13), the realization of compliance risks may inflict various forms of either direct or indirect damage on the organization. Such damage may include the following:

- Damage on reputation and public image
- Negative impact on stock share price and company value
- Investor's withdrawal and decrease in the availability of funding
- Loss of employee loyalty and commitment
- Loss of customers
- Loss of operating permits or business prohibition
- Financial impacts such as fines, damage liabilities and loss of income
- The realization of the board of directors and management's legal responsibilities
- Loss in organizational focus as crisis management takes over business
- Loss of business prerequisites or end of business

All the fore mentioned damage cases are extremely severe in today's business environment, including cloud computing business. In addition, the damage cases apply on security compliance, perhaps even more so than other compliance requirements. Therefore, this finding further underlines the need of transparency in corporate operations supported by a well built and thorough information security management system, that again can be concretized in a certification issued by a third party, such as an accredited certification body.

To follow up on the importance on IT compliance, Ratsula further elaborates the risks on securing immaterial property or intellectual property (IPR) in her publication (p. 125). Information is one of the most important properties for an organization. Information security includes the encryption of valuable data and preventing unauthorized use of devices including mobile. Agreements and contracts with third-party stakeholders should be solid so that there won't be any disputes on responsibilities in case an information risk realizes. This is crucial especially in cloud computing, as the security responsibilities are always spilt between the customer and provider as presented in subchapter 2.3.3 of this study. Ratsula has narrowed the key information risk issues in compliance to the following (p. 126):

- Information security management – How is the organizational information security controlled and managed?
- Intellectual property rights (IPR) – Is the necessary intellectual property adequately secured?
- Information confidentiality, integrity and availability – How is the authorization for critical and sensitive information organized? How is the

availability ensured? Is access managed? Are passwords adequate? Is the information integrity secured when transferring or handling data to avoid corruption?

- Data collection and sharing with third parties – What data is being collected and how? Is the data transfer between the stakeholders adequately secured? Do we possess proper clarification on the external parties' data handling procedures and controls?
- Information classification – Does the organization have a classification policy in place for sensitive and valuable data?
- Training – Has the personnel been properly trained to handle sensitive and valuable data?
- Information disposal or anonymization – How is the disposal or anonymization organized when the data lifecycle comes to an end? Has security been considered in the disposal of devices containing sensitive or valuable data?
- Personnel turnover – Has the risk of sensitive data leak been considered when terminating an employment?
- Information security – How is the IT-infrastructure, software and device security controlled?
- Privacy – Have the systems and processes containing personally identifiable information been adequately controlled?

As further studied in subchapter 3.1, Types and domains of requirements and controls, all of these general-level information risk compliance issues are addressed in the cloud security specific frameworks, either in complete requirement domains or separate requirements within domain. It can therefore be summarized that the cloud computing shares a spectrum of risks with general-level IT-security mindset, however in cloud computing there are certain unique risk domains to be addressed. Gul, ur Rehman and Islam (2011, p. 147) recognize that cloud computing was still in its stage of infancy at the time of research, and common, interoperable and cloud-specific auditing mechanisms must be designed to maintain trust and transparency within the cloud environment. The emergence of cloud-specific security frameworks has since filled this void to some extent, as covered in chapter 3.2

It should be noted that compliance ongoing processes include several challenges. According to Marchetti (2012, pp. 132-133), a few examples of such challenges can be that the majority of compliance activity time is spent on remediation, leaving little time to develop a long-term compliance plan or create more efficient processes. The cost of compliance can in some cases grow due to a substantial rise in material weakness disclosures and restatements as well as an increase in audit fees. In cloud computing security compliance, this challenge could be faced if the auditee fails to provide sound audit evidence, leading to extension of the audit process. Finally, many organizations do not have an appropriate infrastructure and implementation plan sufficient to sustain compliance, mitigate risks and cost reduction. Therefore, according to Marchetti, any discussion on sustaining compliance should be focused on developing an integrated plan that facilitates cost reduction or minimization, increasing reliability and confidence with financial results and delivering benefits and value.

The last definition of compliance in this chapter is provided by Carstensen, Morgenthal and Golden (2012, p. 257) in their book on risk assessment in cloud computing, taking a cloud-specific point of view. The authors define compliance in general as "*conforming to a rule, such as a specification, policy, standard or law*" – all requirements that are typically external to the organization. According to the authors, often in real-life situations and environments the fore mentioned definition may be expanded and tends to additional objectives. These additional objectives

3.1 Abbreviations and key terminology

The following table includes the abbreviations and definitions used throughout the research.

Abbreviation/Term	Definition
AICPA	American Institute of Certified Public Accountants Reference: https://www.aicpa.org/
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. Reference: ISO/IEC 19011:2011, 3.1
Audit Conclusion	Outcome of an audit, after consideration of the audit objectives and the audit findings. Reference: ISO 9000:2005, definition 3.9.5
Auditee	Organization being audited. Reference: ISO 9000:2005, definition 3.9.8
Auditor	Person who conducts an audit. Reference: ISO/IEC 19011:2011, definition 3.8
BSI C5	The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) Cloud Computing Compliance Controls Catalogue.
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.

	Reference: https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements. Reference: https://www.iso.org/certification.html
CSA	Cloud Security Alliance Reference: https://cloudsecurityalliance.org/
CSC	Cloud service customer
CSP	Cloud service provider
Control Objective	Statement describing what is to be achieved as a result of implementing controls Reference: ISO/IEC 27000: 2016
GAAS	Generally Accepted Auditing Standards by AICPA Reference: https://www.aicpa.org/Research /Standards/AuditAttest/DownloadableDocuments/AU-00150.pdf
IaaS	Infrastructure as a Service
Information Security	Preservation of confidentiality, integrity and availability of information Reference: ISO/IEC 27000:2016
IPR	Intellectual Property Rights
IRM	Information Risk Management
ISMS	Information Security Management System
ISO	International Organization for Standardization Reference: https://www.iso.org/home.html
ISO 19011	ISO 19011:2018 Guidelines for auditing management systems Reference: https://www.iso.org/standard/70017.html
ISO/IEC 27001	ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements Reference: https://www.iso.org/isoiec-27001-information-security.html
ISO/IEC 27017	ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

	Reference: https://www.iso.org/standard/43757.html
Management system	System to establish policy and objectives to achieve those policies. Reference: ISO 9000:2005, definition 3.2.2
NCSC-FI	Finnish National Communications Security Authority
Nonconformity	Non-fulfilment of a requirement Reference: ISO 9000:2005, definition 3.6.2
SaaS	Software as a Service
SIEM	Security Incident and Event Management system (also Security Information and Event Management system)
SLA	Service Level Agreement
SME	Subject Matter Expert
SOC	Security Operations Center
PaaS	Platform as a Service
PiTuKri	Cloud Security Assessment Framework, NCSA-FI, Traficom, Finland. Reference: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf
Requirement	A need or expectation that is stated in a standard, law, regulation or other documented information, generally implied (i.e. it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied), or obligatory (usually stated in laws and regulations) Reference: ISO/IEC 27000:2016 Overview and vocabulary

Table 2: Abbreviations and key terminology

3.2 Cloud computing security certification schemes

Ryoo, Rizvi, Aiken and Kissell (2014, p. 70) have concluded in their research article about cloud security auditing challenges that effective cloud security auditors must be familiar with cloud computing terminology and have a working knowledge of a cloud system’s constitution and delivery method. A good cloud security audit should question whether a cloud security provider provides a solid balance between security controls and end user access. This is especially difficult as cloud computing systems are typically based in large datacenters, possibly managed by a third-party subcontractor. This setup might end up with the customer having very little to no information on which parties handle the data and where exactly on the system it's stored. To expose the risks associated with this setting, an external audit can be conducted to increase transparency. In case the audit is conducted against a recognized security framework, the auditee can often apply for a security certification if found nonconformities are fixed after the audit process.

When a cloud service provider (CSP) is looking to get certified against, for example ISO/IEC 27001 certificate of compliance, the CSP is in the role of an auditee. The auditee provides the auditor, an accredited certification body with evidence on how the requirements/controls of the applied standards have been met. The auditor then proceeds to review whether the evidence of compliance, collected by the auditor or provided by the customer is sufficient and appropriate to attest for compliance or non-compliance for a specific control. Additionally, the definition for audit, as described in ISO/IEC 19011:2011, chapter 3.1 is *"Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled"*.

Carstensen, Morgenthal and Golden (2012, p. 261) state in their book that cloud computing has brought forth opportunities that have thought to be tough to provide assurance, transparency and accountability on before cloud computing's emergence. As cloud platforms are mostly consolidated and centralized, assurance of the services has thus become possible, enabling improved transparency. According to Carstensen, Morgenthal and Golden (2012, p. 262) cloud technology and services are constantly developing and adapting at a rapid rate, it is likely that compliance will not be keeping up with the development. The greatest challenges in cloud computing according to the publication are international data flows, data ownership, monitoring, logging and reporting among many others.

According to Salazar's research paper (2016, p. 16), by auditing and implementing frameworks, most of breaches and risks can be reduced through the utilization of cloud provider environments. A certification is an official proof of compliance against a framework with an expiration date, for example one year for ISO27001 certification. An attestation on the other hand is an unofficial statement that the requirements for compliance have been met. Attestation has been defined in ISO 17000:2004, 5.2 as *"An issue of 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"*.

European Cyber Security organization (ECSO) has listed 101 recognized standards for cyber security in their publication *"Overview of existing Cybersecurity standards and certification schemes"* (December 2017). Of the 101 schemes, 8 are intended to be used for evaluation of cloud service provider's security maturity. Out of the eight CSP-specific schemes, six are internationally applicable, while two are more nationally specified, taking the national legal requirements in consideration respectively.

ENISA's overview of existing relevant standards for cloud security from 2014 lists 16 relevant standards of which a majority are purely technical standards such as network protocols and five are frameworks or certification schemes. However, the frameworks listed are not completely cloud-specific excluding CSA CCM. Compared to ECSO's listing published three years after ENISA's mapping, it can be noticed that more cloud-specific schemes and frameworks are entering the market. This is an indicator of increasing need for security assurance in cloud computing. A good example of a modern security framework not covered in ECSO's listing would be *PiTuKri* framework published published by the Finnish National Communications Security Authority (NCSA-FI) in May 2019, further covered in this study.

An advanced organization should have nominated a compliance officer whose responsibility is to supervise the compliance processes, including information security and cloud security compliance. According to Ratsula (2016, p. 212-213), common methods for a compliance officer collecting evidence for evaluation may include physical visits to the organization's premises and unofficial discussions and interviews crossing the management levels. Different compliance-themed questionnaires may be used to collect evidence or compliance-themed questionnaires may be added to existing employee questionnaires. Documentation reviews and trend analyzes are also viable tools for a compliance officer to collect up-to-date information on the state of the compliance program. The last two methods mentioned by Ratsula are the investigation of suspected internal or external compliance violations and the exit interviews of employees leaving the company.

As a single certification or a framework is often a part of an organization's compliance program that often includes multiple schemes that must be maintained, the compliance officer must frequently evaluate the efficiency of the program. According to Ratsula (p. 213) the compliance officer assessing the effectiveness of a compliance program should look for an answer to multiple evaluation-related questions. An answer should be provided to the following questions:

- How is the success of the compliance program evaluated, how is the information collected?
- What are the major domains of the compliance risks in the organization and how are they supervised and audited?
- Are the audit plans risk-based?
- How is continuous monitoring conducted?
- How are the managers performing on their supervising duties?
- What about the executive management?
- What kind of independent supervision is conducted at our company?
- Does it provide reliable enough information on the state of the compliance?
- What other assurance services does our company have?
- How is the co-operation coordinated to prevent overlap and ensure sufficient coverage?

Understanding this grand scheme of compliance viewpoints through the questions presented above provides the mindset required in building any compliant system or a process, including cloud computing services and platforms. It should however be emphasized, that especially in security management, compliance isn't an end-all solution to solve all of the security issues a system or an organization may face. As per Vladimirov, Gavrilenko and Michajlowski's book (2014, p. 121), information security-related standards are somewhat paradoxical. This is apparent as in essence and on paper, the regulations and standards, including frameworks may be very lax in the practical implementations and their assessments. According to Vladimirov, Gavrilenko and Michajlowski, the main reason for this "looseness" is that the standards are too general in nature, meaning that they might not take system-specific details into consideration sufficiently. On the other hand, some of the standards and regulations may only address limited areas of specific systems indirectly, such as general security and management system auditing schemes, ISO27001 series and the Finnish KATAKRI for example. Auditing a cloud service or platform against these frameworks would leave out a lot of critical cloud-specific objectives, so choosing the right tool, a security framework is this context is critical for success and avoiding missing the objective.

3.3 Cloud-specific security objectives

An often-heard phrase in the information security community goes *"There is no cloud, it's just someone else's computer"*. Thus, it could be over-simplified that cloud platforms are just as traditional on-premise information technology operating environments, only with the hardware and a vast part of the responsibilities outsourced. However, the mere existence of security frameworks focused on cloud computing specifically gives away the fact that cloud computing cannot be approached or evaluated with the same qualities as old on-premise IT environments that cloud platforms are now rapidly overtaking in popularity in the corporate domain.

Ryoo, Rizvi, Aiken and Kissell (2013, p. 69) state that cloud computing comes with its own set of security challenges. A cloud service provider should keep data safe from security threats while giving clients access from anywhere through internet service. Additionally, the client organization must verify that the cloud computing enterprise contributes to its business goals, objectives, and future needs. The authors recognize that while both conventional IT security auditing and cloud security auditing share many concerns, a cloud security audit must address unique problems that are typically not handled in traditional IT security audits.

Carstensen, Morgenthal and Golden (2012, p. 263) state in their book that as with traditional in-house data centers, organizations using cloud services are required to be compliant with required frameworks. In addition to traditional in-house computing, the organizations as customers (CSC) should be aware or regulatory challenges when considering a specific cloud service or a service provider (CSP). Cross-border data flows should be controlled, or not used at all if compliance or legal regulations do not permit it. Responsibilities should be clearly separated and outlined between the cloud service provider (CSP) and the customer (CSC). Possible third-party providers regarding the service should be recognized and assessed accordingly. The service provider should be able to prove compliance, clear reporting, adherence to best practices and evidence to customers where required to ensure transparency. According to Carstensen, Morgenthal and Golden, the above-mentioned details should be revised with current compliance practices when a customer is considering transition to a specific cloud service.

To further comprehend the cloud-specific security objectives, the auditor, client and service provider should understand the basics of the most common cloud service models. In ENISA's publication (2014, p. 2) the service models are divided into three main categories. The categories are: Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS services provide the customer with storage or computing resources that are accessible online. PaaS delivers the customer a platform to run selected applications on, such as web applications or scripts. SaaS is the most complete of the three service models, providing the client with fully functional software or applications usually accessed via browser or web client.

In addition to the services, the provider is responsible of the assets required to run the services, such as the facilities and the organization. Facilities include the data centers, servers and network, while the organization cover the human resources and processes required to maintain the services. The service models with respective customers and service providers responsibilities are described in the following figure:

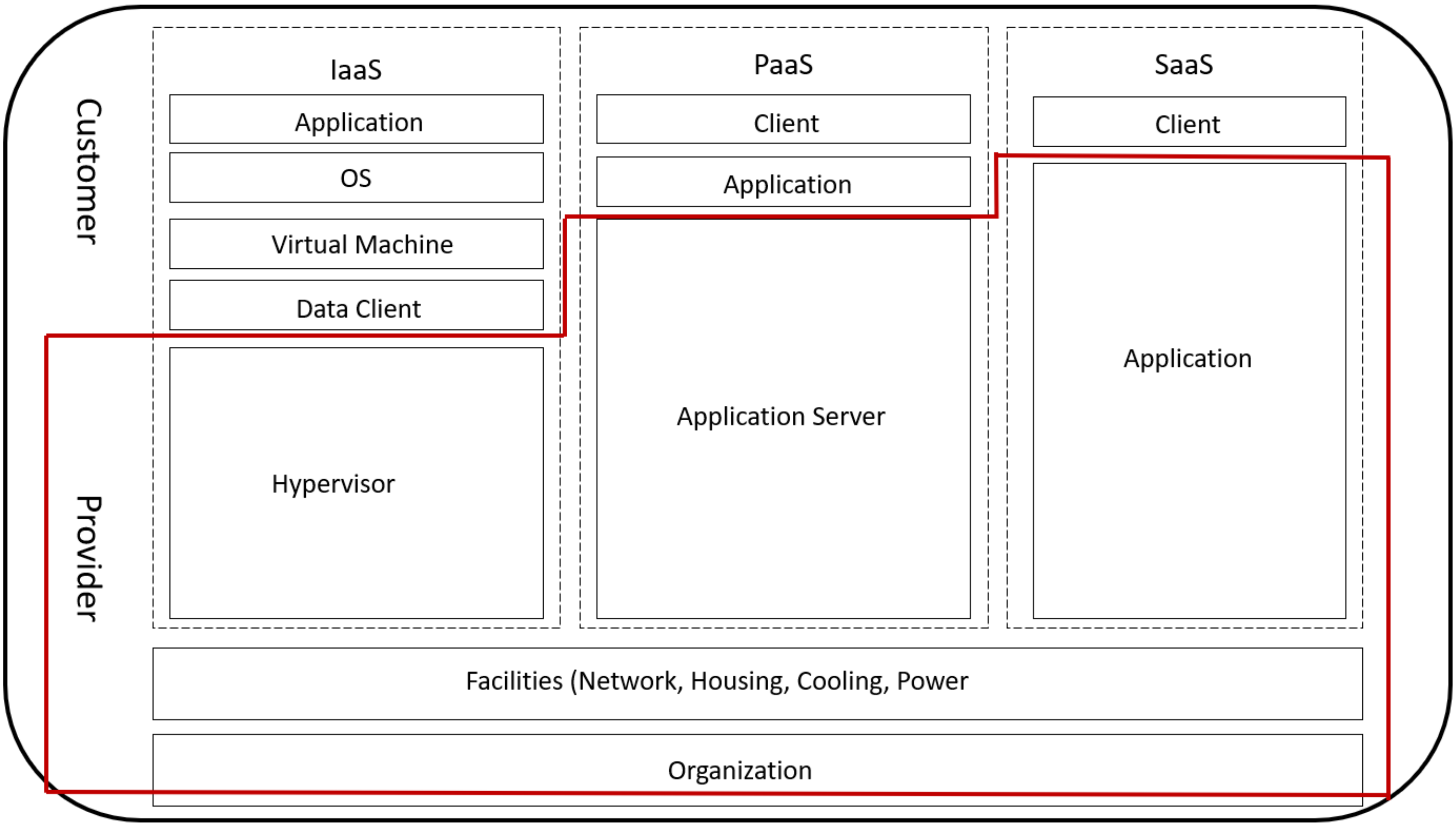


Figure 2: Security responsibilities in different types of cloud services. (ENISA, Cloud Standards and Security, 2014, p. 2)

In cloud security auditing, traditional audit objectives and domains found in security frameworks are often as applicable as they would be in a traditional or legacy IT infrastructure. Yet there are crucial objectives that traditional security frameworks may not consider that are applicable for cloud infrastructure specifically. These unique audit objectives are based on the decentralization of security responsibilities in cloud infrastructures. In other words, cloud infrastructures are often borderless in nature, meaning that the user and the physical location of the service, such as data center may reside in different countries and jurisdictions.

The scope of the audit may vary from the viewpoint for who the audit is conducted on, the service provider or the client. ENISA states in their publication (2014, p. 12) that standardization makes it easier for cloud customers to compare and evaluate cloud services. According to Salazar's research paper (2016, p. 4) the cloud security responsibilities are distributed between the service provider (CSP) and client (CSC) by the type of the of service as follows:

Solution	Client Responsibility	CSP Responsibility
	Configuration of log	**Data**

Software as a Service (SaaS)		**Applications**
Platform as a Service (PaaS)	**Logs from own apps**	**System Management**
Infrastructure as a Service (IaaS)	**Local surveillance**	**Network**
	Application logs	**Hardware, host**
	OS logs	**Procedures etc.**

Table 3: Cloud security responsibilities (Modified from Salazar, 2016, p. 4)

When auditing a cloud service with a cloud security-specific framework, such as CSA Cloud Controls Matrix or ISO/IEC 27017:2015, the main focus of the audit is in the objectives under CSP's responsibility. However, risk-based approach may extend the audit scope to client's responsibility objects if risk assessment documentation includes risks controllable only on client's (CSC) side. Common industry-leading security frameworks, such as ISO/IEC 27001 and KATAKRI include often both CSC and CSP involvement when applied with full scope of requirements. In general, ISMS audit schemes are not restricted to the auditee organization only, but often include possible cloud service provider's responsibilities as well where applicable.

3.4 Audit and assurance process

The goal of an audit and assurance process in information security is to assess whether the requirements for risk management controls have been met. ISO/IEC 27000:2016 standard defines audit as *"systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled"*. The evidence collection process in compliance assessments is conducted by an auditor, either an internal auditor or an external certification body. Usually evidence must be produced from both technical and non-technical domains to be reviewed against respective requirements.

According to S. Anantha (2002), the objective of information security audit is to review and provide feedback, assurances and suggestions. The above-mentioned procedures are conducted to ensure that the following three core principles for data are met:

- Confidentiality – Information is only disclosed to those who have a need to see and use it.
- Integrity – Information is accurate and up to date, unauthorized modification of information is prohibited.
- Availability – Crucial information is available and accessible when required.

As an information system is not only a technical definition, but a combination of people, processes and technologies involved, IS audit must cover a wide area of domains ranging from purely technical to physical subjects. For example, the Cloud Security Alliance's Cloud Controls Matrix v3.0.1 covers 13 different domains. The domains cover a range from technical objectives such as identity and access management to infrastructure & virtualization to physical and administrative subjects such as human resources policies and governance & risk management. Anantha (2002) states in his article that in a general level, the major elements if information security audit can be classified into the six following procedures:

- Physical and environmental review
- System administration review
- Application software review
- Network security review
- Business continuity review
- Data integrity review

While the six domains are still applicable today, modern information security frameworks usually include ten to twenty domains. For example, *KATAKRI 2015 – Information security audit tool for authorities* contains 9 control objectives, like domains. PCI-DSS v3.2 standard includes 12 control objectives respectively, while the widely adopted ISO27001:2013 framework contains 14 groups of control objectives. Even though an audit scheme contains a wide range of possible domains, it doesn't mean that all the domains apply to every audit as many modern audit frameworks can be conducted by a *risk-based approach.*

As not all risks are equal, and the likelihood and impact vary greatly from one audit objective to another, a risk assessment is conducted usually before or during the audit kick-off. A risk-based approach allows the audit to be focused on the most critical risks and avoid wasting time auditing irrelevant criteria that may not apply to the organization or system that's being audited for compliance. A risk-based audit includes a risk assessment that is conducted prior to the actual audit or at the audit planning phase. The risk assessment process results in an overview of the risks that the audit objective, an organization or an information system is facing and an evaluation of the risks. The evaluation should include at least the likelihood for the realization of the risk and a rough estimate for the severity of the impact. the likelihood and the impact add up to the risk criticality. However, there are a lot of ways and formulas to calculate evaluate risks with the principles being the common baseline.

According to Gantz (2013, p. 155) the validity review of the audit process itself is conducted by recording the types of information and used evidence collection methods. The complete audit process is then reviewed by the audit manager, or an accreditation body in case the auditor is required to report the findings to an external accreditation body. An example of such external supervising accreditation body in Finland would be the NCSC-FI, that keeps a record for all conducted ISO27001-audits in nationally, and for whom all ISO27001-accredited certification bodies have to provide the finished audit reports for the record.

When the main audit process comes to a close, the initial report is often reviewed with the auditee to assure the quality of the report. However, even though no guidance is available for cloud computing specifically, Wright (2016, pp. 134-136) has written about the review process of the audit report itself. This publication was written from general IT auditing's and Information Risk Management's (IRM) point of view. As this is an example of meta-review, the findings may be applicable for cloud security auditing as well. Wright (p. 134) states that once the audit work has been completed, it needs to be checked for factual accuracy and quality. This means that by confirming the factual accuracy with those being reviewed ensures that there are won't be any mismatches in facts later on or "embarrassments" as the author puts it. The report may lose credibility if the findings will later have to be altered or removed. According to the author, the discussion of findings yet again reduces the risk of "nasty" surprises the auditee and giving the auditee time to consider how to respond to possible noncompliance findings. In general, the reason for the quality review is to ensure that the objectives for the review have been met and that the working papers and report are aligned with the findings. The quality review process thus ensures the consistency of work and reporting.

According to Wright (2016, p. 135), after the audit report has been reviewed and issued, the management of the auditee organization should prepare an action plan to implement any findings, depending on their priority and urgency. The management should also ensure that the findings are shared with all the related organizational areas, such as details, units and specialists. There should be a mechanism implemented to review and report on the progress of the action plan. According to the author, using key performance indicators (KPI) is a good way to ensure that the actions have been implemented and continue to operate effectively. The key performance indicators may give an early warning of any changes so that the management can investigate root causes and take appropriate actions.

As Wright mentions in his book (p. 136), planning and the process of undertaking an information risk management (IRM) audit or assurance process is no different to a similar process in another context, except for the tools used and the form of analysis. Also shared by all audit processes according to the author is the need for a logical process for the review, and that the findings are supported by good analysis and working papers. Wright adds that the process is less important than the outcome which should be to provide a level of assurance that the risks are covered, or to provide recommendations as to how this can be achieved. A concept for a tool to assist in this logical process is presented in chapter 6.1.

As quality assurance of the audit is complete, resulting in a certificate if the organization or system has been found compliant against all requirements, it should still be remembered that compliance doesn't equal to complete security. As stated in Vladimirov, Gavrilenko and Michajlowski's book on Assessing Information Security (2014, p. 120, being fully compliant to any existing information security standard should never instill a false sense of security. Compliancy is at best only a step on a long way to becoming adequately secure, whether reviewing a single information system, such as a cloud computing platform or an organization as a whole.

3.5 Audit evidence

The reason of existence of audit evidence is described well in Flint's book *Philosophy and Principles of Auditing* (1988, p. 104) in the first of the three basic postulates for auditing that is:

> *"The subject matter of audit, for example conduct, performance or achievement, or record of events or state of affairs, or a statement or facts relating to any of these, is susceptible to verification by evidence".*

The author further elaborates this postulate by explaining that if the subject matter is not susceptible to verification by evidence because it is a matter for which no evidence as required for the ongoing audit exists, then there cannot be an audit. In other words, if an audit cannot provide evidence against a requirement, then no audit report cannot be made for the requirement due to the lack of evidence. This first postulate by Flint provides perhaps the most solid description for the reason for existence for audit evidence.

As stated in Fitzgerald's book (2012, p. 70) audit liaison is one of the key activities an organization's security function must conduct. The security department or coordinating body should be well advised to have nominated a subject matter expert that understands the security controls to coordinate the audits. While and internal non-security audit department might lead the overall audit with an audit firm, they may not have the technical expertise to understand the security-specific requirements. Therefore, it is suggested that the information security detail should at least assist if not completely conduct the audit with the auditor.

As stated in the research problem, the requirements for evidence on compliance have often not been defined in the standards but left on" the professional judgment of the auditor". However, an auditor should be able to provide a reasoning of how they have come into conclusion that the evidence, a statement without means to explain the conclusion is not credible. According to ISO/IEC 9000:2005, chapter 3.9.4, the definition for audit evidence is "records, statements of fact or other information which are relevant to the audit criteria and verifiable. The evidence may be qualitative or quantitative.

Audit criteria on the other hand is described in ISO/IEC 19011:2011, chapter 3.2 as "A set of policies, procedures or requirements used as a reference against which audit evidence is compared. As evidence has been collected, the next step in evidence handling process in audit is composing of audit findings. ISO/IEC 19011 standard defines audit findings as "results of the evaluation of the collected audit evidence against audit criteria". The findings indicate conformity or non-conformity against a select control objective or objectives. The findings can also lead to the identification of opportunities for improvement or recording good practices. The final step in audit where evidence is processed is the audit conclusion, which is defined in ISO/IEC 19011:2011 as the *"outcome of an audit (3.1), after consideration of the audit objectives and all audit findings".*

According to Zabihollah etc. (2001, p. 156) in their research regarding auditing in IT, in order to issue an audit report, the auditor should determine the following general requirements:

- What evidence is required to address each assertion;
- What audit procedures gather competent and persuasive evidence for each of the assertions;
- How much evidence is sufficient; and
- The most reliable and efficient means of gathering sufficient and competent evidence

To fulfill the evidence sufficiency requirements, the auditor should provide an answer to the following questions (Zabihollah etc. 2001, p. 156):

- Are the electronic records available?
- What is the client's record retention policy?
- What control activities are in place to safeguard records?
- Are detail and summary records available for the audit period?
- Are the electronic records reliable?
- Are encryption and authentication controls in place to ensure integrity of electronic documents?
- Is the internal control structure adequate and effective to ensure the reliability of electronic evidence?
- Where do the numbers (financial items, e.g. inventory) on the financial statements come from?
- What are the origins of the client's electronic records?
- Is there an audit trail and to what extent?
- When, where, and how will the electronic records and documents be audited?
- Can the audit evidence be audited using the client's computer facilities?
- Does the auditor have adequate hardware and software resources available to conduct an audit of electronic evidence?

- What audit software packages are available?
- What computerized simplifying techniques are available to audit electronic evidence?

The above-mentioned detailed list could be summarized into three main high-level requirements: the evidence must be *sufficient*, *appropriate* and *relevant.* A general observation is that there are very few exact definitions available in information security compliance frameworks for what is required of audit evidence for it to fulfill the three characteristics. Therefore, it makes sense to look for evidence definitions beyond IT compliance from other fields of scientific research to find out if universal definitions for evidence exist and can they be applied to cloud-specific compliance evidence evaluation as such.

A practical example of evidence required by a framework is described by Gantz (2013, p. 156), who refers to ISO19011 framework (Guidelines for auditing management systems. According to the author, the audit guidelines provided in ISO 19011 framework, a host of acceptable information References are recognized that the auditors may select depending on the audit scope, complexity, and the criteria that must be satisfied that include:

- Documents such as policies, plans, procedures, standards, guidelines, technical specifications, contracts, licenses, and service level agreements
- Interviews with organizational personnel responsible for operating or managing the subject under examination
- Direct observation of activities occurring in the organizational environment
- Applications, databases, user interfaces, and other technical components
- Performance data such as customer and supplier satisfaction ratings or quality reports produced by third parties
- Simulated or actual control testing, modeling or exercises

ISO 19011 sets the guidelines for all of the other ISO/IEC standards that are suited for management system audits, such as ISO/IEC 27001 (Information Security Management) and ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services). The majority of the other mentioned cloud-specific security frameworks in this study refer to the ISO/IEC practices, such as CSA CCM, or are built on derived from these frameworks, such as PiTuKri, that adds national requirements and other best practices to refine the general requirements set by the longer-running standards. Therefore, the list above can be seen as universally correct in the scope of cloud security auditing practice. An in-depth look into evidence types is included in subchapter 3.2.

4 EVIDENCE COLLECTION PROCESS IN CLOUD COMPLIANCE

The evidence gathering process, especially in cloud security compliance is often a demanding task requiring professional expertise from multiple domains in information security and cloud computing as well as understanding of management systems. Often, multiple subject matter experts (SME) with different skillsets are required for the audit process, both on the auditors and the auditee's behalf. Ratsula (2012, pp. 257-259) has covered the planning process for internal investigation, which is also applicable to audit planning taking place prior the evidence collection.

The audit and assurance planning phase should be well understood to define a concise audit scope. Most modern cloud security frameworks are risk-based; therefore, the scope varies between each audited system or organization. In Anantha's publication (2012, p. 2) the risk-based audit approach is described as the best way to determine what to audit as well as when should the audit be conducted and how often should the process be repeated. Anantha states that as risks impact different systems in different ways, risk-based approach is a way to conduct the audit more efficiently. Most existing cloud-applicable security frameworks are indeed risk-based by definition, such as ISO27001 and CSA STAR. However, some common security frameworks such as PCI-DSS, although not directly cloud-specific, however applicable must be conducted in a stricter criteria-based approach.

Anantha (2012, p. 2) presents a four-step process for a risk-based audit plan. First, the information systems used in the organization should be inventoried and categorized. This helps to find out which systems are included in the audit scope. Next, is should be determined which of the systems could impact critical assets, including money, physical assets or customer data etc. The systems working at or closer to real time are thus more at risk than systems with indirect impact on operations. This is followed by business impact assessment for each of the systems. Finally, the systems are ranked based on the assessment, in order to prioritize the audit resources, schedule and frequency.

According to Ratsula (2012, p. 268) the planning phase should provide an answer to the following questions complemented with the could security-specific details:

- What is the objective of the audit? Is the organization applying for a certificate or an informal attestation of compliance?
- What is the scope of the audit? Is the whole organization covered of just a specific part such as an information system or a management system?
- What documentation is relevant for the audit? Should the audit team review accounting or information system reports, contracts, meeting minutes, e-mails, memos etc.? Is the required documentation readily available?

- Who should be interviewed? In what order should the interviews be conducted? How are the interviews conducted and who should participate?
- What is the schedule of the audit? When should the conclusion be done?
- Which internal participants should be consulted before starting the audit process?
- Who should be informed of starting and the progress of the audit?
- Who are taking part in the audit? Is an internal audit sufficient or is an external audit required?
- What are the roles of participating internal functions such as executive management, legal department, internal audit, compliance department, security department, human resources etc.?
- How is the audit process documented?
- Are there legal restrictions for the audit? If so, how do they affect the process?
- Which immediate procedure should be conducted?
- How is the tampering of audit evidence prohibited?

When the fore mentioned requirements have been fulfilled, the scope finalized and the audit team established, the collection of the audit evidence may begin. As all unique audit plans should be customized according to scope and objective, all of the aforementioned bullet points may not be applicable universally. For example, some audits may contain only technical testing that would exclude interviews for the most part.

However, as the planning phase has been completed and the audit plan and team finalized, the evidence gathering may begin. The evidence is collected to decide whether the organization, information system or management system is compliant or noncompliant with the selected set of requirements applicable for the audit scope. According to Ratsula's publication (2012, p. 261) regarding internal investigation the following questions must be audited in order to succeed in evidence collection. The list has been iterated to contain only the questions applicable in security audits for the integrity of this study:

- What kind of evidence is available? How reliable the evidence is?
- How is the evidence secured?
- How is the evidence collected and how is the collection process documented? Should the legal validity of the evidence be verified? How is privacy taken into consideration?
- Is the confidentiality of the evidence secured? Is the evidence handled only with need-to-know basis?
- How are the relevant personnel, such as SME's communicated with?
- How much evidence is needed? How much evidence can be considered sufficient?
- Is it possible to make conclusions based on the evidence?

In conclusion, not taking cloud security specific the evidence collection process can be divided into two subsequent phases; planning and execution.

In planning, careful thought has to be put into considering what kind of information is going to be collected to be able to attest compliance or noncompliance against the requirements. Especially in security audits and assessments, the confidentiality, integrity and availability of the evidence must be secured with utmost care as an unauthorized publication of evidence or compromise or corruption of information might cause major harm to the auditee.

In order to understand the general qualities that a security-conforming cloud computing system or infrastructure must include, a few common cloud-specific security frameworks have been selected in this chapter for a further review. This review helps in understanding the scope of cloud computing security management in general.

4.1 Types/domains of requirements and controls

This chapter provides a detailed look into the types of security controls and requirements included in select cloud-specific security frameworks. Before going into the cloud-specific security frameworks, the general classification of control types should be understood. Gantz (2013, p. 32) has provided the following figure to separate the three main types of controls that an organization has to utilize in order to safeguard their data:

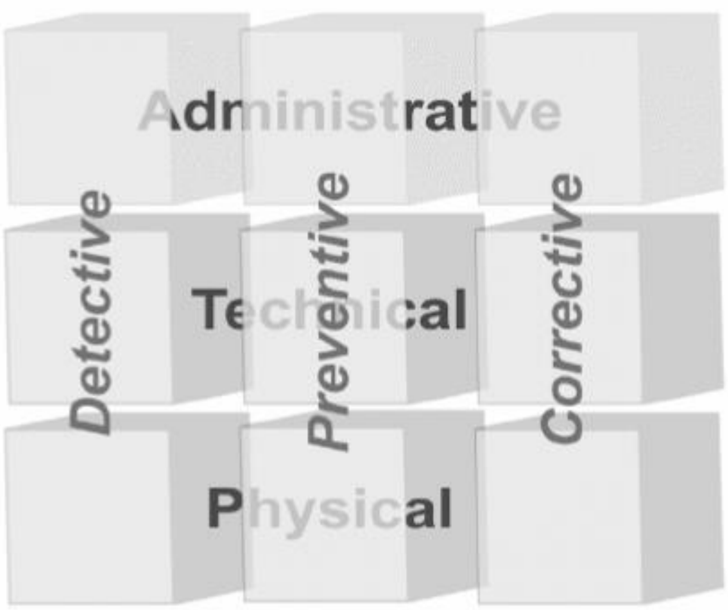


Figure 3: Gantz (2013) The Basics of IT Audit: Purposes, Processes, and Practical Information (p. 32)

Gantz classifies the controls by two categories: purpose-based controls and function-based controls. The purpose-based controls include three subcategories that are *preventive, detective* and *corrective* controls. The preventive controls are used by organizations to prevent unintended or undesirable events or risks from happening, while the purpose of detective controls is to detective controls is to discover if such events have happened. Corrective controls are used to respond to unwanted events that may have occurred. Controls classified by function include *administrative, technical* and *physical* controls. The administrative controls cover organizational policies, procedures and plans specifying the organization's actions in securing the integrity of its operations, information and other valuable assets.

Technical controls on the other hand include the technologies, operational procedures, resources and other concrete mechanisms that an organization has implemented and maintains to achieve the set control objectives. Physical controls include the type of activities and provisions that the organization utilizes to maintain, secure the availability of, restrict or monitor the access to premises such as facilities, storage areas, data centers and equipment and information assets. An example of the control categories is provided in the table below:

	Preventive	**Detective**	**Corrective**
Administrative	Acceptable use policy; Security awareness training	Audit log review procedures; IT audit program	Disaster recovery plan; Plan of action and milestones
Technical	Application Firewall; Logical access control	Network monitoring; Vulnerability scanning	Incident response center; Data and system backup
Physical	Locked doors and cabinets; Biometric access control	Video surveillance; Burglar alarm	Alternate processing facility; Sprinkler system

Table 4: Modified from Gantz (2013, p. 33)

The number and type of requirements vary greatly from one framework to another, as do the domains under which the requirements belong to. The CSA CCM (Cloud Security Alliance, Cloud Controls Matrix) is perhaps the most comprehensive cloud-specific security controls framework at the time of writing. This thesis refers to version 3.1.0 that was published in 2017. The latest version at the time of writing contains 16 control domains that are as follows:

1. Application & Interface Security (AIS)
2. Audit Assurance & Compliance (AAC)
3. Business Continuity Management & Operational Resilience (BCR)
4. Change Control & Configuration Management (CCC)
5. Data Security & Information Lifecycle Management (DSI)
6. Datacenter Security (DCS)
7. Encryption & Key Management (EKM)
8. Governance & Risk Management (GRM)
9. Human Resources (HRS)

10. Identity & Access Management (IAM)
11. Infrastructure & Virtualization Security (IVS)
12. Interoperability & Portability (IPY)
13. Mobile Security (MOS)
14. Security Incident Management, E-Discovery, & Cloud Forensics (SEF)
15. Supply Chain Management, Transparency, and Accountability (STA)
16. Threat & Vulnerability Management

The control domains contain 3-13 individual requirements each. As seen in the list of CCM control domains, the framework has a very broad scope covering the whole spectrum of service components from physical data center security to human resources policy to purely technical issues such as encryption and key management to infrastructure and virtualization security. Verifying a service with CSA CCM is a demanding task for an auditor due to the mere number of required controls as well as for the provider to build the service to comply with. However, as "no stones are left unturned" in auditing a service with the CCM framework, the perceived trust from an issued CSA CCM certificate can be held in high value. For comparison the latest cloud security auditing framework, PiTuKri, has a more concise and narrow scope of domains that are the following:

1. Esiehdot (Prerequisites)
2. Turvallisuusjohtaminen (Security Management)
3. Henkilöstöturvallisuus (Personnel Security)
4. Fyysinen turvallisuus (Physical Security)
5. Tietoliikenneturvallisuus (Network Security)
6. Tietojärjestelmäturvallisuus (Information System Security)
7. Tietoaineistoturvallisuus (Data Storage Security)
8. Käyttöturvallisuus (Operating Security)
9. Siirrettävyys ja yhteensopivuus (Transferablility and Compatibility)
10. Muutoksenhallinta ja järjestelmäkehitys (Change Management and development)

Compared to the massive CSA CCM, PiTuKri has its focus more on the information system, network and administrative security of the service, however some requirement domains from outside technical subject matters are included, mainly in the domains of personnel security and physical security. The requirement domain overviews from CSA CCM and PiTuKri serve as great examples in what kind of subject matter expertise is required from both the auditors and service providers.

It is often misunderstood that cloud computing audit is completely or mostly technical testing and evaluation of the information system and networks only, however a quick glance at the two aforementioned frameworks reveals that decentralizing the services into cloud doesn't mean that traditional security objectives such as personnel background checks or the security of the physical premises such as data centers can be neglected.

4.2 Evidence types and collection methods

To comprehend the evidence collection process in cloud security, the principles of general IT and security evidence collection process should be understood. According to Gantz (2013, p. 182), the auditors rely on evidence collected from the organization to determine the extent for which the elements reviewed satisfy the audit criteria. According to the publication, there is a distinguishable difference in terminology on evidence, with the main takeaway being that raw evidence should be classified as either information or evidence. The main difference is the Reference; information is generally provided the auditee organization or gathered by the auditors.

Evidence on the other hand consists of information that the auditors can verify by using appropriate methods nor not only the information being reviewed, but for the scope, objectives and criteria of the audit as well. The key elements for evidence collection in IT audits often include observing operational procedures or activities. Methods may also include checking technical configuration settings for IT components, reviewing documentation provided by the organization or gathered from interviews with personnel and testing other controls. The key evidence collection activities are shown in the figure below:

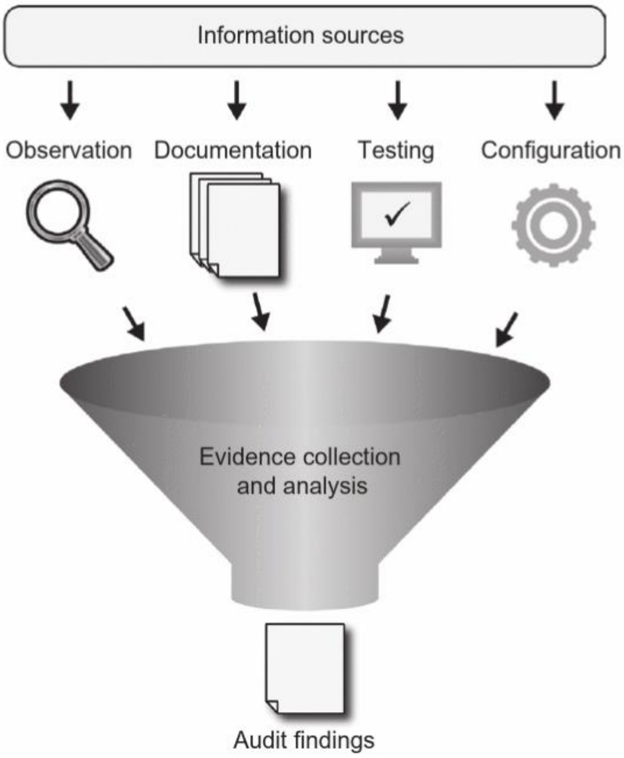


Figure 4: Gantz (2013) p. 183

As pictured in the figure 4 above, the *information* References become *evidence* when and if the auditors are able to process the information by evaluating it. The evaluation process includes confirming the accuracy and completeness, among other necessary qualities of the information and correlating the findings against audit criteria. The evidence qualities are further detailed in chapters 5 and 6.

As stated by Gantz (p. 155), the evidence collected by auditors provides the basis for audit findings, including indications of insufficient or ineffective controls or determinations of conformity. Information technology audit evidence References vary by the type of audit and the purposes and objectives. In order to completely examine a system, environment or a process that has been built on administrative, physical or technical controls, the auditors must consider a vast range of criteria that corresponds to many References of information and evaluation methods.

Methods	Applicability
Examination	▪ System documentation, specifications, diagrams ▪ Plans, policies, procedures, instructions, guidelines ▪ Standards, frameworks, methodologies
Interviewing	▪ Employees with operational responsibility for audit subjects ▪ Managers responsible for governance, risk and compliance ▪ Customers, support personnel, system end users
Observation	▪ Software or hardware functionality ▪ Operational activities, processes, practices, exercises ▪ Personnel behavior
Testing	▪ Technology components ▪ Hardware devices ▪ Application software and systems ▪ Procedural controls and technical capabilities

Table 5: Modified from Gantz (2013) p. 157

The four collection methods according to Gantz are *examination, testing, observation* and *interviewing*. It is crucial to understand the applicability of each method on the type of requirement being reviewed. Cloud security auditing frameworks at the time of research include requirements for each of Gantz's applicability categories, thus the table can be seen applicable for cloud security as is.

5 EVIDENCE DEFINITION IN SCIENTIFIC RESEARCH

According to Schwandt (2009, p. 199), evidence in general means information that is helpful in forming a conclusion or judgment. Moreover, evidence means information bearing on whether a belief or proposition is true or false, valid or invalid, warranted or unsupported. In absence of cloud- or other information security specific scientific definition for evidence, the research was broadened to other fields of study with longer history in defining evidence. For this research, the fields of economics and legal policy were chosen for further study. Even though nearly all scientific research is evidence-based, the aforementioned scientific fields are known to include different kinds of auditing practices, therefore it is reasonable to look for common nominators in between evidence qualities across the disciplines.

5.1 The scope of the cross-scientific review for definition of evidence

This chapter focuses in the definition of evidence beyond information technology and cloud computing-specific research in order to gain a holistic understanding into the concept of quality evidence. In their publication on understanding and using scientific evidence, Duggan & Gott (2011) summarize the process of evidence-based decision making in a very simple form as presented in the following figure:

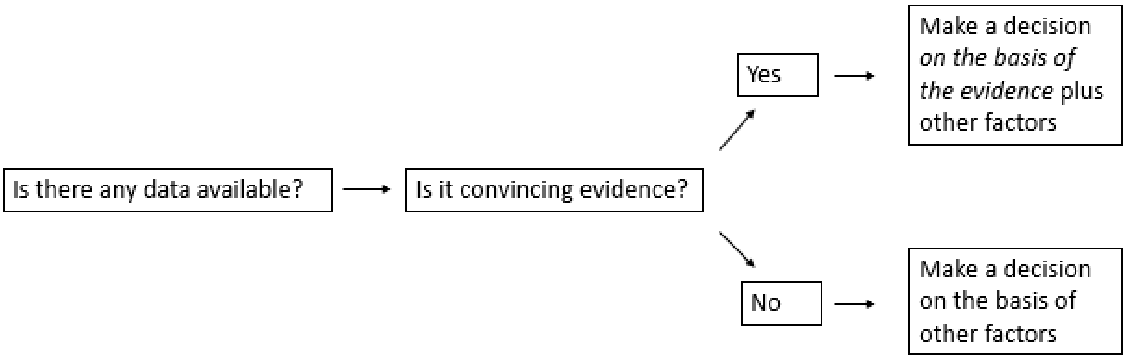

Is there any data available?
Is it convincing evidence?
Yes
Make a decision *on the basis of the evidence* plus other factors
No
Make a decision on the basis of other factors

Figure 5: Gott & Duggan (2011), p. 4

This scenario provides a prerequisite to the research question of this thesis:" *What quality requirements can be applied on cloud security audit evidence?"* According to the figure, in case convincing evidence is not available, the decision would have to be made on the basis of other factors. It is to be noted that even if a decision could be made without convincing evidence, the decision should be considered an assumption or a hypothesis at best. In information security auditing, such assumptions do not suffice for compliance.

Gott & Duggan (2011, p. 4) state that there are three main ways in which scientific evidence is used that are looking for a *link*, *difference* or a *change*. To understand how these use cases, work according to the authors, a summary of each case has is provided below with an added proposal of how the use case would apply into information security auditing.

1. The first use case for evidence according to Gott & Duggan is a *link*. This is described as data that can be used as evidence to demonstrate the "strength of a link, relationship or an association in various ways". The link is further elaborated as a direct association between *cause* and *effect* that in its simplest form means that if change X is implemented, then Y will happen. A simple practical example of the use case according to the authors is the relationship between mass and the stretch of a rubber band.

   The link in this case is the knowledge in what would happen if a known mass would be attached to a rubber band; i.e. would the band stretch within its limits or snap. In information security auditing the link could be for example the strength of cryptography applied to a security critical system component, such as a password hash, i.e. knowing approximately how much computing capability would it take to crack a password has encrypted with 256-bit AES-encryption as opposed to a weaker 128-bit variant.

2. The second use case presented in Gott & Duggan's publication is a *difference*. A difference as an evidence use case is data that can be used as evidence to decide whether two or more groups of data differ significantly from each other or not. In theory, according to the authors, the difference can be verified by looking if there's a significant difference in outcomes between the treatment of an illness in area X compared to area Y.

   This requires gathering information from both samples X and Y and applying appropriate statistics in order to establish the probability of whether or not the two outcomes are different. In information security auditing, difference-type evidence could be looked for example in validating if an organization has trained the personnel in information security basics equally; i.e. interviewing employees from different functions with the same questionnaire to find out if a specific key personnel group would be lacking in required knowledge.

The last use case for evidence according to Gott & Duggan is a *change.* This use case according to the authors is best described as data that can also be used as evidence to establish change with time, i.e. in order to find out how the vitamin content of a type of apple changes between the time it was picked and the day it was sold on the market. The change is measured by gathering data and using appropriate statistics to provide a comparison. In information security auditing, change-type use cases could be for example validating the efficiency of a network intrusion detection (IDS) component by looking at SIEM log data between different points of time, such as before and after the implementation of the IDS component.

5.2 Evidence and its evaluation in scientific research

According to Gray & Manson in their book on financial auditing process (2000 p. 154), the audit can be defined as "a search for evidence to enable an opinion to be formed". The authors summarize the process of searching for evidence in external audit as a "process that enables the auditor to form an opinion". Specifically, "the opinion is formed from a whole series of conclusions in pursuit of the main audit objectives". The objectives according to the authors are as follows:

- Verifying the accuracy and dependability of the accounting records.
- Giving an opinion on the truth and fairness of financial statements
- Being satisfied that CA 1985 and accounting and reporting standards have been complied with.

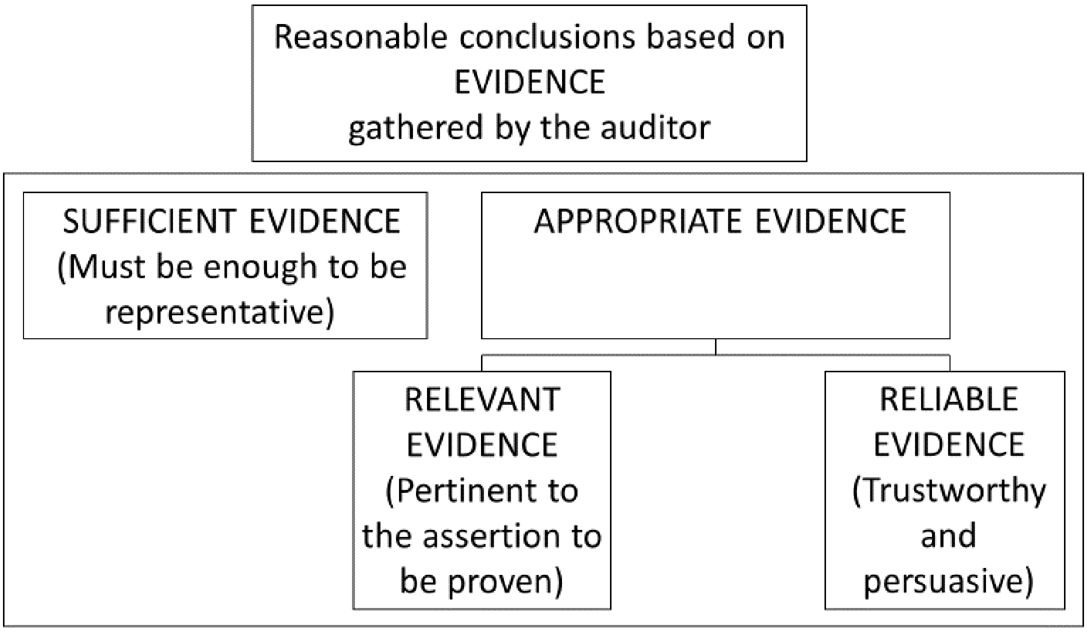

Reasonable conclusions based on EVIDENCE gathered by the auditor
SUFFICIENT EVIDENCE (Must be enough to be representative)
APPROPRIATE EVIDENCE
RELEVANT EVIDENCE (Pertinent to the assertion to be proven)
RELIABLE EVIDENCE (Trustworthy and persuasive)

Figure 6: Gray & Manson (2000, p. 155)

In the figure above it should be noted that, according to the authors (p. 156), the evidence is persuasive rather than conclusive, meaning that the auditors therefore must seek evidence from different References to support the same assertion. This means that the auditor seeks *corroborative* evidence, linking the relevancy and reliability boxes in the figure above. In other words, corroborative evidence is evidence that is consistent with the data or information that has been previously collected (p. 161). The authors further emphasize the meaning of evidence in financial auditing, stating that evidence is the cornerstone of the audit process and a prerequisite for forming an opinion. Without evidence, in the words of the authors, it would be impossible to come to a reasoned conclusion about anything. Gray & Manson have also covered the subject of reliability of audit evidence extensively in their book from financial auditing's point of view. There are ten guidelines proposed for assessing evidence reliability in the publication (2000, pp. 158-162) that are summarized in the following chapters. The guidelines are presented primarily from an external auditor's point of view, however understanding these guidelines might be beneficial for the auditee as well. To start off with the guidelines, the first one is that the existence of physical objectives should be confirmed by the auditors themselves. This example can be seen as applicable for a variety of audits beyond financial auditing, such as having the auditors visit a data center in cloud security audit and have them verify the physical security controls in person.

Next example is analysis that the auditors should conduct on received information. In practice this means that the information shouldn't be accepted "as is". However, as pointed out by the authors, the outcome of the analysis is as good as the figures used in measurement, applicable obviously in financial auditing. However, as Gray & Manson propose a quantitative analysis, qualitative analysis might also be an option for different evidence types, such as the ones encountered in cloud security audits. The third proposed guideline is evidence from independent third parties. The authors have summarized this strategy in a rule that is: *"Evidence from third parties is good evidence, particularly when received from persons acting in a professional capacity"*. However, it should be noted that this rule doesn't apply to all evidence examples, such as in cloud security auditing where third-party evidence is not common due to the requirements. However, if such third-party evidence is available, the fore mentioned rule is worth considering.

The fourth guideline suggests that evidence from third parties in the hands of the company is good evidence but may have been manipulated by the management. Even though this guideline may seem self-explanatory, it is worth remembering that an auditor shouldn't accept third-party evidence from the auditee at face value but apply further analysis on the information as per the second guideline suggests. The fifth example is the evidence created in the normal course of business is better than evidence specially created to satisfy the auditor. In practice this means that evidence collected by observing the day-to-day operations in less likely to be biased than specifically created evidence.

This guideline can be seen as universally applicable regardless of audit type, in case information collection is possible from day-to-day operations. In the authors' words, this sort of evidence will have greater value than evidence produced just to satisfy the auditor. However, is to be noted that this guideline, even though efficient, is not the easiest nor the most cost-efficient as the audits are often done on a strict budget. The sixth example provided by Gray & Mason is that the best-informed Reference of audit evidence will normally be the management of the company subject to audit, but management's lack of independence the management's lack of independence reduces its value as a Reference of such evidence. In addition, the authors stress that even though these guidelines emphasize external evidence, this doesn't mean that internal evidence would be bad evidence. Internal evidence may be very useful in case the controls surrounding it are good and the integrity of management is high. In other words, internal evidence must be evaluated with special care.

The next, seventh guideline by Gray & Manson (p. 160) is that written evidence is of greater value to the auditor than oral evidence. In practice, this means that as during an audit, the auditor receives a variety of oral evidence through interviewing etc. from the auditee's representatives. This oral evidence will then have to be reflected in the auditing framework, requirements, plans and other working papers of the auditor and recorded in order to make the evidence more useful and *reliable.* According to the authors, the recording of oral evidence is a common practice among audit firms, fortifying the assumption that the evidence must be *reliable* and *repeatable*.

This guideline is well applicable for the most common cloud security auditing frameworks as well, as interviewing is most likely required to verify a host of the administrative requirements and processes. The eight guideline is that properly established and tested systems of control enhance the reliability of evidence derived from them. In cloud security auditing, this could mean for example when auditing a physical data center, if relevant data such as upkeep costs and other maintenance accounts and relevant controls are available and verified by for example a financial auditor, the presented security evidence may also be seen as more reliable and trustworthy for the specific physical asset. While applicable for audits outside financial auditing, this guideline may not be the most useful for security audits.

The ninth example (p. 161) is that evidence about the future is particularly difficult for the auditor to obtain and is less reliable than evidence about past events. The auditors provide a breakdown of this guideline as follows: although it may be more difficult for the auditor to obtain evidence about the future, the main problem being the uncertainty associated with it, there are ways in which the uncertainty can be mitigated. According to the authors, (p. 161) The auditor's view of future events is likely to be colored by their opinion of the reliability of management, the extent to which management has proved able to anticipate the future in the past and the means by which management itself attempts to control the future.

Summarized, when evaluating evidence that points to possible future events such as predictions, the applicability of the evidence should be carefully evaluated. This guideline can be seen to recognize the both the auditor's and auditee's fallibility to biased decision making, which is discussed in detail in subchapter 5.4. The tenth and last guideline is that evidence may be upgraded by the skillful use of corroborative evidence. In practice, according to Gray & Manson (p. 161) this means that other evidence may corroborate statements by client officials and that evidential material may be rendered more useful by the Reference from which it is derived being subjected to adequate control. In other words, this guideline means that as evidence corroborates with another piece of evidence, the value of both pieces is enhanced. According to the authors, if two separate pieces of evidence corroborate, they become more valuable than the sum of their individual values.

Even though the ten guidelines presented have been developed with financial auditing in mind, many overlapping potential use cases were recognized for use beyond financial domain. Some of the guidelines could be useful in cloud security auditing as is, while the remaining ones could be made fitting into security auditing with modification, primarily reviewing the requirements with IT and cloud computing audit evidence in mind. However, as the guidelines aren't made specifically for information technology, they might be applicable beyond financial auditing as the guidelines are rather universal and not bound on financial accounting evidence in particular.

Stefan Zuca (2013) has also researched the concept of audit evidence in his essay in Procedia Economics and Finance journal vol. 20 (pp. 700-704). Zuca states that audit evidence is defined as all the information used by the auditor in arriving at the conclusions on which the audit opinion is based. These conclusions can be classified as the underlying accounting records maintained by management to support the preparation of the entity's financial statements and other information. Even though Zuca's essay has been written from financial auditing's point of view, the fore mentioned *other information* could be seen to include the compliance information beyond financial subjects. The author explains that the auditor obtains audit evidence through the performance of auditing procedures and from other References, such as a firm's quality control procedures etc. This statement further validates the descriptions on the audit process in the other financial audit research reports. However, Zuca further elaborates the qualities of audit evidence, split into sufficiency and appropriateness as follows.

The international standards on auditing (ISA) are professional standards for the performance of financial audit of financial information. These standards are issued by International Federation of Accountants (IFAC) through the International Auditing and Assurance Standards Board (IAASB). ISA according to Zuca (p. 701) defines *sufficiency* of audit evidence as the "measure of the quantity of audit evidence". This definition can be illustrated as the following figure from the publication:

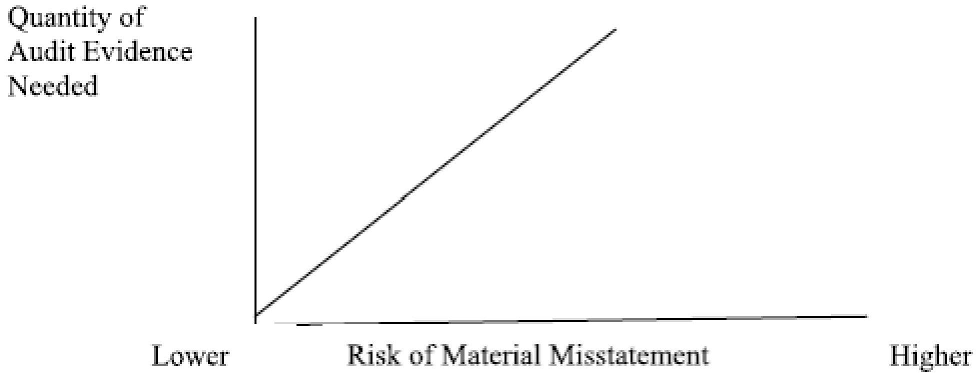


Figure 7: Relationship of Risk of material Misstatement to Suffciency (Quantity) of Audit Evidence required (Zuca, 2013, p. 702. originally from Puncel, L 2009.)

As shown in the figure 7, the quantity of audit evidence required will be greater if the risk material misstatement increases related to an account balance, class of transaction or disclosure. *Appropriateness* is described similarly as the" measure of the quality of audit evidence, or in other words, its relevance and reliability in providing support for, or detecting misstatements in, the classes of transactions, account balances and disclosures and related assertions". Summarized, according to Zuca and ISA, sufficiency measures quantity and appropriateness measures quality. Furthermore, appropriateness can be explained by the following figure from Zuca's essay:

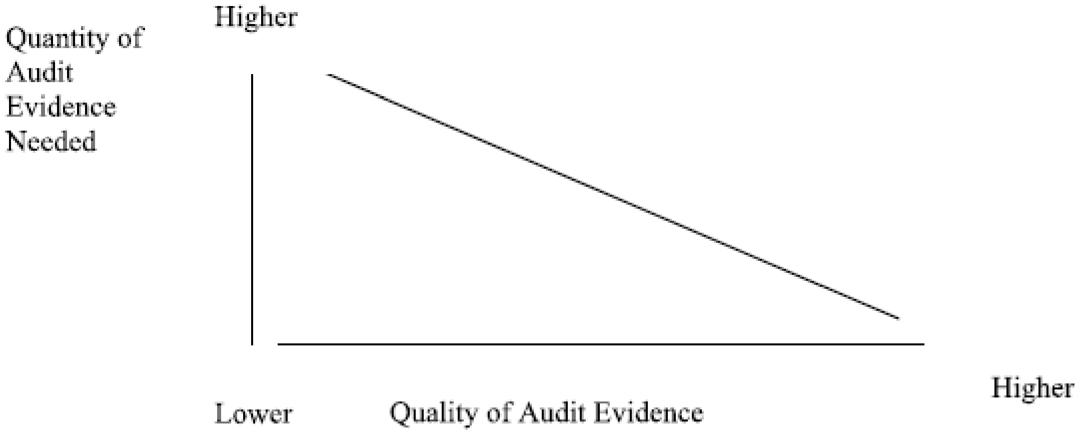


Figure 8: Relationship of Appropriateness (Quality) to sufficiency (Quantity) of audit Evidence Required (Zuca, 2013, p. 702. originally from Puncel, L 2009.)

The figure 8 above describes the relationship between *appropriateness* (quality) and *sufficiency* (quantity) of audit evidence. According to Zuca's and ISA's definition, the quality of audit evidence decreases as the obtained evidence (quantity) increases. This discovery is validated by several Gray & Manson's guidelines (pp. 44-45) that emphasize evidence validity by supporting, independent evidence. In general, the figures 7 and 8 illustrate the general interrelationships between the quantity of evidence required and the risk of material misstatement and the quantity of evidence required and the quality of the evidence (Zuca 2013, p .702). According to the figures, the relationships are not necessarily linear. According to the author, merely obtaining a greater quantity of lower quality audit evidence may not compensate for a lack of higher quality audit evidence. Thus, the auditor's judgment requires support in order to determine the sufficient amount of audit evidence. This discovery validates the research problem and the need for an external tool to support the decision-making in audit evidence evaluation.

In addition to the fore mentioned evidence characteristics, Zuca also describes the reliability of evidence in detail. According to the author (p. 703), reliable evidence must also possess the following characteristics:

- Audit evidence is more reliable if it is obtained from a knowledgeable, independent Reference outside the entity;
- Audit evidence generated internally is more reliable if the entity's related internal controls are more effective;
- Evidence obtained directly by the auditor through physical examination, observation, computation and inspection is more persuasive than evidence obtained orally. For example, written documentation prepared by the company of the performance of a control is more reliable than evidence obtained through subsequent oral representations by the individual who performed the control:
- Original documents provide more reliable evidence than photocopies or facsimiles.

In summary, Zuca recognizes *reliability* and *sufficiency* as the main characteristics or qualities for evidence. However, the author also mentions other qualities, *accuracy* and *completeness* and included these as sub qualities of reliability as opposed to a several other References that have them categorized as independent qualities. Additionally, Zuca mentions the importance of *evidence corroboration*, as some other studies reviewed (see p. 44). Zuca concludes his essay (p. 704) in stating that the auditors must document and collect evidence concerning important issues both in preparing the report and supporting the opinion expressed and all other evidence to prove that the the audit was conducted in accordance with international Standards of Auditing, coming from financial auditing's point of view. According to Zuca, (2013, p. 704) the audit documentation may be perceived as a "mission story", that should allow any user to understand the risks, assertions tested, procedures, how the evidence was obtained and concluded so that the statements match the financial report and pertinent audit opinion.

Marris (2010) has also studied subject of evidence collection in her publication "The Challenges of Obtaining Audit Evidence in Information Technology Environment". According to the author, more than 90% of audit evidence at the time of writing in financial accounting were in digital form, while 80% of audits failed due to poor audit evidence. As ten years have passed since the publication, it is expected that the percentages may be now higher, and accounting the digital nature of cloud security evidence, the discoveries in Marris' research may be applicable somewhat universally beyond financial auditing. Marris refers to AICPA's (American Institute of Certified Public Accountants) Generally Accepted Auditing Standards (GAAS) throughout her publication, also conducted for financial auditing. According to Marris' publication (p. 2), the third GAAS standard states "the auditor must obtain sufficient appropriate audit evidence by performing audit procedures to afford a reasonable basis for an opinion regarding the financial statements under audit".

Marris explains that audit evidence is all the information used by the auditor in arriving at the conclusions on which the audit opinion is based and includes the information contained in the accounting records underlying the financial statements and other information according to AICPA. Marris also goes into detail in describing sufficient and appropriate evidence. According to the author, sufficiency is the quantity of audit evidence, while appropriateness is the measure of the quality of the audit evidence. The quality consists of relevance and the evidence's reliability in providing support for, or detecting misstatements in the classes of transactions, account balances, disclosures and related assertions according to AICPA.

Marris (2010, pp. 3-4) explains that both sufficiency and appropriateness must be taken into consideration when assessing risks and designing the audit procedures. Additionally, the reliability of the Reference and type of evidence has to be considered. This procedure is based on the observation that the higher the risk of material misstatement, the quality of the audit evidence should be higher. In other words, if the quality of the evidence is high. the amount of audit evidence needed is less. The mentions on evidence quality in this publication correlate with the other research on the subject, and further verify that sufficiency and appropriateness are the core qualities that evidence must possess. Marris (2010) also mentions completeness as a requirement for evidence (p. 12). In electronic evidence, according to the author, an electronic system may substitute codes or cross-references to other data files that may be hidden from users. This quality could be seen as a form of evidence corroboration, as mentioned in other studies.

Other qualities mentioned by Marris (p. 15), also found across other research publications are occurrence, classification and understandability, and accuracy and valuation. In the words of the author, occurrence means that the occurrence of disclosed events and transactions can be verified. In other research, this is often referred to as repeatability or reproducibility. Completeness means that all disclosures that should have been included have been included. This correlates to the common description of sufficiency. Accuracy and valuation mean that the information is disclosed fairly and at appropriate amounts, hence this quality correlates with appropriateness.

The SAS 106 – Audit Evidence standard by AICPA, as referred to by a several References on audit evidence, contains a through description on audit evidence, relevant assertions, qualitative aspects and various audit procedures. In general, the standard verifies the discovered audit qualities, audit process description and the other discoveries from across the reviewed studies and related disclosures. However, the SAS 106 standard uses again partially different terminology on the subject of evidence quality. The standard describes the key evidence qualities under chapter "The Use of Assertions in Obtaining Audit Evidence". While the classifications have been constructed according to financial periods, the assertions could be again applicable beyond financial context. These assertions have been categorized in the standard in the following way:

A) Assertions about classes of transactions and events for the period under audit:

   1. *Occurrence.* Transactions and events that have been recorded have occurred and pertain to the entity.
   2. *Completeness*. All transactions and events that should have been recorded have been recorded.
   3. *Accuracy.* Amounts and other data relating to recorded transactions and events have been recorded appropriately.
   4. *Cutoff.* Transactions and events have been recorded in the correct accounting period.
   5. *Classification.* Transactions and events have been recorded in the proper accounts.

B) Assertions about account balances at the period end:

   1. *Existence.* Assets, liabilities, and equity interests exist.
   2. *Rights and obligations*. The entity holds or controls the rights to assets, and liabilities are the obligations of the entity.
   3. *Completeness.* All assets, liabilities, and equity interests that should have been recorded have been recorded.
   4. *Valuation and allocation*. Assets, liabilities, and equity interests are included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded.

C) Assertions about presentation and disclosure:

   1. *Occurrence and rights and obligations*. Disclosed events and transactions have occurred and pertain to the entity.
   2. *Completeness*. All disclosures that should have been included in the financial statements have been included.

3. *Classification and understandability*. Financial information is appropriately presented and described, and disclosures are clearly expressed.
4. *Accuracy and valuation*. Financial and other information are disclosed fairly and at appropriate amounts.

While the SAS 106 standard adds very little to the knowledge obtained on evidence qualities so far, it is noteworthy that the qualities required again vary on the type of evidence. In addition, the standard introduces multiple assertions on a single sample of evidence, validating that there may be multiple applicable quality requirements depending on the evidence type, such as for financial transactions under the period of audit (category A), for which the SAS 106 introduces five different assertions.

As discovered in the previous chapters, there are various definitions available in different scientific fields. In order to find out whether these definitions would be sufficient in computer science and cloud security compliance, this subchapter sums up the common nominators found on two or more References found in the previous cross-scientific review. Perhaps the best Reference of evidence definition in general was economics and specifically financial auditing; the practices found in the area are often very well internationally adopted and carried over to other types of audits. When looking into evidence definitions in law and criminology however, it was noticed that the definitions vary greatly between the national origin of the text and the time or era of writing. To sum up the discoveries, the most commonly found evidence qualities have been divided into for classes as follows:

Common nominator 1: **Sufficiency / Completeness**

Sufficiency was perhaps the first attribute that came up when searching for evidence definition regardless of the scientific field or scope of the study. In some definitions, this evidence quality was discussed as completeness. In general, sufficiency measures the quantity of evidence. In security assessments, this quality may be used in judging for example whether a sample size is enough or not.

Common nominator 2: **Appropriateness / Accuracy** (Relevancy, Reliability)

Another often discovered evidence quality was appropriateness or accuracy, sometimes mentioned as relevancy or reliability. Generally, this evidence quality is a qualitative measure of the evidence. In security assessments, this quality can be used to measure whether the evidence answers to the requirement or not.

Common nominator 3: **Trustworthiness / Integrity** (Corroboration)

Often discovered term, however not found in every evidence quality description publication is trustworthiness or integrity. This quality can be either a qualitative or a quantitative measure, depending on the information the evidence is constructed on. Sometimes this quality was mentioned as evidence corroboration, meaning that the findings can be verified by other independent evidence samples.

Common nominator 4: **Repeatability / Reproducibility**

Perhaps the least met quality, however found in a several References was repeatability or reproducibility. This quality can also be a measure of either quantitative or qualitative attributes of the evidence depending on the information. In general, repeatability measures if similar evidence can be obtained by repeating the collection and assessment process.

Gantz (2013, p. 157) has stated in his book, that the primary purpose of collecting evidence In IT audits is to enable auditors to correlate the evidence to applicable audit criteria and analyze the evidence to determine the extent to which those criteria are satisfied. The audit evidence analyzing practices encompass a vast range of methods. In practice, the auditors select the most suitable methods for the type of control under review as well as for the type of audit and its purpose and objectives.

The auditors must resort to whatever guidance is available on analyzing the evidence to choose the correct method for reviewing administrative, technical and physical controls. The types of methods for different types of evidence are described in subchapter 4.2, table 4. As the terminology for evidence varies between standards and References of guidance, as well as between different sciences as noticed in subchapter 5.2, the selection of the analysis method is down to the auditors professional judgement as no official or unofficial tools are available for evaluating qualitative evidence in cloud security compliance.

5.3 The effect of cognitive bias on evaluation process

Even though audit processes, including information systems and cloud security audits are designed to be evidence-based in order to avoid opinionated decision making, the auditors are still at the time of conducting this study in principle human and thus fallible to human error. As stated by Schwandt (2009, p. 201) evidence by itself cannot be wrong or right in an absolute sense. Our interpretations of the evidence can be flawed. Westhausen (2019, p. 52) has studied the effects of cognitive biases of external auditors, and states that even if the auditing goals of external and internal auditors may be different, the presence of bias-prone situations may endanger both types of auditors similarly. Thus, cognitive biases might be transferable between internal and external audits similarly.

Westhausen (2019, p. 53) presents five common types of cognitive biases that may occur in external auditing. The first example is *confirmation bias*. This bias is the most common, practically it means that the auditor may seek for information that confirms pre-existing beliefs and expectations. The second example is *overconfidence bias*; this may happen is the external auditors or other specialists overestimate their ability of being bias-immune, neutral and accurate. In practice, the external auditor may make decisions on insufficient information as they may consider themselves to be able to have the skill even if the evidence is lacking. *Hindsight bias* means that individuals, such as external auditors, after having been provided with the outcome of an uncertain event, tend to believe that they could have predicted the outcome. This is usually accompanied by the belief that the outcome had affected the auditor's predictions. According to the author (ibid p. 53), hindsight bias may influence audit judgments, internal control evaluations, audit opinion decisions, preliminary analytical review judgments and going concern judgments.

The fourth mentioned bias type is *knowledge bias*. In practice this means that as the auditors receive information, conclusions or opinions from external References, for example from subject matter experts by interviewing, it is up to the auditors to decide whether the received information is fairly stated. This make the external auditors vulnerable to the knowledge bias as they may be unable to ignore the information provided by the external References and form their own conclusions independently. An independent conclusion would require further processing of the information, such as data analysis, interviews or technical testing which the auditor may exclude if they are biased and judge the received information correct without verification. The fifth and final bias presented by Westhausen is recency bias. This bias concretizes as a tendency in which the auditor may put a greater emphasis on the most recently received information, disregarding the earlier information. According to the author, recency bias may be mitigated by professional skepticism within the external auditing process. This bias is always effective to some extent, with a stronger impact if the information is presented sequentially rather than simultaneously.

To mitigate and combat biases in auditing, Westhausen proposes several debiasing strategies (p. 59). The strategies are presented from internal auditing's point of view, however as mentioned, the bias-issues in external and internal auditing are often common so it can be interpreted that the strategies are interchangeable as well though not specifically confirmed by the author. The strategies have been separated in five different strategy groups, each including a set of separate strategies. The first group is *general strategies,* that includes the following strategies; feedback, statistical analysis, critical thinking, debiasing awareness, training and education, heterogeneity and quality management. The group of *specific strategies* includes reframing, assessing uncertainty, implementation of instructions and increasing the accountability of the decision maker.

Technological strategies include quantitative methods, checklists, decision support systems and auditing software. The category on *motivational strategies* include increasing accountability of the decision maker and monetary and non-monetary incentives. The last subset of *cognitive strategies* includes decomposing and restructuring the relevant information, perspective change from decision maker to an "outsider", reviewing alternate hypotheses and strengthening self-control. As mentioned by Westhausen, these 19 strategies cannot always be applied at one time simultaneously, but rather partially and gradually. The applicability of these strategies in cloud security auditing has been further discussed in subchapter 6.5

As the fore mentioned biases have been scientifically recognized, they cannot be overlooked in the quality management of audit processes, cloud security audits included. The existence of the biases also indicates for a need for an evidence evaluation tool that leaves less room for interpretation, effectively mitigating biased or uninformed decisions. In the context of this study, biases in auditing are only briefly explored, however it should always be remembered that whenever humans are involved, the human factor introduces potential pitfalls such as biased decision-making.

Harrison, Srivastava and Plumlee (2002, p. 161) also recognized the issue in their research paper, "Auditors' Evaluations of Uncertain Audit Evidence: Belief functions versus Probabilities". According to the research, many auditors use probabilities to measure risk express ignorance by giving equal weight to support and for support against the objective. As probabilities are indeed not included in the good auditing practices covered in this research, such as in the Generally Accepted Auditing Guidelines, this type of decision-making includes a high risk of auditor's personal bias effecting the outcome.

In the future, as auditing may be partially automatized as proposed by Knoblauch (2017, p. 15), enabling continuous assessing of a system's compliance status, as opposed to the point-in-time type of traditional auditing and certification processes. Also, Gul, ur Rehman and Islam (2011, p. 147) state that in cloud computing, security auditing can be enforced through a third-party auditor or an automated auditing interface/mechanism to improve trust in cloud computing paradigm. This automatized auditing may however be conducted on technical requirements as proposed by the researcher, stating that technical and physical requirements will still be audited by humans in the foreseeable future. Biased decision making will thus be an issue that has to be recognized whenever assessing information and refining it into evidence. The best ways to mitigate biases are tools to help confirming the validity of the conclusions and awareness of the biases.

6 QUALITY APPRAISAL OF THE DISCOVERIES

Throughout this study, it was found out that the qualities and requirements of evidence were not covered in depth or at all in any of the cloud-specific security compliance frameworks that were released at the time of conducting the research. However, the definition of evidence was found to have been well studied and described in other fields of research and for IT-auditing in general. These qualities, as covered in chapters 4 and 5 provide the four reoccurring qualities that will be tested in this chapter against actual cloud security requirements from the CSA CCM framework with theoretical evidence. It should be noted, that this concept doesn't include every individual found evidence quality or guideline but is rather focused on the most common qualities appearing in multiple References on evidence evaluation.

Moreover, as for the systematic literature review research method requires the discoveries to be analyzed and synthesized, the concept tool of presented in this chapter shall verify the applicability of the discoveries from the previous chapters. According to Templier & Paré (2015, pp. 118-119), the synthesis should follow a logic of configuration by drawing conclusions based on a coherent assembly of findings. Additionally, narrative reviews should confirm findings through the repetition of thematically similar evidence. Therefore, the applicability of the discovered evidence qualities and requirements will be tested in through several empirical cases built on hypothetical evidence.

6.1 Evidence evaluation checklist concept

To summarize the findings in this study, a concept checklist for cloud security evidence evaluation has been produced. The checklist can be found below. The list follows a similar structure as many of the security frameworks referred to in the study. The first paragraph contains an indicator for the evidence itself. The evidence can be for example a policy document or a network packet capture file.

Evidence ID	Evidence requirement	Description	Applicability (Yes / No)	Compliance (In Place / Not in Place)	Notes
E-1	Repeatability / Reproducibility	The evidence collection must be repeatable under similar circumstances.	Yes	Not in place	-
E-1	Trustworthiness / Integrity	The evidence must be provided by a trustworthy and appropriate Reference.	Yes	In Place	-
E-1	Sufficiency	The evidence must provide enough information, etc. snapshot of a long enough timeframe.	Yes	In Place	-
E-1	Appropriateness	The evidence must provide an answer as directly as possible to the respective requirement.	Yes	In Place	-

Table 6: Evidence evaluation checklist concept

As the evidence collection process may include dozens of different examples of evidence, the auditor should list the evidence with separate evidence identifiers in order to help with the evidence evaluation. An example of such list is presented in the following table:

Evidence ID	Evidence headline
E-1	Information security strategy, Company X
E-2	Risk management policy, Company X
E-3	Information security compliance process
E-4	Physical access control policy for premises
E-5	Cloud service agreement, vendors
E-6	Change management process
E-7	Packet capture file, cloud to client
E-8	Identity and access management policy
E-9	Data backup policy
E-10	Crisis management policy
E-11	Security event log snaphot

Table 7:Evidence identifier list example

6.2 Evaluation checklist for an administrative requirement

The following chapter presents a hypothetical case to test the checklist in practice. The auditee is looking to get certified against CSA STAR certification, and the auditor uses the CSA CCM framework to assess the requirements. In this hypothetical case, the auditor is looking for answers for the following CSA CCM requirement from the organization's identity and access management policy provided by the auditee. This first example was chosen for its administrative scope. To keep the research concise, an example of the evidence is not presented.

Control Domain	CCM V3.0 Control ID	Updated Control Specification
Identity & Access Management Policies and Procedures	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

Table 8: CSA CCM requirement IAM-04: Identity & Access Management, Policies and Procedures

The provided Identity and access management policy document has been given an evidence ID "E-8". The auditor has made their decision about the evidence and edited the last three paragraphs accordingly.

Evidence ID	Evidence requirement	Description	Applicability (Yes/No)	Compliance (In Place / Not in Place)	Notes
E-8	Repeatability / Reproducibility	The evidence collection must be repeatable under similar circumstances.	Yes	In Place	The policy document follows the company documentation procedures, a journal number is included.
E-8	Trustworthiness / Integrity	The evidence must be provided by a trustworthy and appropriate Reference.	No	Not in Place	The policy document is over 4 years old, the policy hasn't been reviewed regularly.
E-8	Sufficiency / Completeness	The evidence must provide enough information, etc. snapshot of a long enough timeframe.	No	Not in Place	The policy doesn't contain a list of the authorized personnel. AD + AD Policy must be reviewed separately.
E-8	Appropriateness / Accuracy	The evidence must provide an answer as directly as possible to the respective requirement.	Yes	In Place	The policy document describes the process of storing and managing system privileges. However, a further AD review is needed.

Table 9: Evidence evaluation checklist in practice, administrative requirement.

In this specific case, the auditor has found the evidence requirements of repeatability/reproducibility, and appropriateness to be in place. However, the document by itself was not enough to verify that the organization operates by the policy, so the auditor has noted that a further technical Active Directory review is needed. Also, the auditor has noted that the policy document is old and most likely hasn't been regularly reviewed, so the auditor is most likely cannot accept the provided evidence as the requirements haven't been met.

6.3 Evaluation checklist for a technical requirement

The second example covers a similar case as in subchapter 7.2, but with a technical requirement and evidence. The following requirement from CSA CCM V3.0.1 framework was chosen for an example for its technical scope, auditing the requirement requires technical evidence as opposed to the previous example (7.2). The chosen requirement for this example was IVS-01, Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection.
To keep the research concise, an example of the evidence is not presented.

Control Domain	CCM V3.0 Control ID	Updated Control Specification
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.

Table 10: CSA CCM requirement IVS-01: Infrastructure & Virtualization Security, Audit Logging / Intrusion Detection

In this example, the auditee organization has an SIEM (Security Incident and Event Management) system in place that the organization grants the admin rights under supervision so that the auditor can gather the required technical evidence to determine whether advanced audit logging and intrusion detection are utilized as required. The provided Identity and access management policy document has been given an evidence ID “E-11”. The auditor has evaluated the evidence and edited the last three paragraphs accordingly.

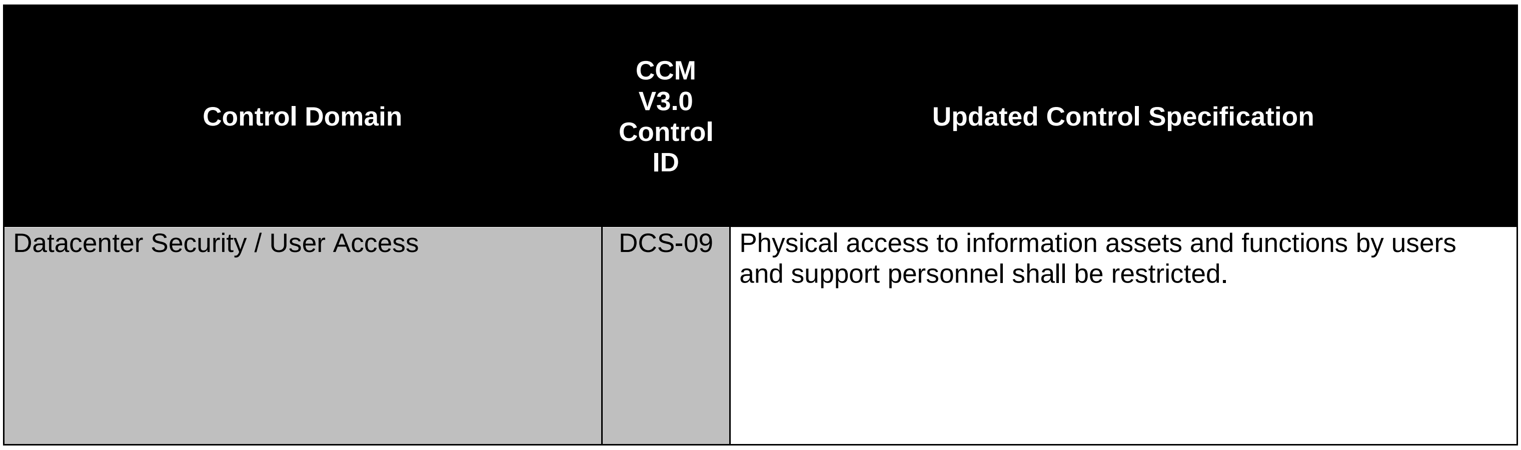
Evidence ID	Evidence requirement	Description	Applicability (Yes / No)	Compliance (In Place / Not in Place)	Notes
E-11	Repeatability / Reproducibility	The evidence collection must be repeatable under similar circumstances.	Yes	In Place	The audit logs could be successfully retrieved from the SIEM.
E-11	Trustworthiness / Integrity	The evidence must be provided by a trustworthy and appropriate Reference.	Yes	In Place	The evidence was retrieved from the organizations SIEM operated by SOC.
E-11	Sufficiency / Completeness	The evidence must provide enough information, etc. snapshot of a long enough timeframe.	Yes	In Place	An example of a previous suspected intrusion event was provided, the information was sufficient.
E-11	Appropriateness / Accuracy	The evidence must provide an answer as directly as possible to the respective requirement.	Yes	In Place	-

Table 11: Evidence evaluation checklist in practice, technical requirement.

As opposed to the previous example, in this case, the auditor did find the evidence to be conforming for all four requirements. No nonconformities were found when evaluating the quality of the evidence. Therefore, the evidence itself can be seen as sufficient and the CSA CCM control IVS-01 could be verified by the evidence.

6.4 Evaluation checklist for a physical requirement

In this example on a physical requirement, the auditee organization has assessed the physical risks and utilized a physical access control policy for premises accordingly. The policy includes a classification for physical assets and areas, and a policy based on "need-to-know" basis according to which the organization grants access rights to different personnel groups. For example, the office space would be accessible for all personnel, data center for network operations personnel only and physical documentation archives for information management unit only



Control Domain	CCM V3.0 Control ID	Updated Control Specification
Datacenter Security / User Access	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.

Table 12: CSA CCM requirement DCS-09, Datacenter Security / User Access

The provided physical access control policy for premises document has been given an evidence ID "E-4". The auditor has evaluated the evidence and edited the last three paragraphs accordingly.

Evidence ID	Evidence requirement	Description	Applicability (Yes / No)	Compliance (In Place / Not in Place)	Notes
E-4	Repeatability / Reproducibility	The evidence collection must be repeatable under similar circumstances.	Yes	In Place	The policy document follows the company documentation procedures, a journal number is included.
E-4	Trustworthiness / Integrity	The evidence must be provided by a trustworthy and appropriate Reference.	No	Not in Place	The policy covers all of the premises in the headquarters, however the new remote office in the city center has not been covered in the document.
E-4	Sufficiency / Completeness	The evidence must provide enough information, etc. snapshot of a long enough timeframe.	No	Not in Place	The access policies for headquarters have been thoroughly described, however the new remote office hasn't been mentioned.
E-4	Appropriateness / Accuracy	The evidence must provide an answer as directly as possible to the respective requirement.	No	Not in Place	Same as previous.

Table 13: Evidence evaluation checklist in practice, physical requirement.

In this specific case, the auditor has found the evidence requirements of repeatability/reproducibility to be in place. However, the document was outdated, and the risk management hadn't been varied out for all premises, specifically a new remote office had not been covered in the document. The auditor cannot accept the provided evidence as the requirements haven't been met. In this case, the auditor may request to visit the premises to observe and verify that the procedures in the documentation are in use. Interviews of physical security personnel such as the security manager and security guards may be needed to verify that the personnel in charge are up to date with the policy and have sufficient education and awareness to conduct the daily physical security duties.

6.5 The results of conceptualization and discussion

The conceptualized checklist provided three examples from actual requirements from the CSA CCM framework. The three example cases were selected by the type of evidence, administrative, technical and physical as covered in detail in subchapter 4.1. The selected requirements were chosen as they represented perhaps the best archetypes for each requirement and evidence type. The concept was found to be successful and applicable for evaluating the selected evidence cases. However, it is to be noted, that the sampling was very narrow and further research on applicability is needed to verify the usability in real-life cases. Also, the checklist concept doesn't include all of the discovered evidence evaluation qualities and guidelines, but only the ones appearing in multiple References.

An example of a quality that was excluded but could be applicable would be the *corroboration* of evidence as presented by Gray & Manson (2000, p. 161). There are numerous examples of potentially applicable controls, however including more controls or requirements into the checklist would require a further study and applicability test, potentially in the size of a doctoral dissertation. Also, including additional requirements or controls would make the concept tool possibly too heavy or complex for real-life use. As of now, a lighter, more generalist-level approach proves the point that a checklist can indeed be created for the intended use, breaking ground towards further research on the subject.

As discussed in subchapter 5.4, cognitive biases are a common pitfall in audit quality management, however there are several strategies to combat and mitigate the risk of having cognitive biases impacting the auditor's decision making and thus the audit overcome. Several of these cognitive bias combating strategies can be directly implemented by conducting the checklist concept. The checklist concept also covers strategies from each of the debiasing strategy categories, *general, specific, technological, motivational* and *cognitive* strategies. The individual strategies within these categories that the concept can be seen as applicable to are: *critical thinking, heterogeneity, quality management, increasing accountability of the decision maker (specific category), implementation of instructions, reframing, assessing uncertainty, quantitative methods, checklists, decision support systems, increasing accountability of the decision maker (motivational category), decomposing and restructuring the relevant information, perspective change from decision maker to an "outsider"* and *reviewing alternate hypotheses*.

The checklist covers 14 out of the 19 debiasing strategies presented by Westhausen (2019, p. 59). With further development, the checklist could cover the complete spectrum, however even at this state the concept can be assumed as useful in combating biased decision-making in information systems security auditing, including cloud security. In case the concept would be expanded to cover the rest of the requirements that it doesn't give a direct answer to, the concept would have to be reviewed and developed further form cognitive sciences point of view, such as psychology and possibly other sciences. The debiasing strategies presented by Westhausen that the concept doesn't take into account at its current state are *feedback, statistical analysis, debiasing awareness, training and education, monetary and non-monetary incentives* and *strengthening self-control*.

It should also be noted, that as in the scope of this study, only three example cases could be selected from one of nine recognized cloud security frameworks (see subchapter 2.4) at the time of conducting the research in 2019. While the frameworks overlap greatly with minimal national differences at best, the checklist may still yield different results depending on the framework. It is expected that the major cloud security frameworks are built rather similarly by structure, most importantly by requirement domain classification, requirement and control settings, implicating that the checklist concept would be applicable for at least ISO/IEC security management standards, the Finnish PiTuKri and of course the CSA CCM that the examples were derived from. However, it is uncertain whether the concept applies to other national standards such as the EuroCloud StarAudit Certification or the German frameworks Cloud Computing Compliance Controls Catalogue (C5) and TüV Rheinland Cloud Security Certification. Further concept testing and review should be conducted before taking the concept into further use, the testing would be best conducted in a broader research of its own, such as a doctoral dissertation.

As of now, in absence of further testing the concept should be used with consideration and approached as a pre-prototype with possible flaws, and the checklist outcome should be judged alongside with an experienced auditors' professional judgement. In its current state, the concept could be used by an experienced auditee either in the internal pre-audit self-assessment stage as a tool to help in creating compliant documentation and processes or an auditor in the external audit stage as assistance in judging the most unclear evidence before declaring it not applicable. This study concentrated mostly in qualitative evidence, as the majority of the requirements in cloud security frameworks are qualitative in nature. However, in case the checklist would be used with other auditing frameworks outside of cloud security, the frameworks could include requirements for which quantitative information collection is required.

The concept may also be beneficial in other types of auditing beyond cloud computing security, as the research material on which the quality requirements were concluded from was collected from various scientific References such as financial auditing and general information technology auditing. However, as the emphasis was on cloud computing security, the concept could be carried over to general information technology auditing with supposedly minor changes, applicability beyond IT, such as general corporate security management system auditing could require the concept to be significantly reworked and reviewed. At a glance, the core evidence qualities, *Repeatability, Integrity, Sufficiency* and *Appropriateness* could be seen as somewhat universal and adaptable for various qualitative assessments. However, it should be noted that the applicability must be considered carefully case-by-case in absence of further real-life case testing.

7 CONCLUSIONS

Through studying the qualities of evidence, it was found that just as in science, cloud security auditing evidence commands a repeatable outcome along with several other qualities. As information systems auditing frameworks still do not include guidelines for the actual evidence collection and review process, the research had to be taken beyond the scientific field of information technology. Having researched the definition of evidence along with the collection process from not only information systems security auditing but also scientific disciplines beyond information technology, it was concluded that a set of qualities that evidence must meet universally indeed exists. These qualities could be used as guidance when evaluating evidence collected for assessing a cloud computing systems security compliance.

The research also revealed that both of the audit parties, the auditor and the auditee are potentially fallible to human errors in their decision-making process. The root cause of this fallibility are the participant's personal biases, that may have an adverse effect on the evidence evaluation and thus the independency and outcome of the audit process. This finding further points out the need for an external guideline or a structured process that would mitigate the effect of biased evidence evaluation results. Based on a study of scientific evidence evaluation, the most common evidence qualities were narrowed down and a concept checklist tool was created based on the qualities.

The four common qualities for evidence were (1) *Repeatability/Reproducibility*, (2) *Trustworthiness/Integrity*, (3**)** *Sufficiency/Completeness* and (4) *Appropriateness/Accuracy*. All of the aforementioned qualities of evidence were commonly met in the evidence definitions in the scientific fields economics (financial auditing) that shares a very similar evidence collection process as information system auditing as found out in the study. The four qualities could be carried over to cloud security auditing as a toolkit to help in reviewing the collected evidence as presented in the form of theoretical checklists included in the study.

As this thesis concentrated only in cloud security assessment, the qualities and checklists could perhaps be applied in other demanding security auditing processes beyond cloud computing as well, such as general information systems security or even corporate security beyond information technology. Ultimately, summing up the four universal qualities, the evidence can be seen to be answering to the needs of an auditor if conclusions can be made based on the evidence. In practice, this means an outcome of either *compliant* or *non-compliant* depending on the requirements under review. If the evidence fails to meet the four qualities, the outcome would be N/A as in not available/applicable, meaning that the requirement couldn't be evaluated in the first place.

It is to be noted that in security auditing only a minor part of the collected evidence requires further evaluation for which the proposed evaluation tool, (chapter 7) would be helpful in. At the time of conducting the research the majority of the requirements in the cloud-specific security frameworks were qualitative in nature, thus demanding qualitative evidence. In case new frameworks emerge with emphasis on quantitative investigation, the limits of the checklist concept should be recognized, and the applicability considered carefully. If the evidence collected for such framework would be thoroughly evaluated, the evidence evaluation tool should be developed accordingly. However, as for the existing cloud security-specific frameworks at the time of writing, the checklist concept is mostly applicable.

It is only the most difficult requirements that can be verified with multiple different types of evidence that may need a further evaluation against the common qualities found in the research. However, the evaluation tool may become beneficial for both the auditor and the auditee, as for the auditor the evidence evaluation process is rather straightforward, the auditee may find use in the tool even before establishing an official external audit. The auditee can use the tool in their internal evaluation process, assuming that the requirements are understood correctly in creating a solid service enabling a smooth audit process with possibly great savings in required working hours and avoiding delays in the absence of evidence. A seasoned auditor or a cloud security subject matter expert will most likely find little to no help in using the evaluation tool as the evidence qualities may be self-explanatory, however the tool concept may prove to be useful especially for IT-professionals new to information system auditing or compliance in general.

REFERENCES

Anantha, S. (2002) The IS Audit Process. *Information Systems Control Journal, Volume 1, 2002* Retrieved from: http://harbert.auburn.edu/~cegieca/5960/IS_audit_process.pdf

Biegelmann, M. (2008) Building a World-Class Compliance Program, John Wiley & Sons Inc.

Caracelli, V.J., & Cooksy, L. J. (2013) Incorporating qualitative evidence in systematic reviews: Strategies and challenges. In *Mixed methods and credibility of evidence in evaluation. New Directions for evaluation.* Mertens., D. M., Hesse-Biber, S. Jossey-Bass, San Fransico, CA. Retrieved from: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/det ail.action?docID=1216101

Carstensen, J., Golden, B., Morgenthal, JP. (2012) Cloud Computing – Assessing the risks, IT Governance Publishing, Cambridgeshire, United Kingdom

Cloud Security Alliance, CSA STAR Certification Retrieved from: https://cloudsecurityalliance.org/star/certification/#_overview)

Cloud Security Alliance, Cloud Controls Matrix Retrieved from: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3/

Duggan, S. & Gott, R. (2011) Introduction In*: Understanding and using Scientific Evidence.* London: SAGE Publications, Ltd. Retrieved from: https://dx.doi.org/10.4135/9780857020161

European Cyber Security Organisation (ECSO), Overview of existing Cybersecurity standards and certification schemes, December 2017 Retrieved from: https://www.ecs-org.eu/documents/uploads/updated-sota.pdf

European Union Agency for Network and Information security (ENISA) (August 2014), Cloud Standards and Security. Retrieved from: https://resilience.enisa.europa.eu/cloud-security-and-resilience/Cloudstandards.pdf

Fischer, M. J. (1996) "Real-izing" The benefits of new technologies as a Reference of audit evidence*: An interpretive field study*. St. Bonaventure University.

Fitzgerald, T. (2012) Information Security Governance Simplified CRC Press, London.

Flick, U. (2011) Introducing Research Methodology. London: Sage Publications.

Gantz, S. (2013) The Basics of IT Audit: *Purposes, Processes, and Practical Information.* Elsevier Science & Technology Books Retrieved from: https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/reader.action?docID=1550527&query=compliance%2Bauditing

Generally Accepted Auditing Standards (AICPA) Retrieved from: https://www.aicpa.org/Research/Standards/Audi tAttest/DownloadableDocuments/AU-00150.pdf

Gray, I., Manson, S. (2000) The Audit Process – Principles, Practice and Cases (Second Edition) Thomson Learning.

Gul, I., Ur Rehman, A., Islam, M. H., (2011) Cloud computing security auditing, the 2nd International Conference on Next Generation Information Technology (ICNIT), Gyeongju, Retrieved from: https://ieeexplore.ieee.org/abstract/document/5967489

Harrison K.E., Srivastava R.P., Plumlee R.D. Auditors' Evaluations of Uncertain Audit Evidence: Belief Functions versus Probabilities. In *Belief Functions in Business Decisions.* Srivastava R.P., Mock T.J. Studies in Fuzziness and Soft Computing, vol 88. (2002) Physica, Heidelberg. Retrieved from: https://doi.org/10.1007/978-3-7908-1798-0_6

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 19011:2011 Guidelines for auditing management systems

ISO 17000:2004 Conformity assessment -- Vocabulary and general principles

ISO/IEC 9000:2005 Quality management systems -- Fundamentals and vocabulary

Jesson, J., Matheson, L., Lacey, F. (2011) Doing Your Literature Review. London: Sage Publications.

KATAKRI 2015 – Information security audit tool for authorities Retrieved from: http://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Knoblauch, D. (2017) European Security Certification Framework deliverable 2.2 Continuous Auditing Certification Scheme Retrieved from: https://cdn0.scrvt.com/fokus/1edfbe2d5ab52e28/e2dd1ac7870b/D2.2-Continuous_auditing_certification_scheme_V1.pdf

Marris, D. (2010), Challenges Obtaining Audit Evidence. SSRN Retrieved from: http://dx.doi.org/10.2139/ssrn.1590634

Marchetti, A.M. (2012) Enterprise Risk Management Best Practices: *From Assessment to Ongoing Compliance*. John Wiley & Sons. New Jersey.

Montesino, R., Fenz, S. (2011) Information security automation: how far can we go? *IEEE Xplore* Retrieved from: http://ieeexplore.ieee.org/document/6045951/

Morse, J., Swanson, J., Kuzel, A. (2001) The Nature of Qualitative Evidence. Sage eBook. Retrieved from: https://dx.doi.org/10.4135/9781412986236

Okoli, C. & Schabram, K. (2010) A Guide to Conducting a Systematic Literature *Review of Information Systems Research.* Retrieved from: http://www.nti.ufpb.br/~evandro/pesquisa/RSL/(Okoli,%20Schabram%202010%20Sprouts)%20systematic%20literature%20reviews%20in%20IS%20research.pdf

PiTuKri – Pilvipalveluiden turvallisuuden arviointikriteeristö, NCSA-FI Retrieved from: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf

Ratsula, N. (2016) – Compliance – Eettinen ja vastuullinen liiketoiminta. Helsinki: Talentum

Rezaee, Z., Elam, R., Sharbatoghile, A. (2001) Continuous auditing*: The audit of the future Managerial Auditing Journal, Vol. 16 Issue: 3* Retrieved from: http://www.emeraldinsight.com /doi/pdfplus/10.1108/026869001 10385605

Ryoo, J., Rizvi, S., Aiken, W., Kissell, J. (2014) Cloud Security Auditing*: Challenges and Emerging Approaches*. IEEE Security & Privacy, Volume: 12. Retrieved from: https://doi.org/10.1109/MSP.2013.132

Salazar, D. (2016) Cloud Security Framework Audit Methods, SANS Whitepapers Retrieved from: https://www.sans.org/reading-room/whitepapers/cloud/cloud-security-framework-audit-methods-36922

SAS 106 – Audit Evidence (AICPA) Retrieved from: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadable documents/au-00326.pdf

Siponen, M., & Willison, R. (2009*). Information security management standards: Problems and solutions*. Information & Management, Volume 46, Issue 5, June 2009 Retrieved from: https://doi.org/10.1016/j.im.2008.12.007

Schwandt, T.A. "Toward a Practical Theory of Evidence for Evaluation" in *What counts as credible evidence in applied research and evaluation practice?* Stewart I. Donaldson, Christina A. Christie & Melvin M. Mark (2009) SAGE Research Methods. Retrieved from: https://dx.doi.org/10.4135/9781412995634.d18

Stufflebeam, D.L. (2011) "Meta-Evaluation" Journal of MultiDisciplinary Evaluation, Vol 7, No.15, February 2011. Retrieved from: https://eric.ed.gov/?id=EJ916544

Takabi, H., Joshi, J.B.D., Ahn, G-J. (2010) Security and Privacy Challenges in Cloud Computing Environments IEEE Security & Privacy (Volume: 8, Issue: 6, Nov.-Dec. 2010) Retrieved from: http://ieeexplore.ieee.org/abstract/document/5655240/?reload=true

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems.* Communications of the Association for Information Systems. Volume 37, Article 6. Retrieved from: https://doi.org/10.17705/ 1CAIS.03706

Thampi, S., Bhargava. B., Atrey. P. (2014) Managing trust in Cyberspace. CRC Press, London

Vladimirov, A., Gavrilenko, K., Michajlowski, A. (2014) Assessing Information Security – *Strategies, tactics, logic and framework.* Second edition. IT Governance Publishing, UK Retrieved from: http://search.ebscohost.com/login.aspx?drect=true&db=nlebk&AN=957891&site=ehost-live

Westhausen, H-U. "Cognitive Biases in Internal Auditing" in *Auditing – an overview*, Cavenagh, T., Rymill. J. (2019) New York: NovaScience Publishers, Inc

Wright, C. (2016) Fundamentals of information risk management auditing – *An introduction for managers and auditors.* IT Governance Publishing, Cambridgeshire, UK

Zuca, S. (2015) "Audit Evidence – Necessity to Qualify a Pertinent Opinion" in *Procedia Economics and Finance, Volume 20.* Airinei, D., Pintilescu, C., Viorica, D., Asandului, M. Science Direct. Retrieved from: https://doi.org/10.1016/S2212-5671(15)00126-4

8 APPENDIX 1 SUMMARY OF REVIEWED TEXTS

Title	Author(s)	Subject(s)	Year
The IS Audit Process	Anantha, S.	Auditing, information security management systems	2002
Building a World-Class Compliance Program	Biegelmann, M.	Auditing, assurance, assessment, compliance	2008
Incorporating qualitative evidence in systematic reviews: Strategies and challenges	Caracelli, V.J., & Cooksy, L. J.	Evidence evaluation	2013
Cloud Computing – Assessing the risks	Carstensen, J., Golden, B., Morgenthal, JP.	Cloud security, information security, assessment	2012
CSA STAR Certification	Cloud Security Alliance	Cloud security framework	2015
Cloud Controls Matrix	Cloud Security Alliance	Cloud security framework	2017
Introduction In*: Understanding and using Scientific Evidence*	Duggan, S. & Gott, R.	Evidence collection, evidence evaluation	2011
Overview of existing Cybersecurity standards and certification schemes	European Cyber Security Organisation (ECSO)	Cloud security framework	2017
Cloud Standards and Security	European Union Agency for Network and Information security (ENISA)	Cloud security framework	2014
"Real-izing" The benefits of new technologies as a reference of audit evidence*: An interpretive field study*	Fischer, M. J.	Audit evidence, audit process, evidence collection	1996
Information Security Governance Simplified	Fitzgerald, T.	Information security management systems	2012
The Basics of IT Audit: *Purposes, Processes, and Practical Information*	Gantz, S.	Information security management systems, auditing	2013

		assurance, evidence collection	
Generally Accepted Auditing Standards	American Institute of Certified Public Accountants	Auditing, evidence collection, evidence evaluation	2011
The Audit Process – Principles, Practice and Cases	Gray, I., Manson, S	Auditing, assurance, assessment, evidence collection, evidence evaluation	2000
Cloud computing security auditing	Gul, I., Ur Rehman, A., Islam, M. H.	Cloud security, auditing	2011
Auditors' Evaluations of Uncertain Audit Evidence: Belief Functions versus Probabilities	Harrison K.E., Srivastava R.P., Plumlee R.D.	Auditing, assessment, evidence collection, evidence evaluation	2002
ISO/IEC 27001:2013	International Organization for Standardization	Requirements, Information security management systems	2013
ISO/IEC 19011:2011	International Organization for Standardization	Auditing, assessment, framework	2011
ISO 17000:2004	International Organization for Standardization	Auditing, assessment, framework	2004
ISO/IEC 9000:2005	International Organization for Standardization	Auditing, evidence, framework	2005
KATAKRI 2015 – Information security audit tool for authorities	Ministry of Defence, Finland	Framework, information security management systems	2015
European Security Certificatio Framework deliverable 2.2 Continuous Auditing Certification Scheme	Knoblauch, D.	Cloud security, auditing, framework	2017
Challenges Obtaining Audit Evidence	Marris, D.	Auditing, assurance, assessment, evidence collection	2010
Enterprise Risk Management Best Practices	Marchetti, A.M.	Risk and security management systems	2012

Information security automation: how far can we go?	Montesino, R., Fenz, S.	Information security, auditing, assessment	2011
The Nature of Qualitative Evidence	Morse, J., Swanson, J., Kuzel, A.	Evidence collection, evidence evaluation	2001
PiTuKri – Pilvipalveluiden turvallisuuden arviointikriteeristö	Finnish National Communications Security Authority	Cloud security framework	2019
Compliance – Eettinen ja vastuullinen liiketoiminta	Ratsula, N.	Evidence, evaluation, compliance, management systems	2016
Continuous auditing*: The audit of the future*	Rezaee, Z., Elam, R., Sharbatoghile, A.	Information security, compliance, auditing	2001
Managing trust in Cyberspace	Thampi, S., Bhargava. B., Atrey. P.	Auditing, assurance, information security, compliance	2014
Assessing Information Security – *Strategies, tactics, logic and framework*	Vladimirov, A., Gavrilenko, K., Michajlowski, A.	Evidence evaluation, evidence collection, information security, framework	2014
Cognitive Biases in Internal Auditing	Westhausen, H-U.	Evidence, evaluation, cognitive biases	2019
Fundamentals of information risk management auditing – *An introduction for managers and auditors*	Wright, C.	Auditing, assessment, information security management systems	2016
Audit Evidence –Necessity to Qualify a Pertinent Opinion	Zuca, S.	Evidence collection, evaluation, auditing, assesment	2015