UNIVERSITY
OF TWENTE.

Master Thesis

Risk Management in Cloud Environments: Towards the Adoption of Continuous Auditing and Assurance With EU-SEC

Author:

Sander Bannink
s.n.bannink(a)alumnus.utwente.nl

Supervisors:

Jos van Hillegersberg
Marten van Sinderen
University of Twente

Dayenne van Winden
Ralf Wijne
EY

Electrical Engineering, Mathematics and Computer Science (EEMCS)
Business Information Technology

August 31, 2018

Summary

Cloud computing has impact on risks compared to traditional in-house dedicated IT infrastructure. Especially financial service organizations rely heavily on compliance reporting and assurance since it is a legal obligation. IT assets are no longer placed in-house but organizations are still legally accountable. Since there is less control, assurance reports and Service Level Agreements are key in managing risks concerning the cloud. They however only provide assurance in retrospect and are point-in-time, which proves to be a big shortcoming in risk management and control.

Continuous auditing intends to solve these issues by providing continuous compliance reporting, based on measurements within the infrastructure and data analysis to reflect this into control testing and compliance. This solves the issue of conventional audits by providing constant feedback. This research is conducted within three financial service organizations and two auditing firms within The Netherlands.

The research objective is to provide insights in risk management and continuous audit developments and determine if continuous auditing can improve cloud risk management and control. The European Security Certification Framework (EU-SEC) aims to provide an EU-wide standard for continuous auditing. Continuous auditing with EU-SEC is investigated, the adoption drivers and barriers are researched by semi-structured interviews. This study concludes that continuous auditing with EU-SEC is a viable addition to current cloud risk control, but several drivers and barriers for adoption need to be taken into account.

Advantages of EU-SEC are that it covers gaps in current risk management and information needs, can be used throughout the EU and may become an industry-wide standard. Barriers to adoption are the willingness for cloud providers to provide information continuously, the uniqueness of their infrastructures, the tailored data-feed for each customer's specific system and the fact that not all controls can be automated. Regulators can stimulate the adoption of continuous auditing by new EU-laws for financial services. When several organizations adopt EU-SEC, it can gain a critical mass which boosts adoption. Additionally the standard should be governed by a governing body, accreditations should be given to ensure EU-SEC becomes an industry standard.

The conducted semi-structured interviews in this research give a consistent overview of the perceived drivers and barriers of EU-SEC, but cannot be generalized to the whole financial sector because of the different nature of the interviewed organizations. They however face the same developments and needs concerning risk control and continuous auditing of cloud computing, which provides support for the findings in this research.

Overall this research contributes to the knowledge of continuous auditing, risk management and the information needs of cloud customers. The cooperation of different stakeholders in this sense is a key driver in adoption of an EU-wide standard. Future research can further improve the EU-SEC framework and prove the viability through pilots, validating if EU-SEC has the potential to grow to an industry-wide standard in cloud environments.

Contents

List of Figures

List of Tables

Acronyms

AAA – American Accounting Association
ACM – Association for Computing Machinery
AICPA – American Institute of Certified Public Accountants
API – Application Programming Interface
APT – Advanced Persistent Threats
ASP – Application Service Provider
BSI – British Standards Institution
CCM – Cloud Control Matrix
CCS CSC – Critical Security Controls for Effective Cyber Defense
CES – Cyber Essentials Scheme
COBIT – Control Objectives for Information and related Technology
CSA – Cloud Security Alliance
CSP – Cloud Service Provider
DDoS – Distributed Denial of Service
DNB – De Nederlandsche Bank (Dutch Central Bank)
EBA – European Banking Authority
EDoS – Economic Denial of Service
EU – European Union
EU-SEC – European Security Certification Framework
EY – Ernst & Young
FSO – Financial Services Organizations
GDP – Gross Domestic Product
GDPR – General Data Protection Regulation
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronics Engineers
ISAE – International Standard on Assurance Engagements
ISO – International Organization for Standardization
IT – Information Technology
IaaS – Infrastructure as a Service
NIST – National Institute of Standards and Technology
OCF – Open Certification Framework
PCI DSS – Payment Card Industry Data Security Standard
PaaS – Platform as a Service
PwC – PricewaterhouseCoopers
SAS – Statements on Auditing Standards
SLA – Service Level Agreement
SLO – Service Level Objective
SOA – Service Oriented Architecture
STAR – Security, Trust & Assurance Registry
SaaS – Software as a Service
TOE – Technology Organization Environment
VMs – Virtual Machines
WFT – Wet Financieel Toezicht

Chapter 1

Introduction

Cloud is an ambiguous term that means a lot more than only your Dropbox, iCloud, OneDrive or Google Drive storage. Cloud is a technology that can be used to provision IT storage and processing capabilities on-demand. Consequence of this is that businesses don't need to invest in IT-hardware and -infrastructure by themselves but can rent these assets in a flexible way. The costs are based on pay-per-use, there is no need for long-term investments in hardware. Only the needed capacity will be requested by the tenant, which provides a flexible cost structure. In the past years the developments in IT infrastructure, hardware and networking dropped significantly which resulted in the possibility to host IT assets off-site.

Cloud computing is a technology that continues to grow in the coming years. The European Commission made an estimate in 2012 that by 2020 €160 billion (1%) of the EU GDP will be generated by public cloud services and 2,5 million extra jobs will be created [28]. Cloud can also expand possibilities for entering new markets and development of new products.

1.1 Cloud computing

Cloud computing in itself can be broadly defined as: the flexible provisioning of IT resources. In this section the history and definition of cloud is given, the different types of cloud and their characteristics are shown and their associated risks are summarized.

1.1.1 History of cloud computing

Cloud computing can be seen as outsourcing of IT assets. The first form of 'on demand' IT assets came up in the '90s of the last century. Software vendors were looking for a way to rent their packages together with the needed computing power. The 'application service providers' (ASPs) used the Internet to offer application services on a rental basis [56]. In this traditional form of outsourcing the customer rents the complete infrastructure from a service provider, including the required hardware or software. Administration is done by the service provider [24]. Business processes get partly or fully outsourced to a third-party service provider. The customer is renting a certain infrastructure and exclusively using it, which is called a 'single-tenant' model [24].

Virtualization is a means to 'simulate' a server, which is called a virtual machine (VM). Multiple virtual machines can be hosted on a single server and are isolated. Virtual machines can be provisioned on-demand which makes it possible to use IT resources more efficiently and flexible. Strong authentication, authorization, and accounting procedures establish security for the data in transit, locking down network and hardening operating systems, middleware and applications to avoid security concerns. Visualization offers better forensic capabilities, faster recovery of an attack, safer and more effective patching, better control over desktop resources and more cost-effective security devices [4]. This paved the way for developments and investments in networking infrastructure, computing technologies and rental-based cost structures which would later prove to be the predecessor of cloud computing. In cloud computing the customer is also renting a certain infrastructure but shares it mostly with others, which is called the 'multi-tenant' model [24]. The data center floor space, power, cooling and operation expenses could be used more efficiently by visualization. By virtualizing the infrastructure and offering it to multiple customers, service providers could change their business model to provide remotely managed services at a lower cost. Services became more distributed, management of these services resulted in the development of a service-oriented architecture (SOA) [5]. Businesses no longer needed to invest in IT assets to host their applications on-premises but could outsource this on a subscription basis. Cloud computing developed out of this need to provide IT resources 'as-a-service' [5].

1.1.2 Defining 'the cloud'

In this research 'the cloud' definition of the National Institute of Standards and Technology (NIST) is used. NIST is the oldest physical science laboratory in the United States of America, which is funded by the US government. It executes technology research and is the developer of one of the industry's most well-known security management standards for IT infrastructures. NIST defines cloud as:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."* [42]

NIST defines the characteristics of cloud as: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [42]. This shows the characteristic flexibility of cloud environments. Cloud comes in three services models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [42]. Providing respectively only infrastructure/hardware, additionally an operating system (platform) or everything including software. The cloud also comes in four deployment models: Private cloud, Community cloud, Public cloud and Hybrid cloud. Each of them have their own characteristics [42]. In Section 1.1.3 and 1.1.4 the different types of cloud are further defined.

1.1.3 Service Models

Cloud computing has three different service models: IaaS, Paas and SaaS [42] which are explained below [2]:

1. ***Infrastructure as a Service (IaaS)*** The most basic form of cloud where the infrastructure (e.g. hardware, storage, network) are provided but the consumer can run his own platform and applications. The customer has limited or no control over hardware and network components.

2. ***Platform as a Service (PaaS)*** Not only the hardware, network and storage are provided but also the platform (operating system) on which the customer can deploy their applications. The customer has no control over the infrastructure including operating system, but has control over the deployed applications and configurations for the applications.

3. ***Software as a Service (SaaS)*** This covers the whole infrastructure, including network, storage, operating system and applications. The customer only has limited control over the configuration of the applications. Applications are accessible on different devices and platforms through web browsers or an interface.

1.1.4 Deployment Models

NIST [42] defines four deployment models of cloud computing which are explained below [2]:

1. ***Private cloud*** The cloud infrastructure is used by a single organization and managed by the organization itself or a third party. The infrastructure may exist on or off premises.

2. ***Community cloud*** The cloud infrastructure is for exclusive use of members of a specific community or a group of organizations that share the same needs. It is managed by one of the organizations of the group or a third party. The infrastructure may exist on or off premises.

3. ***Public cloud*** The cloud infrastructure can be used by the general public. It can be managed by any organization and exists on premises of the cloud provider.

4. ***Hybrid cloud*** A combination of the above types. The cloud infrastructure is a composition of two or more types that are bound together by technology to enable data and application portability.

1.2 Cloud characteristics

Cloud computing can be seen as the outsourcing of IT assets. It is similar to classic IT outsourcing, where the client transfers the custody of parts of its information systems to a service provider [38]. The cloud computing paradigm differs from the characteristics of classic IT outsourcing: the outsourcing provider offers a 'customized and unique service' that does exactly what the client requests at the client's terms, in a 'well-controlled and discrete environment' [38]. Cloud computing offers highly standardized services to multiple customers from a shared IT infrastructure. Cloud computing offers some kind of customization but its main purpose is to offer a 'one-size-fits-all' solution. Because the usage of a shared IT infrastructure across clients, it limits the ability to have the same level of control known from classic IT outsourcing [38].

1.3 Cloud benefits

Cloud computing has multiple potential benefits, like savings on IT investment costs and lower maintenance; no hardware needs to be bought and the support is included. Costs for running servers (like power, cooling and space) are moved to the cloud provider. This reduces operational costs because only the used capacity is paid. Cloud computing offers flexibility and agility in computing platforms which improve scalability and access to high-performance resources. These resources typically have a high reliability and availability. When using cloud, there is a high advantage because of economies of scale [4, 5]. "Benefits for business and IT include reduced costs, scalability, flexibility, capacity utilization, higher efficiencies and mobility. Many of these cloud computing benefits are achieved through virtualization." [4].

1.4 Cloud risks

Businesses are increasingly moving their IT assets to the cloud, thus the risks for the usage of cloud environments need to be taken into account. Mitigating risks in cloud environments is a big challenge, because the IT-assets (infrastructure and data) are not located in-house. Therefore some additional challenges that need to be tackled. Risk assessments need to be done to ensure that all risks are addressed. The European Union Agency for Network and Information Security (ENISA) published an overview of perceived risks when using cloud solutions [12] which was also adopted by the Dutch Central Bank (DNB) as the starting point for risk management guidelines and classification. Previous research by Bannink [2] provided a risk categories framework which in his study was used to map the most used risk management standards and gaps were identified. Traditional IT control frameworks lacked mainly on the Virtualization, Identity & Access Management, Datacenter Security and Encryption in the context of cloud computing.

When using cloud computing there is an increased risk profile, because the infrastructure, platform, data and applications are no longer located in-house. Chapter 3 will elaborate on the risks that come with cloud computing and the way to handle them.

1.5 Cloud risk management

Standards have been developed to cope with risks in IT and cloud solutions, which give a set of guidelines and controls to reduce these risks. The two most widely applied security management frameworks, ISO 27001 and NIST 800-53, are lacking to cover all identified cloud risks [2]. This poses a problem in making cloud a viable solution in the financial world, where highly sensitive data such as Personally Identifiable Information (PII) and financial information is processed. Since IT assets are not located in-house, being 'in control' of these assets is a big challenge. Research of Julisch et al. [38] in 2010 pointed out that new security challenges arise with cloud computing and SLAs are mainly used to stipulate legal accountability between cloud providers and cloud customers. Transference of risks doesn't solve the lack of control over cloud computing. Companies are accountable for their assets, including assets that were outsourced to a cloud provider. Cloud computing transfers the responsibility to complete a specific task to the cloud provider, but accountability remains with the cloud customer [38]. The main message to cloud providers in this research [38] was to reveal their controls and allow clients to monitor the CSP's controls. Since risk transference is not the solution (because legal accountability stays with the cloud customer), CSPs and cloud customers should work together to provide transparency and align their risk management practices.

Conventional security audits only provide an infrequent 'snapshot' of the cloud provider's control environment and the cloud customer has to trust that everything is 'OK' between certifications, this is unacceptable since the cloud customer can be held accountable for the security and compliance of their systems [38]. Infrequent reporting about the effectiveness of controls and risk management from the CSP side, is not enough to cover current information needs for cloud customers who want to be in control. Additionally, the ISAE 3402 framework is not a certification by itself but rather a framework for conducting audits. It does not specify any specific controls but the cloud provider defines their own control objectives of which it wants to be certified for [38]. Service-level agreements (SLAs) tend to be conservative and typically transfers risk to the cloud provider. The potential results of a control failure can be a penalty payment or loss of customers for the cloud provider. The cloud customer remains accountable towards its own customers, regulators and directors for any failures, for which a control failure can have an immense impact [38]. As such, cloud customers want to align their risk management process with their CSP's. Monitoring of risks and involvement in risk management of the CSP will be the key in this sense.

1.6 Continuous assurance in cloud

Additional measures need to be taken in order to address the disconnect in current risk management frameworks between CSPs and cloud customers, and to provide improved assurance in cloud environments. Conventional security certifications and assurance frameworks test security management by documenting the presence of controls at a moment in the past, instead of proving their real-time effectiveness which can for example be done by adopting continuous monitoring and assurance frameworks in cloud environments. IT assets with the highest risks (like PII or financial information) need additional security management controls for the cloud customer to be able to prove they are 'in control'. To monitor the effectiveness of risk management controls, real-time data analytics can be used as input for security audits. This satisfies information need of cloud customers as well, providing insight to be more in control.

1.7 Research goal

In this research the developments in risk management and continuous auditing of cloud computing are investigated to determine if they cover the gaps in current cloud risk management standards and identify the challenges in adoption. The term 'continuous auditing' can be used in multiple contexts: this research specifically focuses on the information security risks management and not the financial auditing part. Additionally the adoption drivers and barriers of continuous auditing for cloud in financial services organizations are investigated. Three financial services organizations are part of the empirical research, as well as two auditing and certification bodies. In the preparation phase, Cloud Security Alliance (CSA) chapter Netherlands was consulted for suggestions. They pointed out the European Security Certification Framework (EU-SEC) project, which provide a continuous auditing framework that can be used EU-wide.

The EU-SEC project was set-up by a consortium of multiple participants, among others the Fraunhofer Institute (Germany), Cloud Security Alliance Europe (United Kingdom), Nixu (Finland), PwC (Germany), Barclays Bank (United Kingdom) and the Slovenian government are taking part in the project [30]. EY (Ernst & Young CertifyPoint) is part of the advisory board. Since this is the only industry-wide and widely supported continuous auditing framework today which can be used throughout the EU, EU-SEC was used as research artifact. In this empirical research, the drivers and barriers for the adoption of the EU-SEC continuous auditing framework are investigated. Suggestions for the adoption and key enablers for this adoption are given.

1.8 Research outline

The outline of this thesis is as follows: Chapter 2 provides the problem statement, research questions and methodology. Chapter 3 elaborates on cloud risk management by a systematic literature research. Chapter 4 defines the principles and state of art in continuous auditing and introduces the EU-SEC framework. Chapter 5 identifies the drivers and barriers to the adoption of EU-SEC by empirical evaluation through semi-structured interviews, which are reflected to an adoption framework. Chapter 6 concludes this research by presenting the findings: key adoption drivers and barriers. Chapter 7 discusses the findings and gives suggestions for future research.

Chapter 2

Research design

This chapter formulates the context, motivation, scope, relevance, problem statement and research questions.

2.1 Context

This research is performed in cooperation with EY (Ernst & Young) as part of a graduation internship. EY is a global accounting, audit and advisory firm which provided the resources to execute this research within the IT Risk & Assurance department in The Netherlands that serves financial service organizations. Preliminary research was performed by a literature research and mapping of the most well known risk management standards [2] as a foundation and motivation for this research. Several experts within EY have given their input through interviews, to come up with a relevant research topic. Concluding that information security risk standards provide controls to manage risks, but don't provide a statement of real-time effectiveness of security measures which has proven to be a limitation in current cloud environments.

In the financial world there is a legal obligation to comply with supervisory demands and regulatory requirements. Financial service organizations are typically under supervision of the national central bank or financial authorities, which is the case in almost every country. Each country within the EU produces its own set of rules on where financial companies have to comply to, in the field of risk assessment/management and security controls. EU regulation is set as a basis of these regulations, but additional local regulations may be applicable as well. These regulations are of high importance to comply with, especially because of the high volumes of personal and financial data contained by IT systems in the financial world.

2.2 Scope

This research focuses on financial services organizations as they are under special regulations concerning supervision and risk management. This deliberate choice is made because of the highly sensitive data contained by financial services and that this research is committed in the Risk Assurance (Financial Services Organizations) part of EY Netherlands.

Specific regulations concerning financial services organizations in The Netherlands will be considered in this research, as well as the EU-wide regulations that are applicable to all financial services within the EU. In this way the results are generalizable throughout the EU financial services industry.

This research aims to provide insights in the drivers and barriers to adoption of a cloud security monitoring and auditing framework for continuous assurance. The feasibility and validation of the technical implementations of continuous monitoring are out of scope of this research, since these validations are done within external pilots.

2.3 Relevance

The relevance of this research can be seen from three perspectives.

1. *Cloud customer*: from a customer perspective the risk management of cloud solutions can be improved. For cloud customers it's important to be able to prove they are 'in control' of their own data, since they can be held accountable for possible data breaches or security issues at their provider. One way to ensure risk mitigation is by making additional arrangements in a Service Level Agreement (SLA) for the cloud provider to provide assurance that sufficient risk management measures are in place. These risk management measures also need to be properly implemented and effective. Currently this is done by showing compliance with risk management standards, which is checked and reported on. However, these reports only provide assurance in retrospect and do not provide insights in the current risk management and compliance of the cloud environment. There is no standard that proves assurance continuously and thus there is need for an additional framework that covers gaps in current practices. Possible solutions can be better monitoring of cloud environment in cooperation with the provider, which can serve as an input to compliance reporting and Third Party Audits. In this way providing assurance that the cloud customer is in control of their information assets and that the risk management process of the CSP is in aligned with that of the cloud customer.

2. *Cloud auditor*: from an auditing perspective there is no standard way to audit cloud providers. Current security management frameworks only specify what is needed, but not how to properly implement it. They provide security in retrospect, instead of 24/7 control and monitoring [2]. There is a need for additional information about the effectiveness of security controls at the CSP, in a more continuous manner in contradiction to point-in-time audits. Automated audits (continuous auditing) can be a possible solution to this problem. This improves audit practices and improves assurance, compared to the common 'checklist' control sampling. Continuous audits can also serve as input for conventional audits, as they provide additional information that is based on real-time data analysis in stead of control sampling.

3. *Science*: in a scientific context this research is relevant to gain more knowledge about the gaps in current risk control frameworks concerning cloud. Related work has shown that compliance with standards is not sufficient to be in control of all perceived risks in cloud environments [2]. Cloud risk management practices need to be further extended to come up with a complete framework to provide assurance in the cloud. Additional measures in the form of infrastructure monitoring or continuous auditing should be implemented to accomplish this. Improvement of audit practices also gains attention in the scientific world, Chou [9] emphasized that auditors must be familiar with cloud computing and follow auditing methods that comply with regulations from auditing authorities. Automated certification of cloud solutions by the use of monitoring or continuous auditing can improve service quality in a matter that cannot be accomplished

by regular on-site audits [2]. The development of continuous auditing frameworks and the drivers/barriers concerning adoption of these standards need to be researched to make it a feasible solution.

This research contributes to the knowledge of continuous monitoring and continuous auditing in cloud environments, additionally it gives suggestions on the key success-factors of the adoption of continuous auditing in financial services.

2.4 Problem statement

Financial services organizations are gradually adopting cloud computing, but their adoption approach is not yet mature. The majority of financial services organizations still rely on in-house infrastructure [52]. Financial service organizations and supervisory authorities have a clear view of the benefits of cloud adoption, yet they remain cautious about the risk of losing control over their information assets [52]. Since no cloud risk standard covers all needs in practice, there is need for a complete cloud risk framework that can test the effectiveness of controls continuously and monitor cloud environments in order to provide continuous assurance. This proves to be a big challenge because of the immense amount of standards, regulations and technology involved.

The Cloud Security Alliance (CSA) addresses cloud-specific controls and in their CloudAudit initiative they created a formalized and standardized approach towards auditing cloud solutions. This resulted in the EU-SEC initiative in which several industry partners cooperate to leverage an industry-wide continuous auditing standard. EU-SEC is funded by the European Commission and addresses the burden of standards and national regulations. It provides EU-wide requirements for continuous auditing using existing standards and provides a framework for continuous auditing. Pilots for the technical implementation of a cloud audit system are currently executed. The goal of EU-SEC is to provide continuous certification for cloud providers by using a standardized method of continuous auditing by means of automated test-data collection.

This research investigates recent developments in continuous auditing, focuses on the industry-wide adoption of the EU-SEC framework for continuous auditing and provides suggestions for successful adoption.

2.5 Main research question

What are the drivers and barriers to adoption of a cloud risk framework for continuous assurance in financial services?

2.6 Subquestions

1. What is the state of art concerning risk management frameworks in the cloud?

2. What research has been done into continuous auditing and what are the recent developments?

3. What are the drivers and barriers in the adoption of EU-SEC?

2.7 Methodology

This section elaborates on the methodology used to answer the research questions.

2.7.1 Systematic literature research

A systematic literature research is performed to gather knowledge about risk management and continuous auditing in cloud computing. The systematic literature review methodology proposed by Webster & Watson [64] is used to do a comprehensive literature research, including forward and backward searching. This literature research will answer Q1 (risk management) and Q2 (continuous auditing). The information gathered will serve as a foundation for the semi-structured interviews.

2.7.2 Expert Interviews

Interviews with security and cloud experts were conducted to come up with a relevant research topic and get relevant input for this research. Several risk experts at Ernst & Young Netherlands gave their input, in addition the network of the Cloud Security Alliance was used to get in touch with experts in the field. In these ways relevant input could be collected in the form of opinions, documents and research suggestions. This founded the research design, motivation and relevance of this research.

2.7.3 Semi-Structured Interviews

To research the drivers and barriers to adoption of a continuous auditing and certification framework, semi-structured interviews were conducted at three financial services organizations. Their roles were in the field of cloud procurement, risk management and security expert. The questions for these interviews were set-up from a risk management and governance perspective, literature findings were reflected in the questions. Cloud security assurance and continuous auditing were the other topics in these interviews. Furthermore the essential factors in technology adoption were implicitly investigated by the use of an adoption framework.

2.7.4 Data Analysis using Coding

For the data processing of the interview results, the method called 'coding' is used. In coding the different concepts in interviews are categorized and labeled, to make a comprehensive analysis of the interview answers. The methodology described by Gorden [31] is used. Concepts are linked to the adoption framework and the interview data is compared.

Subquestion	**Used Methodology**
Subquestion 1	Systematic Literature Research
Subquestion 2	Systematic Literature Research, Expert Interviews
Subquestion 3	Semi-Structured Interviews, Data Analysis

Following from the interview results, this research gives suggestions for possible improvements and developments needed to accelerate the adoption of EU-SEC.

Chapter 3

Risks in cloud computing

This chapter elaborates on the results of the systematic literature research and answers the knowledge question:

> *Q1: What is the state of art concerning risk management frameworks in the cloud?*

3.1 Systematic Literature Research

This systematic literature research complements the preliminary literature research by Bannink [2]. The literature index of Google Scholar is used, because it gives an overview of a broad set of databases, which include:

- IEEE
- ACM
- Springer
- Elsevier
- ResearchGate
- Academia.edu
- Several other journals or open access databases

3.1.1 Search terms

In table 3.1 the used search terms and results are given for the answer to Q1.

Keyword	**Results**	**Selected**
"cloud risk management"	140	19
"cloud risk assessment"	147	10
"cloud risk" control	585	18
"cloud risk" framework	524	33
"cloud security framework"	302	23
"cloud security monitoring"	642	32

TABLE 3.1: Search terms and results for Q1

3.1.2 Selection criteria

To come up with a selection of relevant articles for this research, a number of criteria were applied:

1. From the search results and gathered data, articles concerning 'state of art' that are older than 5 years (2013 or before) were omitted. Furthermore, technical papers concerning security measures are deemed irrelevant for this research and omitted as well, since they are out of the scope of this research.

2. Relevant topics were identified from the search results, which are reflected in the section titles below.

3. From the search results, the articles were mapped and combined to fit into the sections.

4. Each section reflects combined knowledge from the selected relevant papers of the previous steps.

3.2 Trust

The lack of trust in cloud computing has been a problem for years. Khan [39] emphasized that challenges do not lay in the technology itself but rather in lack of transparency, a loss of control over information assets and unclear security assurances. Trust is defined as: [39]:

> *"an act of faith; confidence and reliance in something that's expected to behave or deliver as promised. It's a belief in the competence and expertise of others, such that you feel you can reasonably rely on them to care for your valuable assets."*

Loss of control is an important issue in trust, because there is less control over assets. "In cloud computing, this lack of control over the data and processes triggers the risk of losing data confidentiality, integrity, and availability. Cloud computing virtually requires consumers to relinquish control of running their applications and storing their data." [39]

Contractual relationships are issued to establish trust between the cloud provider and cloud customer. In the traditional IT environment the organization is compensated if the service isn't delivered as expected. Cloud providers use service-level agreements (SLAs) to establish trust with their customers. However, this might not be enough in cloud computing since it should be more focused on prevention rather than compensation if a violation occurs. For example a data breach cannot be repaired, no amount of money could repair the damage that has been done. In cloud environments the focus should be on preventing failure instead of post-failure compensation [39].

3.3 Virtualization and Security

Virtualization plays a vital role in cloud computing. Virtualization enables multiple operating systems and applications to be run on a single physical machine. It also allows multiple Virtual Machines (VMs) to share resources of the physical host machine which results in better utilization, optimization and efficiency. The resources are dynamically allocated and when needed provisioned and de-provisioned [4]. Virtualization is the enabling technology for cloud computing but on its turn also accounts for a big risk. The VMs need to be properly isolated to secure systems and data.

Security has a central role in creating trust, cloud providers need to secure their virtual environments [39]. Security risks are perceived as the most important risk in cloud computing [5]. Services for multiple clients can be run on the same infrastructure, which raises risks in the field of virtualization management, identity management, data breaches, access control, VM-protection, the prevention of cross-VM side-channel attacks, compliance, confidentiality, integrity, availability of data, encryption, network security, physical security and inadequate audit/event logging [4, 39].

3.4 Risk identification and classification

The cloud customer needs to assess the business risks of moving to the cloud. In risk management this is seen as outsourcing. The costs, security and business risks can be compared between different providers. The economic terms of costs are important but should be balanced against privacy rights, customer expectations and mandatory legal requirements. Major challenges lay in the realistic representation of this decision in a qualitative and quantitative way, the collection of accurate information from the cloud provider and the identification of contextual requirements and assessment of the privacy impact when moving to the cloud [60]. Conventional risk assessment methods cannot handle the dynamic cloud environment and there is a need of an approach for dynamic (or real-time) risk management for the cloud, accompanied by new modeling languages and tools [60].

This research builds on the risk identification and categorization as done in preliminary research by Bannink [2]. Cloud risks found in literature were identified, categorized and integrated in a risk categories framework that was used to reflect to security management frameworks. For the assessment of risks, best practices can be used, for example ISO or NIST compliant risk method. However, cloud specific threats are not covered by these methods [2, 60].

In preliminary research of Bannink [2] the following risk categories were identified:

1. Data security, identity management and access control [1, 3, 24, 35, 40, 55, 59] ;
2. Regulatory compliance, data location and breaches [1, 3, 24, 35, 40, 55, 59];
3. Multi-tenancy [1, 3, 24, 35, 40, 55, 59];
4. Backup, recovery [1, 3, 24, 35, 40, 55, 59];
5. Investigative support, monitoring cloud environment [1, 3, 24, 59] ;
6. Availability, data integrity, vendor lock-in [1, 3, 24, 40, 55, 59];
7. Sanitization of deleted data [1, 24, 35, 40];
8. Security management and stakeholder involvement [1, 40].

Reflecting on the before mentioned framework there needs to be special attention given to the industry-leading cloud threats identification of the Cloud Security Alliance [59]. CSA regularly publishes a document with the latest 'Cloud Computing Top Threats', the most recent in 2017. The threats are in order of severity based on survey results. Data breaches are considered the biggest threat in this overview [2].

3.5 CSA Cloud Computing Top Threats

1. *Data Breaches*: “A data breach is an incident in which sensitive, protected or confidential information is released, viewed, stolen or used by an individual who is not authorized to do so” [2, 59]

2. *Weak Identity, Credential and Access Management*: data breaches can occur because of a lack of identity, credential and access management. [2, 59]

3. *Insecure APIs*: these APIs are used by customers to interact with cloud services. The security and availability of cloud services is dependent on the security of these APIs. From authentication and access control to encryption and monitoring, the design of these systems must protect against both accidental and malicious attempts to circumvent policy. [2, 59]

4. *System and Application Vulnerabilities*: exploitable bugs can be used to gain access to a system, stealing of data, taking control or disrupting the system. Vulnerabilities put the security of all services and data at risk. [2, 59]

5. *Account Hijacking*: when attackers gain access to credentials of users of the system this poses a severe threat to transaction and data security, integrity and a possible base for new attacks. [2, 59]

6. *Malicious Insiders*: someone who had authorized access to an organization’s network, system or data and attempts to misuse that access which results in a violation of confidentiality, integrity or availability of the information systems. [2, 59]

7. *Advanced Persistent Threats (APTs)*: APTs are a form of cyberattack in which the attacker infiltrates into the computing infrastructure to gather data and intellectual property. Mostly in a stealth way of penetrating into the network with malicious code on a USB stick or hacking into the system (sometimes through other networks). [2, 59]

8. *Data Loss*: all kinds of disasters can lead to data loss, thus proper measures for backup of data need to be in place, following best practices in business continuity and disaster recovery. [2, 59]

9. *Insufficient Due Diligence*: organizations willing to adopt cloud solutions need to take into account all risks that are accompanied with it, including commercial, financial, technical, legal and compliance risks. [2, 59]

10. *Abuse and Nefarious Use of Cloud Services*: this includes misuses of cloud services to launch for example DDoS attacks, send e-mail spam and phishing, mining digital currency, automated click fraud, brute forcing databases or hosting of pirated content. [2, 59]

11. *Denial of Service*: DoS attacks prevent users from accessing their data or applications. The system is overloaded with requests and thus the service slows down or collapses completely. [2, 59]

12. *Shared Technology Issues*: this is the risk accompanied with the multi-tenant feature in cloud, where resources (e.g. CPU, RAM, storage) are shared an need to be properly isolated between clients. This can be a vulnerability, not only for leakage of data but also bugs or security leaks in applications that can be abused. [2, 59]

3.6 Guidelines and regulations

Specific cloud risks need to be addressed and threats need to be taken into account. This call for cloud risk assessment methods has resulted in the cloud-oriented risk assessment method of the European Union Agency for Network and Information Security (ENISA), which addresses various cloud risks based on expert opinions and provides guidance to cloud providers and customers [60]. The ENISA-framework identifies several threats in cloud computing [12]. This 'Cloud Computing Security Risk Assessment' was published in 2009 and has been the foundation of risk guidelines from governments and regulators, such as the Dutch Central Bank (DNB). ENISA provides a list of questions that can be used to assess risks in cloud solutions. The goals of the document are for cloud customers to assess risks, compare offerings, obtain assurance and reduce the assurance burden on cloud providers. "The security checklist covers all aspects of security requirements including legal issues, physical security, policy issues and technical issues." [12]. In Appendix A the comprehensive set of risks identified by ENISA is given.

The Dutch Central Bank (DNB) is the regulator and the supervising body for financial service organizations in the Netherlands. Because the interviewed companies are located in the Netherlands, they are under supervision of the DNB. As such, the Dutch regulations and DNB supervision are within the scope of this research. The DNB supervision is legally binding and based on the financial supervision law 'Wet op het Financieel Toezicht' (WFT) [65]. This law enforces the right of supervision and audit by the DNB. In 2012 DNB stated [63] that an increasing number of financial companies considered to incorporate cloud solutions into their operations. DNB draws attention to the fact that there are risks that need to be considered and they have supervisory rights to the systems that are deployed, because cloud is seen as some form of outsourcing. DNB points out the risks of data location, confidentiality, integrity, availability, auditability, assurance and recovering data after termination of contract [2].

ENISA has also published a document on the secure use of cloud computing in financial services [52]. In that document it is emphasized that the financial service organizations see the benefits of cloud computing but that they remain cautious about the risk of losing control over information assets. Financial organizations mostly migrate test environments and e-mail management to the cloud. They consider private cloud as the best overall fit in the financial market due to privacy and compliance concerns, as it provides more control over data and operations [52]. This document refers directly to the Dutch Central Bank (DNB) as one of the initiators of legislation to allow financial organizations to use cloud based services. DNB has a set of CSPs that they made direct agreements with concerning their right to audit. The DNB guideline requires organizations to [52]:

- Notify their intention to use cloud computing to DNB beforehand;
- Draw up a risk analysis;
- Also meet the requirements laid down in the Financial Supervision Act (Wet op het financieel toezicht – WFT [65]);
- Allow DNB the right to examine the bank.
- Make sure exit clauses are included in the contract

The ENISA-risks [12] can be mapped 1on1 to the DNB risk guidelines [23]. The additions made by the DNB are: Organizational risks (Changing regulations; Insufficient skills and knowledge to identify risks related to Outsourcing / Cloud computing), Compliance risks (Right to audit for supervisors; Where is the data; Specific local data privacy; Risk of conflicting regulations; Exit clause in contract), Other not cloud specific risks (Conflict of interest; Bandwidth limitations). The main addition is the 'right to audit' of DNB which is based on the WFT-law [65]. The other additions are focused on compliance with regulations, abuse and portability of data and the dependence on Internet infrastructures. In general these aspects were already covered by the ENISA framework, the added risks are more specific and emphasize the supervision of DNB. Thus can be concluded that the DNB risk guidelines are fully covered by the ENISA framework.

3.7 Risk management principles

To make the concept of risk management clear, this section elaborates on the principles of governance and risk management.

3.7.1 IT Governance

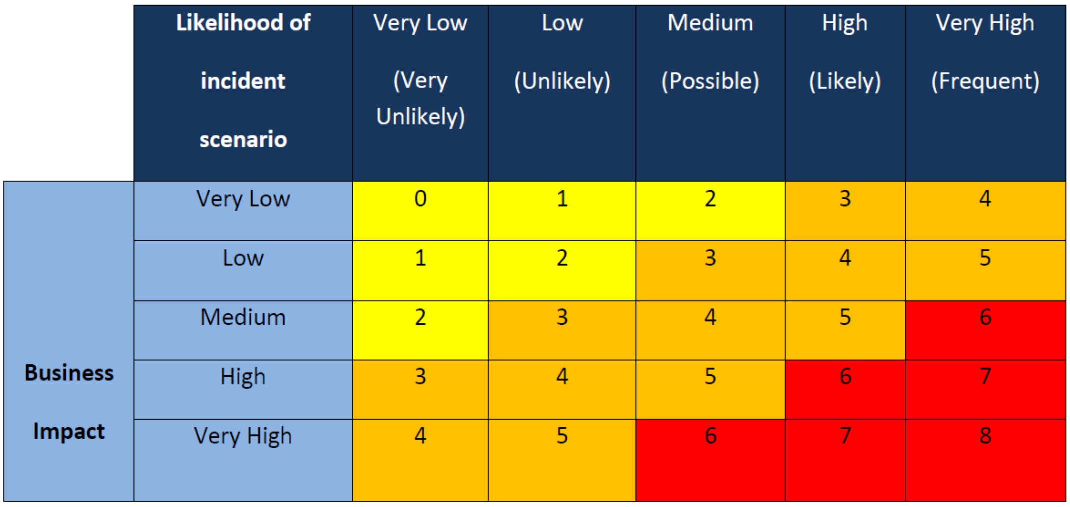
Governance, risk and control are critical in risk management. Governance is enforced through the implementation of policies and procedures. These procedures are based on best practices and should be aligned between business and IT objectives [4]. A typical framework that is used for IT governance is COBIT [37]. Company data is no longer under the control of management when it's in the cloud, uncontrolled or unforeseen risks can lead to information being compromised. Concerning financial service organizations this can lead to withdrawal of their permit by the Central Bank. Risk identification and analysis is important to prioritize the implementation of governance and controls, as well as the scope for reviewing and auditing cloud computing environments. Based on the risk identification and analysis process, controls should be designed and implemented to ensure that the necessary actions are taken to address risks and to achieve business and IT objectives [4]. Risk mitigation is essential when it comes to cloud environments and control, especially in the current environment of cyber threats and usage of cloud computing on a large scale.

3.7.2 Risk management in the cloud

Even though the cloud has many advantages, moving to the cloud is not without risks. A set of controls is required to mitigate the risks and protect data and applications in the cloud. When data and applications are hosted in the cloud, the data is no longer under the control of management and prone to vulnerabilities [4]. The use of Internet technologies or wide area network access to access IT capabilities and data increases vulnerabilities and risks related to continuity and security of information [27].

Outsourcing results in loss of control because of the dependence on another party to fulfill the business needs and to provide adequate controls [27]. Because of the multi-tenant model where various enterprise's data is stored at the same location, there is a risk of data breaches or access by an unauthorized third party. Additionally the transportation of data across networks increases risk of unauthorized access, manipulation or corruption of data. There is also a risk of non-compliance with laws and regulations [27].

The ENISA risk assessment [12] follows the risk management method of ISO/IEC 27005:2008 [36]. Risk classification is done by estimating the likelihood of an incident and the possible impact. The ENISA risk classification has a risk level of 0 to 8. This



	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

FIGURE 3.1: ENISA estimation of risk levels based on ISO/IEC 27005:2008 [12, 36]

can be categorized into 'Low Risk' (0-2), Medium Risk (3-5) and High Risk (6-8). Figure 3.1 shows the risk estimation from ENISA.

The amount of acceptable risks (risk appetite) depends on the type of system that is moved to the cloud. Hence a system with semi-public data has lower risks than a system containing privacy-related information or financial information. In the latter the effectiveness of security controls needs to be taken into account, as well as some form of monitoring the cloud environment and detect breaches or anomalies. Only in this way immediate action can be taken when security incidents happen.

3.8 Responsibility and accountability

With outsourcing of assets, there is a difference between being *responsibility* and *accountability*. "*Accountability* is 'the ultimate responsibility'; it is the state of being 'where the buck stops'. *Responsibility* is an obligation to do something according to certain parameters." [38] When located in-house, the business itself is both responsible and accountable for implementing proper controls and security measures. When outsourced, the responsibility lays at the cloud provider but the client can be held accountable for effective security, possible data breaches and regulatory compliance [38].

As soon as the cloud is used, the cloud provider becomes responsible for the storage of data and security of the infrastructure. Being 'in control' over IT assets is a legal obligation, especially in the financial world which is strictly regulated. There needs to be a certain transparency about security measures being taken and for example the location of data which might be located in other jurisdictions, where law enforcement agencies might have the possibility to access it. Deleted data needs to be properly sanitized and it might be difficult to transfer to another provider (vendor lock-in). The notification of possible data breaches is also an important issue as well as the transferability of data when the provider goes bankrupt, is taken over or merged [45]. The *responsibility* of fulfilling the above demands lays at the cloud provider but the *accountability* for when things go wrong lays at the cloud customer. Policymakers are putting more emphasis on accountability and increased protection when using the cloud [45].

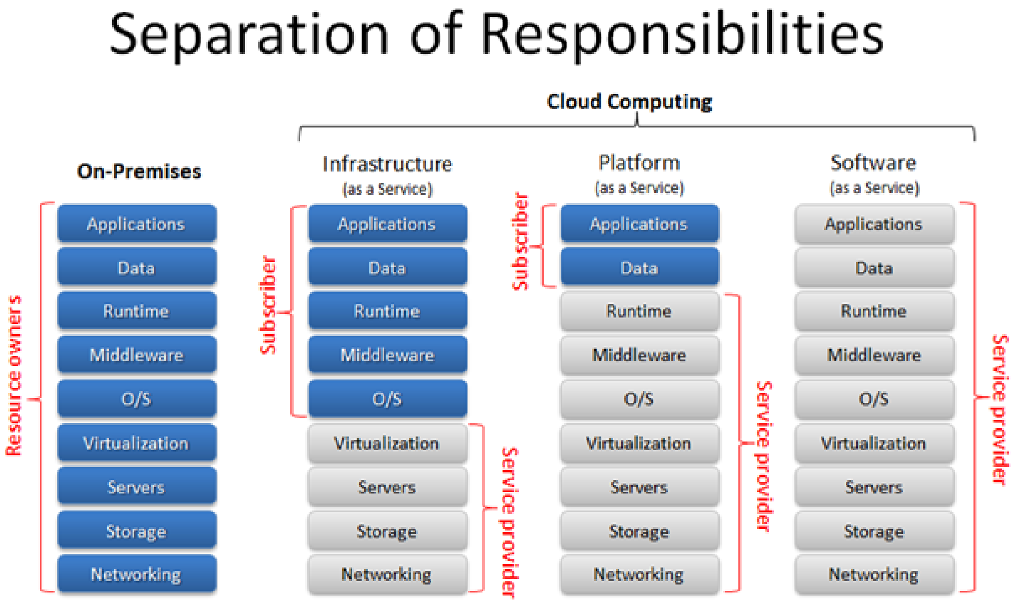


FIGURE 3.2: Separation of Responsibilities
Source: Microsoft TechNet

Contractual agreements between cloud providers and customers are highly important, ensuring a sufficient level of control over IT assets. Service-level agreements (SLAs) are used to define the legal accountability between the cloud providers and their clients and establish trust [38, 39]. Because of this accountability and the increased risk profile, cloud providers have responded by offering certifications like ISAE 3402 or ISO 27001 to prove that their security controls are of a certain quality level [38].

All security controls for the cloud are in general the same as in traditional IT environments, but the cloud customer has to trust the cloud provider that security is properly taken care of. The risk is dependent on the service model used. The lower down the stack of the cloud provider, the more the customer is responsible for [45].

In **all three service models** the cloud provider manages and controls the infrastructure: the servers, network, electricity, human resources and site services. The cloud provider is responsible to implement and operate infrastructure controls e.g. physical security, firewalls, employee training and others. Protecting the infrastructure is of vital importance, because if physical access is possible it doesn't matter how digitally protected the servers are if they can be stolen [38].

In **IaaS** the cloud customer manages and controls all software that runs on the infrastructure, the customer is responsible for all software security controls e.g. patching, anti-virus, application access control, identity management and others [38].

In **PaaS** the customer manages the applications while the provide manages and controls operating system, middleware and the infrastructure. The customer is responsible for all application controls, while the provider is responsible for the IT general controls [38].

In **SaaS** the cloud provider manages all controls on all layers of the software stack and is responsible for their security. The provider is responsible for infrastructure, operating systems, middleware, data and application security [38].

3.9 Security risk control frameworks

Cloud customers can transfer risks to the cloud provider, for example through SLAs. Not all risks can be transferred to the cloud provider and as such the cloud customer can be held legally accountable for security issues. These can have a big impact on the reputation and continuity of the business and can have big financial consequences [45]. Regulatory obligations (for example concerning personal data) cannot be transferred to the provider and remain mandatory for the cloud customer [60]. For financial organizations that do not comply to regulations or are not in control, there is a risk that their bank permit is withdrawn which has a high impact and could put them out of business.

Because of the above mentioned reasons, cloud customers need to get assurance from their providers that security is functioning properly. It may be needed that they are notified of security and privacy incidents and have certain certifications to prove that they are fully in control [45]. Commonly utilized approaches for cloud providers relied on the adoption of security certifications based on standardized 'control frameworks (for example ISO/IEC 27002 and the cloud-specific 27017) to provide their customers a reasonable degree of assurance and transparency [41]. However, to provide cloud assurance and transparency the use of security control frameworks has proven to be rather limited in practice. The cloud provider is not aware of the specific security requirements of the customer, customers can only get a view of the provider's implemented security policies and mechanisms which are problematic for deploying advanced features such as monitoring and end-to-end security assurance [41].

The industry's most widely used and well known control frameworks for information security focus on IT assets that are placed in-house, like the ISO/IEC 27001 and the NIST 800-53 standard that were developed before the appearance of cloud technology. They provide guidelines to set up an *Information Security Management System (ISMS)* which manages information security risks. The mapping of these standards in related literature [2] showed that they mostly fell short in the field of Infrastructure & Virtualization Security, Identity & Access Management, Datacenter Security, Encryption and Data Flows. In order to cope with changing environments, there were additions made to these frameworks specific for cloud.

The Cloud Security Alliance tried to address these shortcomings in their framework, which combines insights from several standards into one framework of controls relevant to risk management in the cloud. They provide the *Cloud Control Matrix (CCM)* which specifies criteria for cloud risk management. This is used as guideline for their CSA STAR certification (`https://cloudsecurityalliance.org/star/certification/`), which is designed to comply with ISO/IEC 27001. This third party independent assessment of the cloud provider is used to audit the capability levels of the cloud service provider. This provides (prospective) cloud customers an understanding of the levels of security controls of their provider.

The limitation of the above mentioned standards is that they describe what to do to be compliant, but not how to do it [2]. The standards are sometimes perceived as checklists, instead of testing the true effectiveness of the ISMS. Testing controls in cloud audits says something about the presence of a control and looks back in time. This ensures that risks are properly managed in the past but doesn't guarantee that for example VM or network based attacks are detected promptly, logs are analyzed and/or monitoring is in place. Only with these measures the security of the most sensitive information assets can be ensured.

There have been initiatives by ENISA, ISO/IEC, NIST and the European Commission to improve SLAs by adding security parameters. These parameters allow cloud providers to describe implemented security controls, associated metrics and committed CSP values for those metrics [41]. This creates more transparency about security levels offered, while at the same time providing information to monitor the fulfillment of the customer's security expectations [41]. The importance for improving SLA management and cloud monitoring as the basis for improving governance, risk and compliance has also been emphasized in other literature [6, 8, 43, 47–49]. The real-time risk management can bridge the gap between operational and management levels of cloud computing. The dynamic risk management combined with SLA and exception management will contribute to continuous risk management [43].

The cloud customer may want to monitor if SLA objectives are met, but the complex nature of cloud infrastructures makes it difficult to do that. Cloud providers need to implement internal compliance monitoring controls, in addition to an external audit process. However, the provision of a full audit trial within the cloud, particularly in public cloud models, is still an unsolved issue [45].

To be able to use cloud systems securely, cloud providers and customers need to share the responsibility of implementing and monitoring security requirements. Cloud customers can identify cloud-specific risk-adjusted security controls, and the provider needs to monitor all identified security controls. Service Level Objectives (SLOs) can be defined and should be monitored [6, 41]. CSA is composing a catalog of cloud security metrics to support his. The Cloud Trust Protocol of CSA is one of the most recent developments of the monitoring of security metrics in the cloud [41].

There is no efficient mechanism for gathering evidence from log data in multi-tenancy environments, the ISO 2700x and NIST standards are operated at a macro-level and usually do not leverage information coming from logging and auditing activities carried out by IT operations [45]. Auditing frameworks cannot bridge nor automate the gap between low-level monitoring and logging and high level requirements. At cloud providers there exist a number of tools, but they are in limited scope. Audit remains a big open issue in cloud computing [45]. Due to the static nature of conventional audits they only provide security in retrospect, instead of giving 24/7 control and monitoring [2].

Continuous auditing of cloud environments can be a viable solution to the above described challenges. Controls can be automatically tested and monitoring of the infrastructure and logs can provide real-time insight in incidents. This puts a high demand on the willingness for cloud providers to provide this information, which can be contractually agreed on. In the end there should be a best practice standard for these audits, providing insight in the parts that are not fully covered by the existing security management standards. Only in that way cloud can be a viable solution for financial services organizations.

Chapter 4

Continuous Auditing

This chapter will review the state of art in literature and concepts of continuous auditing, together with the most recent developments in the field. The knowledge question:

> *Q2: What research has been done into continuous auditing and what are the recent developments?*

4.1 Systematic Literature Research

This literature research builds on the literature research and sources of Chapter 3. The same method and selection criteria are used. Furthermore, the references in the documentation of the EU-SEC project are used as input for this systematic search by means of backward searching.

4.1.1 Search terms

In table 4.1 the used search terms and results are given for the answer to Q2.

Keyword	**Results**	**Selected**
"cloud audit"	519	15
"cloud audit" automation	257	5
cloud "continuous audit" 2014-2018	175	10

TABLE 4.1: Search terms and results for Q2

4.2 Continuous auditing

Continuous auditing is a phenomena that was initiated by the financial accounting industry. By ways of automating audits they cloud detect anomalies and fraud with data analytics. The American Accounting Association has acknowledged that continuous auditing is of high importance. They say continuous auditing can "identify and investigate exceptions on a regular basis shortly after a transaction has occurred" [54]. AAC acknowledges the need for a continuous auditing framework "that will detect errors and fraudulent transactions as they occur, identify business improvements, and provide assurance over key preventive controls" [54]. For example the use of software agents for continuous auditing [51] and forensic cloud log processing [61] have been proposed.

Continuous auditing will eventually replace conventional audits, business processes will be continuously audited [7]. Standardization of data collection and formalization of control policies are essential in this context, the auditor's role may shift to becoming an independent certifier of the internal audit's control system [7]. This can however not fully solve the problem, since there needs to be a wider range of disciplines combined to come up with a complete solution of the problem [26].

4.3 Continuous cloud auditing and monitoring

The continuous auditing paradigm was originally developed within the financial accounting industry. However, continuous auditing can also be applied to verifying security controls and monitoring cloud environments. This concept has been proposed to fill the gap in the information needs of the cloud customer concerning compliance, security and risk management of the cloud provider. There is a number of organization that work on cloud security standards, such as CSA, NIST, ISACA but also some more specific industry standards. Duncan et al. [25] summarized a non-exhaustive list of more than 30 different standards in 2016. Duncan et al. [25] provide an overview of the cloud audit literature, which elaborates on data collection, integrity and possible security problems when collecting data vor a Third Party Audit (TPA). Furthermore the existence of frameworks for data processing and prototypes of cloud security audit systems are indicated. The existence of SLA's is not enough to measure risks in cloud environments and mainly focus on quality of service [26]. Anomaly detection mechanisms and virtual machine monitoring are essential parts of cloud security monitoring. The continuous monitoring system should be protected as well, a (virtual) machine shutdown should not result in the shutdown of the data collection system. The monitoring already existent at the cloud provider (CSP) can serve as an input for continuous monitoring systems.

4.3.1 SLA and SLO

Pearson et al. [46] indicate that "SLAs should facilitate cloud customers in understanding what is being claimed for the cloud service and in relating such claims to their own requirements." The SLA is an agreement between the CSP and the cloud customer that agree on services provided and Service Level Objectives (SLOs). If a SLO is not met there can be financial compensation, but when the SLOs cannot be measured it cannot be confirmed if the SLA is met. This is in particular important for security SLAs but defining useful (and quantifiable) security and privacy SLOs is a difficult task [46].

A SLO is typically composed of metrics who set the margins and boundaries of errors CSPs have to comply to. The factors that these metrics should consist of are proposed by ISO/IEC, CSA and CICA and within workgroups of the European Commission (EC) or cloud industry [46]. SLO metrics can be mapped to standards and be used as input for continuous certification / continuous audits.

The general message delivered by Pearson et al. [46] is that empirical validation of SLA security and privacy elements should be done. Research should be done by cloud stakeholders to guarantee the creation of standards and best practices, for example a Cloud-Adapted Risk Management Framework. In the next section the developments in this sense will be elaborated on.

4.4 Developments in continuous auditing

To get an overview of the developments in the field of cloud auditing, monitoring and continuous audits, the Cloud Security Alliance (Netherlands chapter) was contacted for consultation. CSA board members and associated security experts were consulted. This provided an insight in the current developments in the industry and provided additional input for the literature research.

4.4.1 CloudAudit

The CloudAudit initiative from CSA [14] was launched to fulfill the need for streamlining cloud audits. Providers can automate their audits, assessments and assurance procedures for their cloud environments and allow authorized cloud customers to do this via an open interface and methodology. By doing this, they provided means to initiate automated audits. The goal of CloudAudit is to enable the CSP to automate repetitive tests that were typically labor-intensive and costly, thus providing assurance and compliance validation via standardized interfaces. Advantages from the cloud customer are the consistent and standardized interface to gather information from the service provider. The focus is on a consistent representation of used tools that can be utilized by cloud customer, a standard schema and data structure for APIs to collect the data, mapped to existing compliance, security and assurance frameworks. This resulted in the Cloud Trust Protocol.

4.4.2 Cloud Trust Protocol

The Cloud Trust Protocol (CTP) [15] ensures that cloud customers can receive information about the fulfillment of duties by their cloud provider. This is aimed to ensure trust between provider and customer. With the CTP, cloud customers receive information about compliance, security, privacy, integrity and operational security history from their services in the cloud.

CloudAudit has built the foundations of a standardization of data collection and a meta-framework for the output of test data. The CloudAudit and CTP served as input for the cloud certification and continuous auditing initiative EU-SEC. CloudAudit and CTP were merged into this project and thus CSA terminated these working groups. The EU-SEC set-up and basics are elaborated on in the next section.

4.5 EU-SEC Continuous Certification Framework

This chapter describes the European Security Certification Framework (EU-SEC) that is funded by the EU. In science there are a number of methods proposed for continuous auditing, but none of them have been able to incorporate EU-wide audit and security requirements, standards, legislation, provided a pilot proof-of-concept nor have been able to combine forces in a mixed consortium of industry partners, auditors and research institutions. This makes EU-SEC the most viable EU-wide framework, which aims to become a standardized approach to cloud audits and certification.

4.5.1 Goal of the EU-SEC project

The EU-SEC project is funded by ’Horizon 2020’, the biggest EU Research and Innovation program. The project aims to improve trust, assurance and compliance in the cloud market. Cloud customers need a high level of trust and transparency, especially in the financial sector. There is a high level of standardization, yet different standards and certifications cause confusion. The aim of the EU-SEC project is to "improve the effectiveness and efficiency of existing certifications by creating a framework for Mutual recognition between different certification schemes. Requirements and controls from the public sector and the banking sector will be incorporated into the framework [29]". EU-SEC will develop a certification framework that complements existing certification and assurance schemes. The newly developed architecture provides a set of tools to improve the efficiency and effectiveness of current assurance schemes. This will be tested and validated in pilots involving industry partners [19].

The EU-SEC project addresses issues concerning security and privacy governance, risk management and compliance in the cloud. Furthermore, the project takes into account the new privacy regulations from GDPR (General Data Protection Regulation). EU-SEC aims to bridge the requirement gaps in current certifications and minimize the lack of transparency toward cloud service customers. The Multi Party Recognition framework for cloud security certifications is based on mutual recognition criteria identified between certification schemes and technical requirements are collected in a repository and mapped onto each other [29].

EU-SEC provides foundations for a continuous auditing-based certification framework, built on definitions, existing literature on continuous monitoring, security parameters and service levels. The literature references concerning continuous auditing were included in this research. Ideally the continuous auditing should be fully automated, but EU-SEC acknowledges that in practice that's not possible today, given the state of art in certification [21]. Requirements from this project took into account automated and non-automated continuous audits, this will serve as the enablers for continuous certification. EU-SEC tries to be the pioneer in continuous auditing, by creating a continuous auditing based certification framework. The requirements for mutual recognition can be apply to continuous certification in the future, when more continuous certification schemes will emerge.

Cloud computing created uncertainties regarding compliance and trust, yet this problem is often successfully solved by using certification or attestation, based on industry-wide standardized compliance frameworks [21]. The success of certification or attestation resulted in many compliance schemes on the market. CSPs rely on general information assurance schemes like ISO 27001 or audit firms who apply ISAE 3000 to provide a SOC 2 attestation report [21]. The Cloud Security Alliance created one of the first global cloud-centric certification and attestation through the STAR program mentioned in Section 4.5.2. Regional authorities or industry players introduced their own compliance standards, to address national or sector-specific needs. This resulted in a high number of certification schemes in the market, which is a key barrier to smaller players in the market [21].

Some industry sectors have special requirements concerning assurance, such as the banking or healthcare sector. Current available certification and attestation schemes don't provide the continuous oversight they need for their cloud solutions. Typically a certification or attestations follows a yearly cycle, but in these sectors that's not enough because they demand a realtime view of compliance in order to react actively when non-compliance or a cyber threat is detected [21]. Since this research is conducted within a financial services auditor and financial sector organizations, continuous certification is a highly relevant and upcoming phenomena that needs to get attention.

The EU-SEC project addresses these shortcomings by building a certification framework which 1) addresses all requirements relevant in the EU-market today, 2) provides a generally applicable auditing requirements scheme, 3) provides a continuous auditing certification framework and 4) offers multi-party recognition in which certification can be used effectively together with existing certification schemes.

4.5.2 CSA STAR

In order to improve transparency, CSPs have published self-assessment results in public registries like the CSA STAR Registry [18]. STAR is a program for security assurance in the cloud, which improves transparency, rigorous auditing and harmonization of standards. Indication of best practices and validation of the security level of cloud offerings are its most important benefits [18]. STAR has three levels of assurance: self-assessment, third party certification and continuous auditing. The EU-SEC project can be seen as an approach to a level 3 certification, see Figure 4.1.

CSA STAR is based upon [18]:

- The CSA Cloud Controls Matrix (CCM) [13]
- The Consensus Assessments Initiative Questionnaire (CAIQ) [16]
- The CSA Code of Conduct for GDPR Compliance [17]

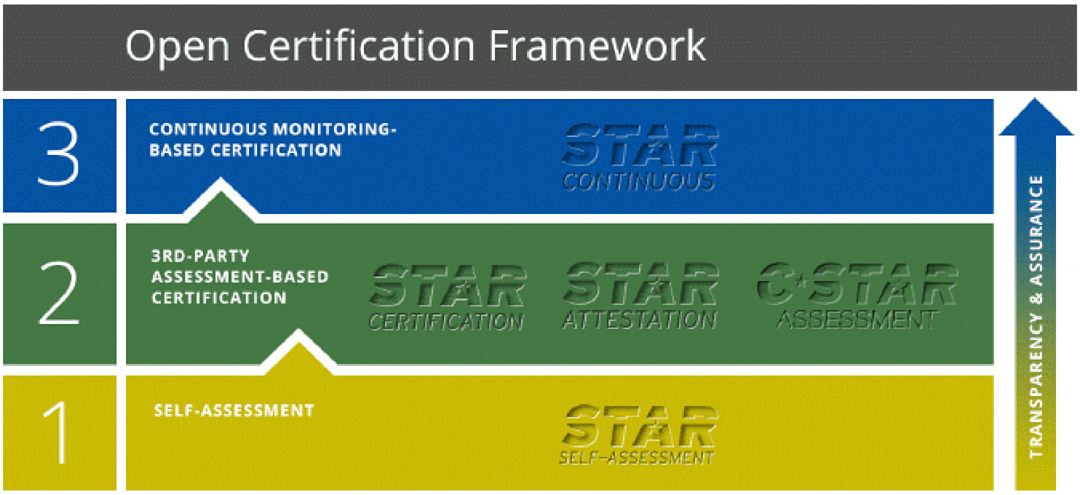


Figure 4.1: CSA STAR [18]

4.5.3 Collection of requirements and controls

Governments of EU countries currently develop and maintain their own standards, guidelines, requirements, controls and conditions for certification or compliance. Sometimes compliance efforts are duplicated. EU-SEC develops a framework that enables and ensures interoperability and compatibility between existing certification schemes and requirements. EU-SEC collected security and privacy requirements and controls, analyzed them and integrated them into a common repository of controls. The scope was set to the international and national standards related to cloud computing, technical specifications and guidelines/documents important for the banking sector. The common repository that was used is the Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) [13]. The mapping of controls lead to the identification of gaps: no, partial or full gap. Partial or full gaps served as a basis for updating the existing CCM controls or to define new controls. This process also indicated the need to ensure that the requirements can be continuously captured and captured in a transparent way. This contributed to an enhanced mapping of laws, regulations and industry requirements to standard cloud controls [29]. These requirements and controls have been published by EU-SEC in deliverable 1.2 [19].

The EU-SEC requirements span the control mechanisms of different standards. For example the requirement OIS-02 in EU-SEC states: "A security policy with security objectives and strategic parameters for achieving these objectives is documented. [19]" This requirement is derived from the CCM control GRM-05 and GRM-06 [13] and ensures the presence and enactment of a security policy, which is based on corporate objectives, business processes, laws and regulations. This requirement is difficult to be measured automatically because it needs human judgment to value if this requirement has been met. An interesting requirement is the requirement RB-20 [19] which states that "the cloud customer is informed by the cloud provider of the status of the incidents affecting them in a regular and an appropriate form that corresponds to the contractual agreements or is involved into corresponding remedial actions." This requirement solves the perceived information gap that was indicated by conventional point-in-time certifications. Some requirements can be quantified and measured, such as CBK-02-06 [19]: Develop and maintain secure systems and applications. This requirement states that appropriate patching and security practices need to be executed concerning systems applications. The timely patching of applications can be a process that is automatically checked and reported on. There are a number of requirements that rely on the appropriate monitoring being implemented by the CSP, which can provide an input for continuous auditing.
The EU-SEC requirements repository was built on a mapping of 23 input documents onto the Cloud Control Matrix. The CCM was already aligned with industry-wide standards, regulations and control frameworks like ISO 27001/27002, ISACA COBIT, PCI DSS, NIST, AICPA TSC and others [19]. The additional input documents were selected if those standards were not mapped to the CCM yet. Additions include [19]:

Standards

- Cloud Computing Compliance Control Catalogue (C5)
- ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 27017: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018: Information technology - Security techniques - Code of practice for PII protection in public clouds acting as PII processors
- SecNumCloud

Technical specifications and good practices

- AICPA Trust Services Principles and Criteria
- ENISA – Minimum Security Measures for DSPs

Banking sector legislation and documents

- Rules published by the European Banking Authority (EBA).
- Guidelines specific to the processing of financial data (PCI).
- ENISA guidelines specific to the financial sector.

The next sections will elaborate on the ENISA and EBA requirements as they are specifically relevant for financial services organizations.

4.5.4 ENISA requirements

The European Union Agency for Network and Information Security (ENISA) leverages knowledge about cyber security within the EU, by working together with member states and the private sector. ENISA has written many publications concerning cloud computing security, for example [19]:

1. The cloud security risk assessment, published in 2009, that is widely referred to across the EU [12].
2. The follow-up of the risk assessment is the assurance framework for information security risks in cloud services, used as the basis for cloud assurance initiatives [11].
3. Security and resilience in government clouds, published in 2011 [53].
4. Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, published in 2017 [57].

Based on advice from the ENISA member of the Advisory Board, the EU-SEC project decided to include minimum security measures for DSPs [57] as input document, instead of the risk assessment [19]. ENISA provided this report in order to have a common approach for DSPs regarding security measures. The report is based on the Cloud Certification Schemes Meta framework (CCSM) that was released in 2014 by ENISA [10]. Additional security objectives for cloud computing that emerged since 2014 have been added to this report, as well as the latest information on security controls and measures implemented, together with good practices and standards deployed by DSPs [19]. The report also provides mapping between security objectives and the following security standards, certification schemes and national frameworks [19]:

- ISO/IEC 27001:2013
- CSA CCM: Cloud Controls Matrix v3.0.1
- BSI C5: Cloud Computing Compliance Controls Catalogue (C5), criteria to assess the information security of cloud services, version 1.0 – as of February 2016
- COBIT5: Framework for the governance and management of enterprise IT
- CCS CSC: The CIS Critical Security Controls for Effective Cyber Defence, Version 6.1, August 31, 2016
- OCF: CSA STAR Program & open certification framework in 2016 and beyond
- NIST: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014
- PCI DSS: Payment Card Industry (PCI) Security Standards Council, Data Security Standard Requirements and Security Assessment Procedures, Version 3.2, April 2016
- CES: Cyber Essentials Scheme, Requirements for basic technical protection from cyber-attacks, June 2014.

The report 'Technical Guidelines for the implementation of minimum security measures for Digital Service Providers' [57] defines 27 security objectives providing: 1) description of the objective 2) examples on the implementation of these security measures and 3) mapping based on the industry standards above. Since the ENISA guidelines are taken into account while developing EU-SEC, it can be concluded that they are in line with the assessment of the Dutch Central Bank as well.

ENISA published specific requirements for the financial sector in their document 'Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations' [52]. This document is set-up in cooperation with banks, experts and supervising authorities. It emphasizes the importance of risk management, SLA negotiations, transparency, understanding, guidance and certification schemes when using cloud computing in financial services. This report gives information, guidance and compliance suggestions which can be used by regulators and financial institutions. ENISA reports that financial services organizations are hesitant to use cloud computing because of the lack of transparency, thus they encourage CSPs to improve transparency and for their customers to understand the security implications of cloud offerings.
The most relevant recommendations from ENISA concerning this research are: extending cloud governance and risk management standards, defining practices and standards for incident information sharing, CSPs to provide transparency and assurance, minimum security measures for cloud in FSO.

4.5.5 EBA Requirements

The European Banking Authority has been appointed by EU law to issue guidelines and recommendations to competent authorities, with the goal of establishing consistent, efficient and effective supervisory practices and the uniform and consistent application of EU law. Authorities and financial institutions are obliged to make efforts to comply with the EBA guidelines. Authorities should incorporate the guidelines in their supervisory practices.

The three documents of the EBA mentioned in [19] are:

- Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) [32]
- Final Guidelines on the security of internet payments [34]
- Recommendations on outsourcing to cloud service providers [50]

The SREP 'Guidelines on ICT Risk Assessment' [32] are aimed at internal ICT strategy, risk identification and governance. The 'Final Guidelines on the security of internet payments' [34] are aimed at providing requirements on the security controls concerning transaction processing. These are internally focused and thus out of the scope of this research. The 'Recommendations on outsourcing to cloud service providers' [50] are recommendations for cloud outsourcing and are thus relevant for this research. Below the key takeaways of this document are mentioned.

General outsourcing guidelines have been published in 2016 in the Committee of European Banking Supervisors guidelines on outsourcing (CEBS guidelines). These new guidelines are specifically aimed at cloud outsourcing. This document is aimed at the process that institutions should follow for informing their supervising authority about cloud outsourcing. The 'right to audit' is the most important driver which should be contractually agreed on.

The EBA document provides guidelines on the security of the data and systems used in the cloud, including the data treatment and processing. A risk based method is proposed to implement adequate controls and measures, for example the use of encryption. Requirements for the adequate mitigation of risks in 'chain' outsourcing under subcontracts are given. The requirements for cloud outsourcing can be divided in these topics:

1. **Materiality assessment** where the risk profile and (potential) impact on operations and confidentiality of data;
2. **Informing supervisors** about outsourcing activities;
3. **Access and audit rights** for the institution and the supervising authorities;
4. **Security of data and systems** to protect the confidentiality of data stored and transmitted in the cloud;
5. **Location of data and processing** to assess risks of data locations;
6. **Chain outsourcing** where risks of subcontracting should be taken into account;
7. **Contingency plans and exit strategies** to ensure that in the event of a termination of the contract, the services can be transferred to another outsourcing provider.

One of the most recent publications that is not yet included in EU-SEC is 'Guidelines on the security measures for operational and security risks of payment services' which was published in January 2018 [33]. These guidelines give attention to governance, risk management and control. In particular the guidelines on outsourcing and monitoring are relevant in the cloud computing context. Payment Service Providers (PSPs) should ensure that "appropriate and proportionate security objectives, measures and performance targets are built into contracts and service-level agreements with the providers to whom they have outsourced such functions. PSPs should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets." This emphasizes the importance of monitoring. Guideline 3 (Risk assessment) and 5 (Detection) [33] emphasize the importance of continuous monitoring in financial service organizations. Physical or logical intrusion detection, as well as data breaches, integrity and availability are mentioned as part of continuous monitoring.

4.5.6 Auditing and assessment requirements

EU-SEC has studied the differences in audit and assessment engagements, and applied audit criteria. To audit the IT operations, a CSP may assign an independent audit and assessment firm to certify or attest on its Information Security Management System or controls. Certification ant attestation processes are governed with well-defined standards such as ISO 27000 and ISAE 3000. A CSP may want to have multiple certifications may benefit from the multi-party audit and assessment engagement of EU-SEC, possibly lowering the cost of compliance for the CSP. EU-SEC recommends building the control environment in compliance with CCMv3 and structured according to ISO/IEC 27001 topics, which allows for ISO 27001 certification. According to EU-SEC this is in good alignment with the requirements of for example ISAE 3000 and does not limit the provider from seeking attestation on controls according to SOC 2 or national requirements [29]. These auditing requirements have been published in deliverable 1.3 of the EU-SEC project [20].

4.5.7 Multi-party recognition

The EU-SEC project emphasizes the importance of multi-party recognition. This means that certifications are inter-exchangeable with each other, the EU-SEC requirements should fit with each certification scheme. For this purpose they created a multi-party recognition framework for third party audit-based certification. The goal of this framework is to identify the key components of a third-party-audit-based certification, compare them and build a generic framework. Principles from different certifications were combined to ensure a good level of quality, robustness and thoroughness. The multi-party recognition is aimed to serve the European market. The EU-SEC governance framework ensures long-term sustainability and exploitability of the framework after the finalization of the project. The requirements for the multi-party recognition are set-up in Deliverable 1.4 of the EU-SEC project [21].

4.5.8 Continuous Auditing Certification Scheme

EU-SEC has published their certification scheme which describes the principles, architectures and enabling methods. This supports the overall aim of the project of delivering a more efficient compliance assessment and new way of compliance reporting by use of a standard certification scheme [22].

The goal of continuous auditing is to provide an always up-to-date compliance status by increasing the frequency of the auditing process, in this case the verification of controls. The limitations of point-in-time audits are overcome in this way. The verifications can be classified into automatable, non-automatable, the automation itself and reasonable frequencies of measurements [22]. The methodology that is used in [22] consists of: limitations in conventional auditing, defining concepts, modeling of interactions, identification of possible shortcomings and evaluation of a novel approach. The different phases in the EU-SEC continuous auditing process are shown in Figure 4.2.

4.5.9 Point-in-time certification vs. continuous auditing certification

The conventional point-in-time certification is well established, for example ISO 27001 validates if an organization meets a standard set of requirements. Compliance is proven by defining a set of controls and control objectives, which can be effective or not. In some certifications like CSA STAR the maturity of a control is also rated [22].

EU-SEC defines continuous audit as: "the continuous process though which an information system is assessed to verify that a predefined set of objectives, (e.g. SQO and SLO) are met." [22].

Control objectives are translated into a set of controls, which are more concrete. The controls still contain some abstraction, dependencies on the context and some elements that need human assessment. Compliance is a qualitative objective that needs to be assessed by a human sometimes. For continuous auditing certification, evidence must be collected continuously and with a pre-defined frequency that can vary from seconds, hours to days [22]. The frequency of checking each control can be defined according to a particular need, based on the specific assurance needs of the cloud customer.

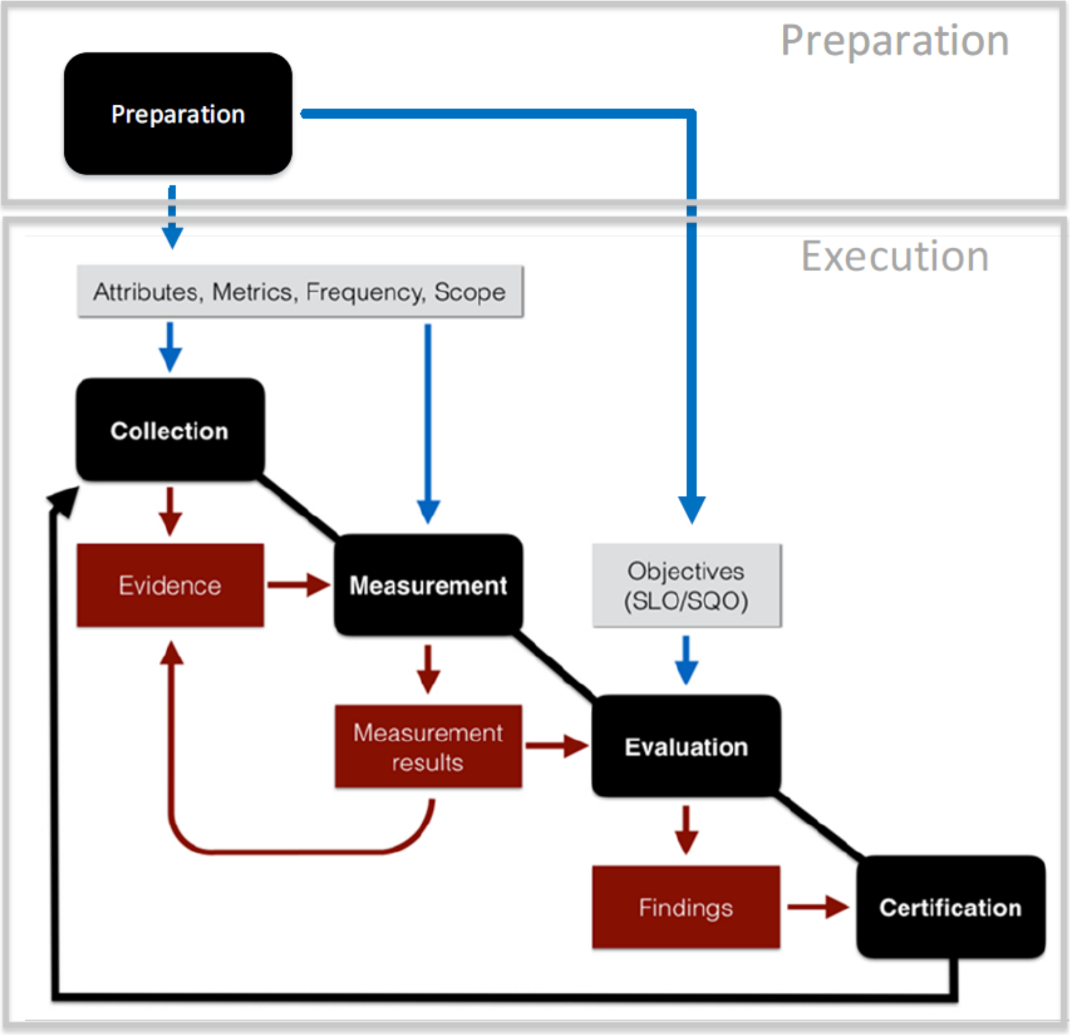


FIGURE 4.2: Model of continuous auditing phases [22]

Continuous auditing establishes the process in which an information system is continuously assessed to verify that a predefined set of objectives is met. Continuous audit-based certification is the "regular production of statements indicating that an information system meets a set a predefined of SLOs (Service Level Objective) and SQOs (Service Qualitative Objective) [22]".

The continuous certification process consists of the following steps [22]:

1. Information is collected from the information system.
2. A measurement is applied to that information, according to a metric, and produces a measurement result.
3. The measurement result is then compared to an SLO (Service Level Objective) or SQO (Service Qualitative Objective) to decide whether or not the objective has been attained.

For illustrative purposes, a visualization of the above described continuous auditing process is provided in Figure 4.3.

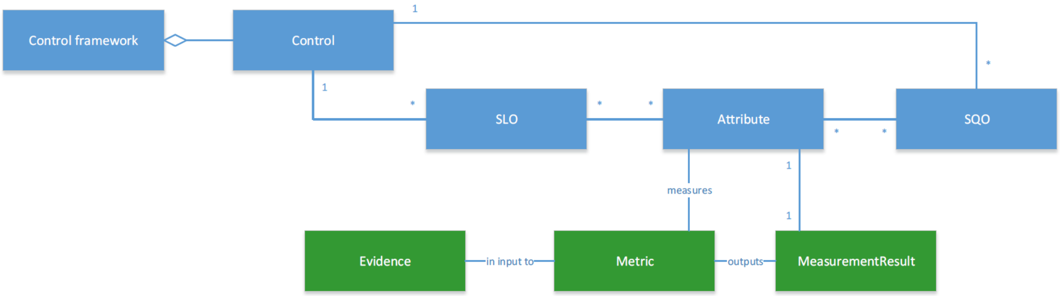


Figure 4.3: Conceptual UML model for continuous auditing [22]

Chapter 5

Adoption of EU-SEC

This chapter will explain the TOE-framework for adoption of new technologies, this framework can investigate the forces that are present in the adoption of the EU-SEC continuous certification framework. The results of the semi-structured interviews that are executed in three financial services organizations will be discussed according to the TOE-framework.

This chapter will answer the following question:

> *Q3: What are the drivers and barriers in the adoption of EU-SEC?*

5.1 Adoption framework

Continuous auditing is a new innovation and certain factors affect the adoption of innovations and standards. Oliveira [44] did an extensive analysis of the empirical studies that use the TOE-model, concluding that the Technology-Organization-Environment model of Tornatzky and Fleischer [62] is the most well suited for inter-firm innovation adoption. The TOE-framework has a solid theoretical basis, strong empirical support and has been applied to study adoption of technological innovations [44]. Very recent related work of Teigeler et al. [58] applies this framework as well in their empirical research in which cloud providers were interviewed concerning continuous certification.

The TOE framework was developed in 1990 by Tornatzky and Fleischer [62]. It identifies aspects that influence the adoption of a new innovation in enterprises: technological context, organizational context and environmental context. Figure 5.1 gives an overview of the framework and factors.

1. *Technological context* describes both the internal and external technologies relevant to the firm. This includes current practices and equipment internal to the firm, as well as the set of available technologies external to the firm [44].

2. *Organizational context* refers to descriptive measures about the organization such as scope, size, and managerial structure [44].

3. *Environmental context* is the arena in which a firm conducts its business — its industry, competitors, and dealings with the government [44].

The TOE framework is an analytical framework that can be used for researching the adoption and assimilation of different types of IT innovation. However, the specific factors identified within the three context may vary across different studies [44]. Since it has a strong theoretical basis, empirical support and the potential to be applied to IS domains, this framework is used to research the adoption of EU-SEC within the industry.

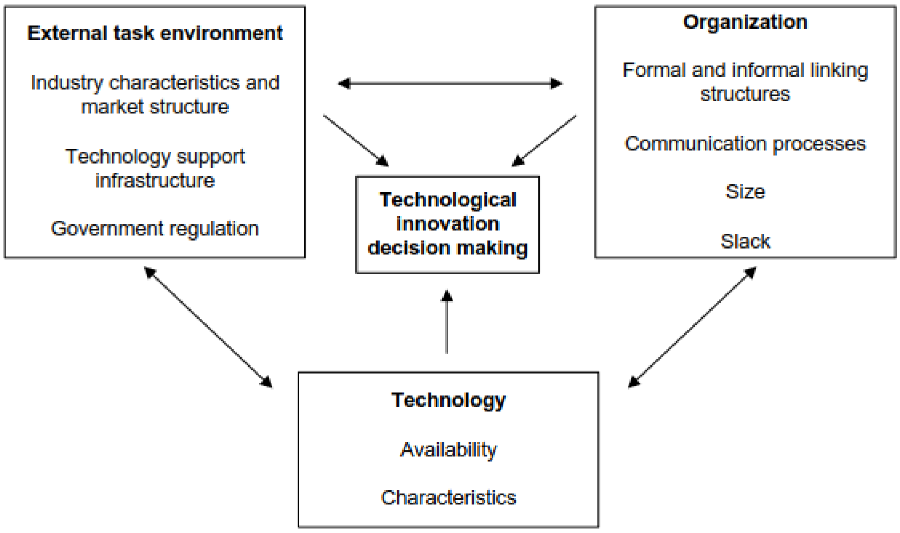

External task environment
Industry characteristics and market structure
Technology support infrastructure
Government regulation
Organization
Formal and informal linking structures
Communication processes
Size
Slack
Technological innovation decision making
Technology
Availability
Characteristics

Figure 5.1: Technology, organization, and environment framework (Tornatzky and Fleischer 1990) [44]

5.2 Interview set-up

Semi-structured interviews were conducted at three financial services companies, all located in The Netherlands and under supervision of DNB. The interviews were based on the set of questions in Appendix B and were not necessarily asked in that order. Additionally, three security/auditing experts were interviewed. The questions for the certification body / auditor can be seen in Appendix C. The questions for the consulted experts were a mix of both types of interviews.

The processing of interviews was done as follows:

- Coding to identify the different topics;
- Mapping the interview results to these topics;
- Identifying similarities and differences between interview results;
- Mapping the relevant adoption drivers and barriers to the TOE-framework, making a distinction between drivers and barriers.

The similarities and differences between the companies were included in text, but not included in the results table. This is done because they are important for providing context but do not contain adoption drivers and barriers for EU-SEC. The adoption drivers and barriers, divided into topics and mapped onto the TOE-framework, can be found in Appendix D. The letter indicates the TOE-category and + (driver) and - (barrier) indicate the influence on EU-SEC adoption.

5.2.1 Comparison of researched companies

Two financial services companies participated in this empirical research, furthermore two security experts from respectively an auditing firm and a big Dutch bank were interviewed. Additionally the opinion of EY CertifyPoint (certification body) about continuous auditing and EU-SEC was used as input.

The characteristics of the participating companies can be seen in Table 5.1.

	Company 1	**Company 2**
Services	Real-estate investment	Health Insurance
Employees	700	1800
Service model(s) applied	SaaS	PaaS / SaaS
Main deployment model	Public cloud	Private cloud

TABLE 5.1: Company information – Interviews

5.3 Interview topics

From the interview transcriptions, main topics were identified by the use of the coding technique. This resulted in the following set of topics:

- Governance / Risk Management / Compliance
- Standards / Regulatory
- Cloudprovider
- EU-SEC

Below the references and interview details are given:

Ref.	**Person**	**Role**	**Date**	**Length**
e1	Expert 1	Auditor / Security Expert	23-5-2018	1:25 h
e2	Expert 2	Bank Security Expert	27-6-2018	1:32 h
c1p1	Company 1, Person 1	Risk manager	24-5-2018	1:03 h
c1p2	Company 1, Person 2	Global IT Servicemanager	05-6-2018	1:16 h
c2p1	Company 2, Person 1	Procurement Manager	19-6-2018	0:36 h
c2p2	Company 2, Person 2	Security Advisor	19-6-2018	1:18 h
ey	EY CertifyPoint	Certification body	20-6-2018	1:03 h

TABLE 5.2: References – Interviews

Despite the fact that the interviewed companies and experts differ from each other in context, there were no contradictions found in the interview responses concerning adoption. As such, the interview responses give a reliable overview and consensus concerning the adoption factors for EU-SEC.

5.3.1 Governance / Risk Management / Compliance

'Minimal security' is the goal at Company 1 **(c1p1)**, in which they are aiming to comply to global requirements of their company and regulations they have to comply to. In recent developments more emphasis is placed in the maturity of operational risk management, as a response to security incidents. They also face regular due diligence checks by their customers **(c1p2)**.

Company 1 noted that contractual agreements were mainly focused on compliance with for example GDPR, only with a GDPR non-compliance they would get an instant notification **(c1p1, c1p2)**. Contractual agreements made the CSP legally accountable. However, as the cloud expert **(e1)** pointed out, the contractual agreements should focus on getting more real-time compliance insights on the CSP infrastructure and their applications.

Being permanently compliant is one of the main advantages from continuous auditing, as stated by the interview participants **(e1, e2, c1p1, c1p2, c2p1, c2p2)**.

There is need for a report of the CSP to prove they have worked according to the agreements and that non-compliance, if that happens, would be reported **(c1p1, c2p2)**. It is also noted that cloud customers should make demands towards their CSP **(e1, e2, c1p1, c2p1)** concerning certification and control.

Company 2 stated that ISO 27k on itself is not enough to guarantee control **(c2p1, c2p2)**. Company 2 has extensively applied the COBIT framework and uses tooling to manage governance, risk and compliance. Furthermore a new standard could become a demand from clients of these companies, to comply to these standards would then be mandatory.

The internal control set of companies is mapped to standards **(e2, ey)**, this is an important enabler concerning control and compliance reporting. This administration is checked by auditors, automation and use of compliance tooling can be an important advantage **(e2, ey)**. Furthermore an important driver for certification is the demand from customers, regulators or the fact that customers also do it **(e2, ey)**.

The TOE adoption-factors identified are: Organization (being permanently 'in control' and compliant, reporting that commitments are fulfilled, internal mapping of controls to standards, automation can improve efficiency of reporting) and Environment (demanding new certification at provider, demands from clients concerning security, support from regulators, customers or competitors)

5.3.2 Standards / Regulatory

Each of the interviewed companies is under supervision of DNB and thus apply the risk guidelines before procuring cloud services. However, Company 1 is not under full supervision because their headquarters are located in the United States. Additionally they offer services and procure cloud-services that do not require full supervision. Company 2 is under full supervision of DNB. Company 1 uses cloud services in several business units and acknowledges that local regulations create a burden and uncertainty to which regulations they need to comply **(c1p1)**. It was also questioned if the current certifications give enough assurance **(c1p1, c2p1)**.

Regulators and supervision authorities should support the use of a single standard for continuous auditing, they have a key role in the adoption of standards in the financial world **(e1, e2, c1p1, c2p1, c2p2, ey)**. It is perceived as a big advantage if there would be an EU-wide standard **(e1, c1p1, c1p2)**, as it would minimize compliance issues between different countries. Every company should adopt to this standard **(c1p1)**. Barriers in this sense are the unique processes, architectures and controls **(e2, c2p2, ey)**, which make it difficult to implement a 'standard way' for gathering data. Additionally, it's possible that compliance with standards is treated differently between countries. Furthermore it was noted by the certification authority **(ey)** that compliance reporting is increasing, thus adding another standard would potentially create more burden.

The TOE-factors identified are: Environment (the regulators/supervisors should adopt the standard, supported by the European Commission, every company should adapt to this standard) and Organization (advantage with an EU-wide standard, different architectures make it difficult to adopt, difference in regulation and compliance between countries, increasing compliance reporting).

5.3.3 Cloudprovider

At Company 1 the risk management of cloud assets is aimed at transferring risk to the CSP **(c1p1)**, which was mainly aimed at financial risks and not security risks **c1p2**. The current contracts with the CSPs are focused on assurance and continuity **(c1p1, c1p2, c2p1)**. The contractual arrangements of Company 1 are focused on risk transference to the CSP concerning security, which means providing a secure environment is the provider's task **(c1p1, c1p2)**. Contractual agreements were made that made the CSP legally accountable.

The initial risk assessment is done by both companies as it is mandatory **(c1p1, c1p2, c2p1, c2p2)**. Company 1 applies their mandatory global vendor-assessment from their US headquarters, further they rely on compliance reporting from their provider. Periodical reviews are not done by Company 1 but Company 2 uses their 'right to audit' to have regular reviews at their CSP.

Both companies get the periodic ISAE/SOC reporting from their CSP, furthermore they make contractual (SLA) agreements to declare the responsibilities of the provider. Data privacy breaches are reported as required by the GDPR. ISO 27001-compliance is deemed insufficient by Company 2 while considering cloud security and control.

The main demand that came forward in the interviews **(e2, c1p1, c1p2, c2p2)** is that notifications of non-compliance should be tailored to their specific cloud system (multi-tenant) and not to the CSPs infrastructure as a whole. Both companies noted that it is sometimes difficult to put demands on a CSP, because they are a small customer who cannot demand a new certification **(c1p1, c1p2, c2p1)**. This is a barrier to the adoption of EU-SEC. Furthermore the willingness of the CSP to provide information is considered an important barrier **(e2, ey)**. Mainly because they in general don't want to disclose any security or incidents-related information publicly.

The implementation of a standard data-feed by the provider is considered an important driver for continuous auditing **(e1, e2)**, as well as the critical mass among CSPs that is needed to make the adoption a success **(e2, ey)**. Since the CSPs have their monitoring automated already, this can be an important advantage for continuous auditing **(ey)**.

The TOE-factors identified are: Technology (system-specific notifications of non-compliance), Environment (difficult to request extra demands/certifications, critical adoption mass) and Organization (data-feed by provider, resistance to share information).

5.3.4 EU-SEC

The unanimous opinion of all interviewees is that the continuous gathering of evidence and executing data analysis is a big improvement and driver for EU-SEC adoption **(e1, e2, c1p1, c1p2, c2p1, c2p2, ey)**. Furthermore, the benefits for the cloud-customer and provider need to become clear **(e2, c1p1, c2p1, ey)** , when the benefits do not compensate the costs for implementation it can be a barrier to EU-SEC adoption. The coverage of additional risks, the added value, costs and viability of EU-SEC is an important driver for adoption **(e2, c1p1, c2p1, ey)**.

Being able to prove continuous compliance is considered an important driver for using EU-SEC **(e2, c1p1, c2p2)**. However, the relevance of non-compliance notifications is considered an issue. The notifications need to be relevant to the customer to be of value **(e2, c1p1, c2p1)**. The impact that the implementation and use of EU-SEC has to the CSP, needs to be considered and can be a barrier to adoption **(c1p1, c2p1)**.

When compliance to other standards can be shown with the Multi Party Recognition (MPR) mapping as enabler, this can be an important driver for the adoption of EU-SEC **(c2p2 ey)**. One of the main barriers to EU-SEC is the fact that not all data (for example qualitative data) can be measured automatically, which is acknowledged by the interviewed auditors **(e1, ey)**. The automation of evidence gathering for audits would be an important advantage for the auditing profession **(e1, ey)**.

Concerning the adoption of EU-SEC as an successful standard, the support and accreditation of this standard by a governing body would be an important driver for adoption **(e2, ey)**. ISO, for example, has a governing body that gives accreditation and checks certification procedures accordingly. For a new standard to be a success this would be an important driver.

Practical questions like withdrawing a certificate within EU-SEC should be handled with care **(e2, ey)**. For example, a grace period to fix irregularities in compliance should be taken into account before withdrawing a certificate. EU-SEC is considered to cover gaps in current certifications, additionally the market moves towards continuous monitoring which is also an important driver **(e1, e2)**. From a technological perspective the most important barriers would be the uniqueness of organizations and their automation and only part of the controls can be automated, the certification authority only sees EU-SEC as a possible additional service offering next to the other types of certifications **(ey)**. The security expert **(e2)** mentioned the importance of the EU-SEC tooling to be open source, since it is funded by the EU. Furthermore this expert considered the mandatory use of EU-SEC for (financial) organizations as an important driver for adoption **(e2)**.

The TOE-factors identified are shown in Appendix D.

5.3.5 Sector-specific

Since this research is focused on organizations in the financial sector, the specifics of this sector were analyzed in these interviews. One of the interviewees **(c2p2)** noted that there is a high dependence on a small number of providers. For example, Microsoft cloud products or SalesForce is used by practically every organization in the financial world. These providers are assumed to be 'too big to fail' but still represent a high dependence within the financial world. His opinion is that regulators and governments should be more involved in mitigating this type of risk and must give directions. Furthermore, one expert **(e2)** noted that the financial sector differs from other sectors, because of the mandatory requirements/regulations. The private sector has more freedom to which standards they want to adopt, which for EU-SEC can be a challenging barrier.

Chapter 6

Conclusion

Risk management in cloud environments proves to be a big challenge these days. While financial services organizations were reluctant to move their assets into the cloud, there has been a shift in favor of cloud adoption. The focus is however on private cloud, which doesn't utilize the full potential benefits that cloud computing has. Trust, risk management and control are the main issues in the cloud, since IT assets are no longer placed in-house but in the hands of a cloud provider. Standards have been developed to tackle these issues and provide cloud customers with assurance reporting on security controls and the importance of risk management has been emphasized by regulators.

By executing a systematic literature search, the state of art concerning risk management frameworks in the cloud was investigated:

> ***Q1: What is the state of art concerning risk management frameworks in the cloud?***

A number of standards have been developed for security management and assurance reporting, like ISO 27001, ISAE and SOC. They however lack the capability to cover all risks in cloud environments and only give a snapshot (point in time) review of controls, rather than a continuous overview of compliance and certification. There is a disconnect between the information need of the cloud customer and the infrequent reporting provided by conventional assurance schemes. Risk management practices need to be aligned between the cloud provider and cloud customer, furthermore the reporting frequency needs to be increased by use of continuous auditing of security controls.

An additional systematic literature search covered the 'continuous auditing' topic:

> ***Q2: What research has been done into continuous auditing and what are the recent developments?***

Continuous auditing ensures that changes in the cloud environment are detected continuously and reported for monitoring and auditing purposes. This continuous feedback is highly important for cloud customers to be able to state they are compliant with regulations and creates trust of being 'in control' over their information assets.

This research puts emphasis on the recent developments within the Cloud Security Alliance and the EU-SEC framework funded by the EU. This framework can fill the gaps that are currently present in cloud risk management and auditing. The EU-SEC framework consists of a control repository that identified and mapped all relevant standards and regulations, auditing requirements and tooling that provides continuous auditing capabilities by the use of a standard meta-framework for input- and output-data.

Monitoring of the cloud infrastructure is already done by CSPs and current compliance is shown by mapping controls to standards. EU-SEC builds the bridge between internal control of CSPs and external third party certification, by using the monitoring data available and analyzing it to show compliance. As such, the efficiency of showing compliance can be increased.

By using a standard output feed, standard tooling can be used to show compliance. System-specific notifications will be an important advantage for cloud customers. Additionally, showing compliance with current standards might be shown by applying the EU-SEC framework with mapping.

Q3: What are the drivers and barriers in the adoption of EU-SEC?

The interview results have indicated that the benefits of this new framework need to be clear to make it a viable addition to current risk management practices. One of the mentioned advantages is that the framework takes into account EU-wide regulations and standards, as such it can be used throughout the EU. Enabling the organization to show permanent control and compliance, by continuous evidence gathering and data analysis, is the biggest added value of EU-SEC.

For analyzing the adoption factors, the TOE-framework was used. The TOE-framework consist of the Technology, Organization and Environment part which influences the adoption of standards.

The barriers and drivers for the **Technology**-part are mainly in usability. The framework needs to be easy to implement, standardization of data interpretation is an important aspect, continuous feedback is seen as a big advantage. The framework covers the additional information needs, in the sense that it guarantees continuous compliance instead of point-in-time compliance. Furthermore the notifications need to be for the specific system that the cloud customer uses. The difficulty to gather qualitative data was mentioned as a shortcoming in the framework. Additionally the uniqueness of provider's way of working could be a barrier, since automation needs to be tailored to a specific provider. The expectation of the certification authority is that EU-SEC won't replace other standards, but instead can be offered as an additional service.

For the **Organization**-part the benefits need to be clear, additional risks need to be covered that are not covered by conventional audits. Notifications need to be relevant to the cloud customer. The proof of real-time compliance was mentioned as the main advantage of EU-SEC. However the costs of implementation need to be taken into account as well. There needs to be a solid business case for financial services companies to stimulate adoption. From the provider side it can be a challenge to implement a data-feed which is compliant with EU-SEC, because the datasets and infrastructure monitoring differ for each provider.

The **Environment** factor is coming forward as a big driver in the financial world when it comes to adoption of standards. Financial services organizations are under supervision of regulatory bodies. Regulatory authorities such as the DNB can provide an opinion about continuous auditing in cloud environments and stimulate the use of EU-SEC. When the viability of the EU-SEC framework is proven, the mandatory use of this framework might be the next step. In that way financial services organizations have an incentive to adopt and this creates a critical mass that stimulates adoption.

The 'critical mass' is perceived as one of the main drivers in adoption, when a number of financial services organizations adopt and support this framework. One perceived advantage of the EU-SEC framework is that it covers EU-wide regulations, in this way the burden of national regulations is solved by adopting one single standard for compliance. However, one of the barriers to adoption is the (un)willingness for CSPs to adopt 'yet another standard' and for them to provide the right data-feed as input for the continuous audit process. Cloud customers should put more emphasis on continuous auditing at their CSPs as it is part of new regulations in the financial industry. Consequently, the incentive for CSPs would be bigger if a number clients ask for continuous certification.

For EU-SEC to become a success, it must be a governed standard. This means that the standardization process should take place, including assigning a governing body and accreditation of certification authorities. The expectation is that EU-SEC will only be adopted when it is a regulatory requirement that is supported by governments and supervising bodies, as well as a governing body and several market parties that adopt it.

Main research question:

What are the drivers and barriers to adoption of a cloud risk framework for continuous assurance in financial services?

Overall the adoption of EU-SEC has advantages in the form of perceived benefits: covering the gaps in current risk management / assurance standards and continuous compliance, as well as bridging the gap between national regulations EU-wide. However, the success of this framework relies strongly on the willingness of the cloud-providers to provide a tailored and standardized data-feed per customer. Furthermore, there needs to be a strong business case to support EU-SEC to boost the adoption. Regulating and supervision authorities should make such framework mandatory for financial services. A 'critical mass' is needed to boost the adoption of this framework, yet standardization of the framework will take some time.

The focus of the EU-SEC project participants should be on getting all stakeholders on board and make the advantages of this framework clear. Making EU-SEC a governed, accredited and certified standard should also be a top priority. Only in that way it can gain the momentum that is needed for adoption of EU-SEC. Furthermore, the new regulations of the EBA and ECB should be incorporated in the requirements of EU-SEC.

The contributions of this research can be put into three perspectives: cloud customer, auditor and science.

For the **cloud customer** within financial services, the developments in continuous auditing are highly relevant. From a regulatory, governance and security perspective there is an increasing demand to gain permanent insights in compliance of cloud solutions. This research gains insight into the adoption of continuous auditing and the barriers that need to be overcome to make this a success. Benefits of adopting this standard need to be clear, as well as the incentive for regulators to stimulate adoption. The resistance from CSPs to provide full insight in their permanent compliance can be a barrier to adoption. Cloud customers should put more emphasis on the alignment of risk management practices with their CSP, as well as the compliance information that should be reported on more frequently.

The **cloud auditor** can further automate the auditing and compliance reporting process. Since most CSPs have already implemented continuous monitoring with permanent insight in their processes, the adoption of EU-SEC can make sure the relevant data for compliance is extracted and analyzed accordingly. In this way, it can be used as addition to the traditional point-in-time auditing and may even be used to show compliance to existing standards. Continuous audit reporting can be a valuable addition to conventional audits, as they provide a more frequent insight in control and compliance. This can be a valuable business case for auditors, since they can improve the efficiency of audits and satisfy the information needs of the cloud customer. Cooperation with CSPs is key in this sense, investments in continuous auditing should be done to make it a success.

From a **scientific context** this research gives insight in the technology adoption factors and the state-of-art concerning risk management and continuous auditing in the cloud. This research also provides valuable insight in adoption drivers and barriers for the participants in the EU-SEC project. Essential factors need to be taken into account, barriers need to be overcome to make the project a success. In the past it has been proven that standards are adopted carefully, resistance to adoption can be a big barrier and benefits of the standard need to be clear. The above mentioned drivers and barriers should be taken into account by all concerned parties, who should be working together to stimulate the industry-wide adoption of a standardized approach towards continuous auditing of cloud environments.

In the next section the discussion and suggestions for future research are given.

Chapter 7

Discussion and Future Research

In this research the factors concerning the adoption of EU-SEC were researched. Risk management principles and cloud control measures, including certification were investigated to provide a foundation for this research.

Three auditing experts and one security expert from a Dutch bank were interviewed, as well as two experts of financial services companies. Concerning the different nature of each of the interviewed organizations, the results cannot be generalized to the financial sector as a whole. They differ in regulatory requirements and attitude towards risk management in cloud computing. However, because of the typical systems and risks that are present in the financial sector, each of the organizations faces the same developments concerning risk control and continuous auditing. The interview results have shown consensus concerning the factors that lead to standards and continuous auditing adoption and give strong support for relevance. Some of the findings have limited support but can still be included because they provide valuable opinions and context of the involved organizations.

Future research can focus on establishing integration with current continuous monitoring systems at CSPs for use with the EU-SEC framework. The barriers for cloud providers concerning adoption of EU-SEC can be researched, to clarify the CSPs views towards this new phenomenon. Additionally the reliability and assurance of test results produced by tooling proposed by EU-SEC needs to be piloted and assessed, to ensure that the output can be legally used as evidence in audits. Validation of the tooling and framework needs to take place to ensure that it covers the requirements for auditing, assurance and certification. Assigning a governing body for EU-SEC and ensuring regulatory authorities and governments to be on board is an important task. Since the financial industry is relying heavily on regulatory demands this is the main driver for adoption. Authorities can stimulate the use of EU-SEC to encourage the adoption, since it can be a valuable addition compared to conventional audits.

Appendix A

ENISA Cloud Computing Security Risk Assessment

An overview of the risks mentioned in [12]

A.1 Policy and Organizational Risks

- R.1 Lock-In
- R.2 Loss of governance
- R.3 Compliance challenges
- R.4 Loss of business reputation due to co-tenant activities
- R.5 Cloud service termination or failure
- R.6 Cloud provider acquisition
- R.7 Supply chain failure

A.2 Technical risks

- R.8 Resource exhaustion (under or over provisioning)
- R.9 Isolation failure
- R.10 Cloud provider malicious insider - abuse of high privilege roles
- R.11 Management interface compromise (manipulation, availability of infrastructure)
- R.12 Intercepting data in transit
- R.13 Data leakage on up/download, intra-cloud
- R.14 Insecure or ineffective deletion of data
- R.15 Distributed denial of service (DDoS)
- R.16 Economic denial of service (EDOS)
- R.17 Loss of encryption keys
- R.18 Undertaking malicious probes or scans
- R.19 Compromise service engine
- R.20 Conflicts between customer hardening procedures and cloud environment

A.3 Legal risks

- R.21 Subpoena and e-discovery
- R.22 Risk from changes of jurisdiction
- R.23 Data protection risks
- R.24 Licensing risks

A.4 Risks not specific to the cloud

- R.25 Network breaks
- R.26 Network management (ie, network congestion / mis-connection / non-optimal use)
- R.27 Modifying network traffic
- R.28 Privilege escalation
- R.29 Social engineering attacks (ie, impersonation)
- R.30 Loss or compromise of operational logs
- R.31 Loss or compromise of security logs (manipulation of forensic investigation)
- R.32 Backups lost, stolen
- R.33 Unauthorized access to premises (including physical access to machines and other facilities)
- R.34 Theft of computer equipment
- R.35 Natural disasters

Appendix B

Interview type 1: Cloud Customer (FSO)

B.1 Introduction

1. Participants in the interview
2. Goal of the interview: standards are not enough to be continuously in control.

B.2 Context

1. Organization: name, number of employees, customers, turnover, services provided.
2. Role of the interviewee.
3. Which regulations need to be complied to? Who is the supervising authority?
4. What does the application landscape look like? Type of system / data
5. Which applications are characteristic for the financial world?
6. What are the risk profiles of these systems? Which systems are high-risk?
7. How is security an privacy managed?
8. Which of these systems are in the cloud? Or going to be in the cloud?

B.3 Governance / Risk Management

1. Which guidelines are followed with outsourcing of IT assets?
2. How is the current risk management applied? Who makes the requirements?
3. Are the 'three lines of defense' applied within the company?
4. What is the origin of the current risk management? Who made it or which standard is applied?
5. Which risk assessment is used for cloud outsourcing?
6. Is the current risk management process aligned with that of auditors and regulators?
7. What are the challenges in risk management for cloud?

B.4 Cloud security management

1. Which agreements are made with CSPs when outsourcing?

2. How do you prove that you are 'in control'?
3. Which certifications do you have internally and which ones has your cloud provider?
4. Which assurances are given by these certifications?
5. Is there any additional information given by your CSP, apart from certifications?
6. Which additional information is needed from your CSP, apart from certifications?

B.5 Continuous assurance in the cloud

1. Which measures are needed to be fully 'in control' over high-risk applications?
2. Who audits the cloud provider? Which assurances does this give?
3. Which additional assurances are desirable?
4. Can a framework for continuous auditing/monitoring be a solution?
5. Which challenges lay in the adoption of such a framework?
6. What is needed to make such framework attractive? What are the essential adoption drivers?
7. Is it important to provide mapping to current standards?
8. Which role has the regulator and supervising body in the adoption?
9. Is it important to have regulators make it an official standard?
10. Which guidance is needed to implement this framework? Which information is needed?
11. What is needed for you to declare full assurance over cloud outsourcing?

Appendix C

Interview type 2: Cloud Auditor

C.1 Introduction

1. Participants in the interview
2. Motivation behind interview / standards are not enough to be continuously in control
3. Which clients is CertifyPoint serving? What are the services offered?

C.2 Certification

1. What is the current procedure concerning certification?
2. What are the bottlenecks and shortcomings?
3. To which extent are certifications automated?
4. Is it sometimes needed to check continuously?

C.3 Continuous auditing

1. How far is EY with continuous auditing?
2. Do clients apply continuous auditing already?
3. Do competitors apply continuous auditing?
4. What's EY's vision on continuous auditing?
5. What implications does continuous auditing have for EY?
6. Is innovation driving developments or is resistance blocking it?

C.4 EU-SEC

1. How is EY involved in the project?
2. What is EY's opinion about the project?
3. What is needed to make EU-SEC a success?
4. Which problems are expected to be solved by using EU-SEC?
5. What are the drivers to adoption?
6. What are the barriers to adoption?

C.5 Innovation

1. Does EY think technology can fully replace a traditional audit?
2. Would EY invest in a continuous auditing system?
3. Who is going to pay for it?
4. Which benefits does EY get from continuous auditing?

Appendix D

Interview results – Adoption

Topic / Results (sorted on occurrence)	**Experts**		**Comp.1**		**Comp.2**		**EY**	**TOE**
	E1	**E2**	**P1**	**P2**	**P1**	**P2**	**CP**	
Governance / Risk Management / Compliance								
Begin permanently 'in control' and compliant	✓	✓	✓	✓	✓	✓		O +
Demands towards provider concerning risk management and certifications	✓	✓	✓		✓			E +
Clients can have certain demands concerning security			✓	✓			✓	E +
Report that nothing happened / fulfillment of commitments			✓			✓		O +
Companies have their internal control set mapped to standards		✓					✓	O +
Internal control set checked by auditors; automation and minimizing efforts to show compliance		✓					✓	O +
Certification is done because: customers, regulators want it or competitors do it		✓					✓	E +
Standards / Regulatory								
Support from governments and supervising authorities	✓	✓	✓		✓	✓	✓	E +
EU-wide framework		✓	✓		✓	✓		O +
Supported by the EC	✓	✓					✓	E +
Organizations must adopt the same framework		✓	✓			✓	✓	E +
Organizations have their internal processes to gather evidence & architectures and control set are unique		✓				✓	✓	O –
Countries interpret rules differently, no general way to show compliance		✓					✓	O –
Multiple standards and increasing reporting, adding another standard would create more burden						✓	✓	O –

TABLE D.1: Interviews – Results

Topic / Results (sorted on occurrence)	**Experts**		**Comp.1**		**Comp.2**		**EY**	**TOE**
	E1	**E2**	**P1**	**P2**	**P1**	**P2**	**CP**	
Cloudprovider								
Specific notifications for my system (multi-tenant data feed)		✓	✓	✓		✓		T +
Small customer, little influence on provider (difficult to demand new certification)			✓	✓		✓		E −
Standard-feed implemented by provider	✓	✓						O +
Providers have their unique management systems: confidentiality / resistance to share information		✓					✓	O −
Market parties must adopt new standards (critical mass)		✓					✓	E +
Providers have own monitoring and compliance checking already (autom.)							✓	O +
EU-SEC								
Continuous evidence gathering / data analysis is an improvement	✓	✓	✓	✓	✓	✓	✓	T +
What are the advantages / benefits of EU-SEC?		✓	✓		✓		✓	O −
Covering additional risks / added value / costs / viability		✓	✓		✓		✓	T +
Being ’demonstrable compliant’ is advantage		✓	✓			✓		O +
Which actions are taken on notifications? Relevant notifications		✓	✓		✓			O −
Impact on CSP			✓		✓			O −
Showing compliance to other standards with EU-SEC (MPR)						✓	✓	O +
Qualitative data cannot be measured automatically	✓					✓		T −
Automation would be an improvement for auditors	✓						✓	T +
Governing body and accreditation; EU-SEC should become full standard		✓					✓	E +
Certificate withdrawn with non-compliance (grace period needed?)		✓					✓	E −
EU-SEC covers gaps, market moves towards continuous monitoring	✓	✓						O/E +
Organizations have their unique way of working, automation needs to be tailored							✓	T −
Only part of controls can be automated, EU-SEC can be additional service offering							✓	T −
Open source ’plug and play’ tooling		✓						T -
EU-SEC must become mandatory		✓						E +

TABLE D.2: Interviews – Results – Contd.

Bibliography

[1] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges”, *Information sciences*, vol. 305, pp. 357–383, 2015.

[2] S. Bannink, “Cloud risks in the financial world: Do current security and compliance standards cover them?”, 2018.

[3] J. Brodkin, “Gartner: Seven cloud-computing security risks”, *Infoworld*, vol. 2008, pp. 1–3, 2008.

[4] M. Carroll, P. Kotzé, and A. Van Der Merwe, “Securing virtual and cloud environments”, in *Cloud Computing and Services Science*, Springer, 2012, pp. 73–90.

[5] M. Carroll, A. Van Der Merwe, and P. Kotze, “Secure cloud computing: Benefits, risks and controls”, in *Information Security South Africa (ISSA), 2011*, IEEE, 2011, pp. 1–9.

[6] V. Casola, A. De Benedictis, and M. Rak, “Security monitoring in the cloud: An sla-based approach”, in *Availability, Reliability and Security (ARES), 2015 10th International Conference on*, IEEE, 2015, pp. 749–755.

[7] D. Y. Chan and M. A. Vasarhelyi, “Innovation and practice of continuous auditing”, *International Journal of Accounting Information Systems*, vol. 12, no. 2, pp. 152–160, 2011.

[8] S. A. de Chaves, C. B. Westphall, and F. R. Lamin, “Sla perspective in security management for cloud computing”, in *Networking and Services (ICNS), 2010 Sixth International Conference on*, IEEE, 2010, pp. 212–217.

[9] D. C. Chou, “Cloud computing risk and audit issues”, *Computer Standards & Interfaces*, vol. 42, pp. 137–142, 2015.

[10] *Cloud certification schemes meta framework (ccsm)*, `https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework`, ENISA, 2014.

[11] *Cloud computing information assurance framework*, `https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework/`, ENISA, 2009.

[12] *Cloud computing risk assessment*, `https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment`, ENISA, 2009.

[13] *Cloud controls matrix v3.0.1*, `https://downloads.cloudsecurityalliance.org/assets/research/cloud-controls-matrix/CSA_CCM_v.3.0.1-09-01-2017_FINAL.xlsx`, Cloud Security Alliance, 2017.

[14] *Cloudaudit working group*, `https://cloudsecurityalliance.org/group/cloudaudit/`, Cloud Security Alliance, 2018.

[15] *Cloudtrust protocol working group*, `https://cloudsecurityalliance.org/group/cloudtrust-protocol/`, Cloud Security Alliance, 2018.

[16] *Consensus assessments initiative questionnaire v3.0.1*, https://downloads.cloudsecurityalliance.org/assets/research/consensus-assessments/CAIQ_v3.0.1-09-01-2017_FINAL.xlsx, Cloud Security Alliance, 2017.

[17] *Csa code of conduct for gdpr compliance*, https://gdpr.cloudsecurityalliance.org/wp-content/uploads/sites/2/2018/06/CSA-Code-of-Conduct-for-GDPR-Compliance.pdf, Cloud Security Alliance, 2017.

[18] *Csa security, trust & assurance registry (star)*, https://cloudsecurityalliance.org/star/, Cloud Security Alliance.

[19] *D 1.2 security and privacy requirements and controls*, http://www.sec-cert.eu/, EU-SEC, 2018.

[20] *D 1.3: Auditing and assessment requirements*, http://www.sec-cert.eu/, EU-SEC, 2018.

[21] *D1.4 principles, criteria and requirements for a multi-party recognition and continuous auditing based certifications*, http://www.sec-cert.eu/, EU-SEC, 2018.

[22] *D2.2 continuous auditing certification scheme*, http://www.sec-cert.eu/, EU-SEC, 2017.

[23] DNB, *Sjabloon cloud computing risicoanalyse - voor op openboek*, http://www.toezicht.dnb.nl/binaries/50-228202.pdf, DNB, 2013.

[24] F. Doelitzscher, C. Reich, M. Knahl, and N. Clarke, "Understanding cloud audits", in *Privacy and security for cloud computing*, Springer, 2013, pp. 125–163.

[25] B. Duncan and M. Whittington, "Cloud cyber-security: Empowering the audit trail", *International Journal on Advances in Security Volume 9, Number 3 & 4, 2016*, 2016.

[26] R. A. K. Duncan and M. Whittington, "Enhancing cloud security and privacy: The power and the weakness of the audit trail", *Cloud Computing 2016*, 2016.

[27] Z. Enslin, "Cloud computing adoption: Control objectives for information and related technology (cobit)-mapped risks and risk mitigating controls", *African Journal of Business Management*, vol. 6, no. 37, p. 10 185, 2012.

[28] European Commission, *European cloud strategy 2012*, https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy, Retrieved: 6-2-2018, 2017.

[29] *Eu-sec newsletter – issue 01 (pdf)*, http://www.sec-cert.eu/, EU-SEC, 2018.

[30] *Eu-sec: The european security certification framework*, https://cordis.europa.eu/project/rcn/207439_en.html, European Commission, 2018.

[31] R. Gorden, "Coding interview responses", *Basic Interviewing Skills. Waveland Pr Inc*, pp. 183–199, 1998.

[32] *Guidelines on ict risk assessment under the srep*, https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep, European Banking Authority, 2016.

[33] *Guidelines on the security measures under psd2*, https://www.eba.europa.eu/-/eba-publishes-final-guidelines-on-security-measures-under-psd2, European Banking Authority, 2018.

[34] *Guidelines on the security of internet payments*, `https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments`, European Banking Authority, 2014.

[35] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing", *Journal of internet services and applications*, vol. 4, no. 1, p. 5, 2013.

[36] International Organization for Standardization, "Information technology — security techniques — information security risk management", 2008, Reference number ISO/IEC 27005:2008(E).

[37] ISACA, *Cobit 5: A business framework for the governance and management of enterprise it*, `http://www.isaca.org/cobit/`, ISACA.

[38] K. Julisch and M. Hall, "Security and control in the cloud", *Information Security Journal: A Global Perspective*, vol. 19, no. 6, pp. 299–309, 2010.

[39] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing", *IT professional*, vol. 12, no. 5, pp. 20–27, 2010.

[40] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: A systematic literature review", in *Future information technology*, Springer, 2014, pp. 285–295.

[41] J. Luna, N. Suri, M. Iorga, and A. Karmel, "Leveraging the potential of cloud security service-level agreements through standards", *IEEE Cloud Computing*, vol. 2, no. 3, pp. 32–40, 2015.

[42] P. Mell, T. Grance, *et al.*, "The nist definition of cloud computing", 2011.

[43] J.-H. Morin, J. Aubert, and B. Gateau, "Towards cloud computing sla risk management: Issues and challenges", in *System Science (HICSS), 2012 45th Hawaii International Conference on*, IEEE, 2012, pp. 5509–5514.

[44] T. Oliveira and M. F. Martins, "Literature review of information technology adoption models at firm level", *The electronic journal information systems evaluation*, vol. 14, no. 1, pp. 110–121, 2011.

[45] S. Pearson, "Privacy, security and trust in cloud computing", in *Privacy and Security for Cloud Computing*, Springer, 2013, pp. 3–42.

[46] S. Pearson, J. Luna, and C. Reich, "Improving cloud assurance and transparency through accountability mechanisms", in *Guide to Security Assurance for Cloud Computing*, Springer, 2015, pp. 139–169.

[47] D. Petcu, "Sla-based cloud security monitoring: Challenges, barriers, models and methods", in *European Conference on Parallel Processing*, Springer, 2014, pp. 359–370.

[48] D. Petcu and C. Craciun, "Towards a security sla-based cloud monitoring service.", in *CLOSER*, 2014, pp. 598–603.

[49] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, and U. Villano, "Security as a service using an sla-based approach via specs", in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, IEEE, vol. 2, 2013, pp. 1–6.

[50] *Recommendations on outsourcing to cloud service providers*, `https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers`, European Banking Authority, 2017.

[51] T. Ruebsamen and C. Reich, “Supporting cloud accountability by collecting evidence using audit agents”, in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, IEEE, vol. 1, 2013, pp. 185–190.

[52] *Secure use of cloud computing in the finance sector*, `https://www.enisa.europa.eu/publications/cloud-in-finance`, ENISA, 2015.

[53] *Security and resilience in governmental clouds*, `https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds/`, ENISA, 2011.

[54] K. Singh, P. J. Best, M. Bojilov, and C. Blunt, “Continuous auditing and continuous monitoring in erp environments: Case studies of application implementations”, *Journal of Information Systems*, vol. 28, no. 1, pp. 287–310, 2013.

[55] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, *Journal of network and computer applications*, vol. 34, no. 1, pp. 1–11, 2011.

[56] L. Tao, “Shifting paradigms with the application service provider model”, *Computer*, vol. 34, no. 10, pp. 32–39, 2001.

[57] *Technical guidelines for the implementation of minimum security measures for digital service providers*, `https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers`, ENISA, 2017.

[58] H. Teigeler, S. Lins, and A. Sunyaev, “Drivers vs. inhibitors-what clinches continuous service certification adoption by cloud service providers?”, in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[59] *The treacherous 12 - top threats to cloud computing + industry insights*, `https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf`, Cloud Security Alliance, 2017.

[60] M. Theoharidou, N. Papanikolaou, S. Pearson, and D. Gritzalis, “Privacy risk, security, accountability in the cloud”, in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, IEEE, vol. 1, 2013, pp. 177–184.

[61] S. Thorpe, T. Grandison, A. Campbell, J. Williams, K. Burrell, and I. Ray, “Towards a forensic-based service oriented architecture framework for auditing of cloud logs”, in *Services (SERVICES), 2013 IEEE Ninth World Congress on*, IEEE, 2013, pp. 75–83.

[62] L. Tornatzky and M. Fleischer, “The process of technology innovation, lexington, ma”, *Lexington Books. Trott, P.(2001). The Role of Market Research in the Development of Discontinuous New Products. European Journal of Innovation Management*, vol. 4, pp. 117–125, 1990.

[63] F. de Vries and E. Koning, *Circulaire cloud computing: English final*, `http://www.toezicht.dnb.nl/en/binaries/51-224828.pdf`, DNB, 2012.

[64] J. Webster and R. T. Watson, “Analyzing the past to prepare for the future: Writing a literature review”, *MIS quarterly*, pp. xiii–xxiii, 2002.

[65] *Wet op het financieel toezicht*, `http://wetten.overheid.nl/BWBR0020368/2018-07-28`, Overheid.nl, 2018.