Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Manuel Fluri

The Impact of Cloud on an Organisation's Information Security Risk Management Process and Risk Exposure

Master's thesis in Information Security
Supervisor: Prof. Dr. Bernhard Markus Hämmerli
June 2021

NTNU
Norwegian University of Science and Technology

Manuel Fluri

The Impact of Cloud on an Organisation's Information Security Risk Management Process and Risk Exposure

Master's thesis in Information Security
Supervisor: Prof. Dr. Bernhard Markus Hämmerli
June 2021

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

The number of cloud service offerings has significantly increased over the past years, thus organisations are reviewing and adapting their IT architectures to enable the transition of applications and data into the cloud. This new way of consuming applications and processing data on third party systems also introduces new information security risks. This work investigated the impact of cloud on organisation's Information Security Risk Management and Third-Party Risk Management processes. It identified both risk focus areas and key criteria which can support an organisation's journey to the cloud. During the process six industry experts from the field were interviewed who raised a total of 15 cloud-specific risks which they perceive as posing a main challenge for their cloud journey. Furthermore, they shared four decision criteria which are used in their organisations on a regular basis to determine if the risk associated with moving a service to the cloud is acceptable or not. This work has analysed these criteria further and considers them plausible, feasible and useful for early recognition of challenges.

Contents

Figures

Tables

Acronyms

API Application Programming Interface. 38

APRA Australian Prudential Regulation Authority. 3

CASB Cloud Access Security Broker. xiii

CSP Cloud Service Provider. 25, 26, 28–33, 46, 47

DDoS Distributed Denial of Service. 39

DKIM DomainKeys Identified Mail. 41

DNSSEC Domain Name System Security Extension. 41

EY Ernst & Young. 16

GDPR General Data Protection Regulation. 4, 29, 30, 37

HSM Hardware Security Module. 25

HTTP Hypertext Transfer Protocol. 1

IaaS Infrastructure as a Service. 21, 26, 27

IP Internet Protocol. 22

ISMS Information Security Management System. 43

ISO International Organization for Standardization. 9

ISO/IEC International Organization for Standardization/International Electrotechnical Commission. 9, 11, 21, 43

ISRM Information Security Risk Management. 5, 49

KPMG KPMG International. 2, 3, 16

MAS Monetary Authority of Singapore. 4

PaaS Platform as a Service. 21, 27

PKI Public Key Infrastructure. 32

PWC PricewaterhouseCoopers. 16

RBS Risk Breakdown Structure. 10

RFI Request For Information. 24

RFP Request For Proposal. 24

SaaS Software as a Service. 21, 22, 26, 27, 30, 33, 36

SAML Security Assertion Markup Language. 38

SME Small and Medium-sized Enterprises. 7, 8, 21, 35, 37, 45–47

SOC System and Organization Controls. 22, 32

TLS/SSL Transport Layer Security / Secure Sockets Layer. 41

TPRM Third-Party Risk Management. v, vii, 2–4, 16–18, 20, 21, 23, 24, 43, 44, 49

URL Uniform Resource Locator. 22

VRM Vendor Risk Management. vii, 20, 22, 23, 34, 41–43, 46, 50

Management Summary

The technological advances around the Internet and the web protocols enabled organisations to offer sophisticated and complex applications over the Web. McAfee's Cloud Access Security Broker (CASB), the leader of Gartner's Magic Quadrant for CASB solutions from 2020 is aware of over 30,000 cloud services. Organisations can find for almost any use case a cloud-based service. Consuming key services over the Internet is also changing organisations' information security processes and risk exposure. This work focused on finding notable differences in the information security risk assessment of the third-party engagements process of organisations. Furthermore, influential criteria on information security were identified for organisational decision support, which allow organisations to identify the security impact of a potential cloud migration project. In addition, criteria were defined which help determine if consuming a cloud services is in-line with the strategy.

As part of this work a qualitative investigation has been done by means of reviewing literature and collecting empirical data from key individuals in the industry. Unstructured interviews were used as a complementary source of information to the literature. Once completed, six semi-structured interviews were held with key experts from the industry. During the interview, potential criteria were received, and later analysed on their practical relevance.

This work has identified that the process for assessing information security risks for third-party cloud engagements is identical with the historical IT approach. There are, however, five cloud specific focus areas which require more in-depth focus. Data Security & Encryption and Identity & Access Management might be the obvious areas with additional scrutiny. Organisations are also concerned about the lack of internal skills to securely configure and operate cloud services as well as the loss of legacy skills sets which could lead to vendor lock-in. The influence of Foreign Governments on Cloud Service Provider (CSP) as well as the collaboration between customer and CSP were also named as cloud-only topics of concern. Four key criteria were identified as being used to determine if there is an information security benefit coming from moving a service to the cloud: IT Maturity, Laws & Regulations, Complexity and Data & Application criticality. All four criteria were further tested and have been approved as plausible, feasible and useful for early recognition of challenges.

Chapter 1

Evolution of electronic communication

The innovation and invention of the telegraph fundamentally changed the way of human communication over long distances [1]. For the first time in history, people could send messages to each other using electric signals rather than relying on written or memorised messages carried by messengers [1]. Over a period of almost two centuries this new way of electronic communication was developed further by a series of inventions. The latest of these was probably also the most impactful: the privatisation of the internet and the introduction of the Hypertext Transfer Protocol (HTTP). Suddenly, people could, regardless of their location, communicate with each other, publish and share information. In 1994 Philip Hallam-Baker published an implementation of a web mail system [2]. The idea was quickly picked up by others and resulted in multiple web mail service offerings. Further technological advances of web protocols combined with the continuous capacity increases of the Internet connections, enabled firms to not only offer basic services and static content but also fully functional applications over the web. The number of these so-called cloud service offerings exploded over the past decade and today you can find for almost everything a public cloud service. There are numerous potential benefits for businesses which range from simplified IT operations to an easier and more transparent cost model compared to a classical on-premises operation. Both can result in a business advantage over competitors [3]. However, this new way of consuming services from a third party also has an impact on the information security risk exposure of an organisation. Previously services were hosted on-premises and the organisation's IT had to ensure it had an adequate level of information security maturity, with cloud services the same must be provided by the cloud service vendor. Therefore, organisations should understand if and how consuming cloud services impacts the way information security risks are assessed and managed, how services need to be secured and how it influences their dependency on third parties.

1.1 Third-Party Risk Management

Organisations have an increasing dependency on third parties, which introduces additional risks potentially impacting their business [4]. Such a third-party network can be vast and stretch across all aspects of a business as illustrated by figure 1.1 [5]. Organisations have noticed this increasing dependency on third parties and with that also the increased risk in case of their failure [4]. A thorough third-party risk management process manages the life cycle of a third-party engagement from the selection, throughout the service delivery until the termination[4] [6]. The scope of TPRM includes all potential third-party risks which span across mul-

Figure 1.1: The figure illustrates the complexity of a third-party network of an organisation. [5]

tiple disciplines [4][5]. There are various different approaches to illustrate and categorise these risks. The approach from KPMG International illustrated in figure 1.2 seems to be the most comprehensive one [4]. Looking at figure 1.2 it also becomes clear that TPRM is not something which can be covered by a single discipline. It requires involvement of various subject matter experts from legal, IT, supply chain management, etc. and somebody needs to take the lead to coordinate everything [4]. Which raises an additional challenge: How can risk perception be aligned across the organisation to create a common understanding about which services can be outsourced and which cannot be. As per KPMG more than half of the respondents struggle with this and stated that they are far away from having an enterprise-wide agreement [4]. Moreover, a proper assessment requires data which need to be acquired and edited before they can be processed. It seems that

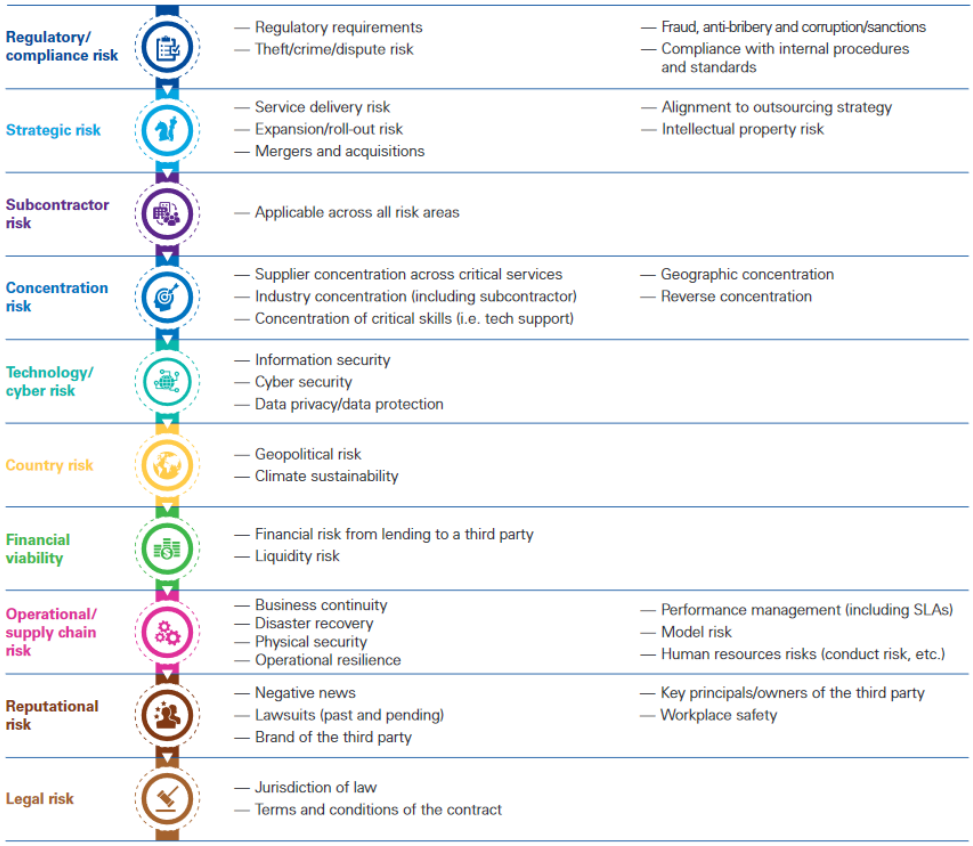


Figure 1.2: List of third-party risk areas. [4]

only 26 percent of the respondents to KPMG's survey feel that they have all the data they need [4]. Concluding, that TPRM is a very useful tool to manage third-party relationships but it is very complex. A lot of stakeholders need to be involved and many risk areas need to be covered. Thus, it is not surprising that many firms feel their process is not as mature as could be.

1.1.1 Law & Regulation

Not only organisations are increasingly focusing on TPRM but also lawmakers and regulators across the globe have picked this up. Especially in the financial services sector numerous regulators have introduced guidelines for firms in the industry [7]. While figure 1.3 is showing the situation from 2017, regulators have introduced revisions or additional guidelines since then. On July 1st 2019, the Prudential Standard CPS 234 Information Security was put into effect. Banks and insurances regulated by the Australian Prudential Regulation Authority (APRA) are obliged to assess a third party's information security capabilities if the third party processes data of the institution. Additionally, the service consuming entity needs to evaluate the impact of an information security incident at the third

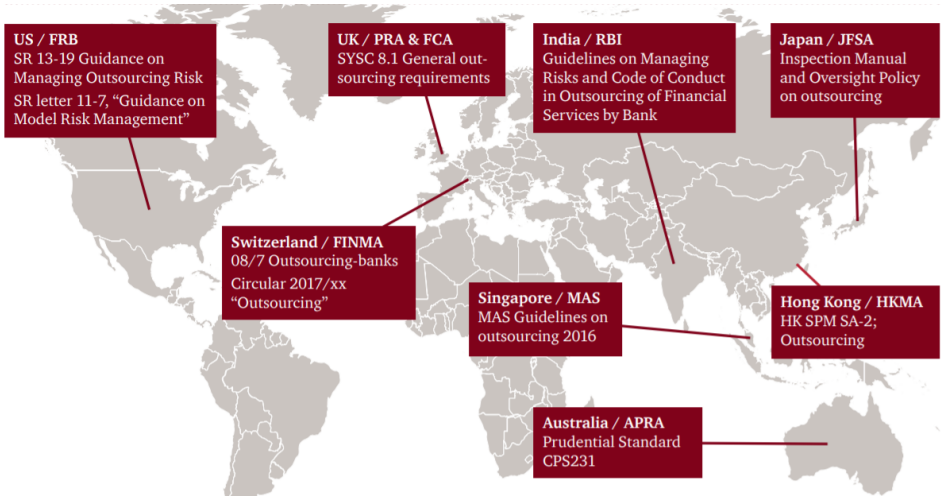


Figure 1.3: TPRM regulations for firms in the financial services in selected financial markets. [7]

party concerning the service consumer's data [8]. As an additional example the Monetary Authority of Singapore (MAS) have revised their Technology Risk Management guidelines in January 2021 [9]. But such requirements were not only introduced in the financial sector. The European Data Protection Regulation better known as General Data Protection Regulation (GDPR) which was put in effect on May 25th, 2018 is not directly mentioning a TPRM process. However, a controller (Art. 4) is responsible for the data even if it is with a third party processing the data (Art. 24). Thus, creating high incentive to apply appropriate due diligence if a third-party processes data.

1.2 Information Security Risk Management as Part of TPRM for different Service Delivery Models

A lot of IT vendors move their offerings from a classical on-premises to a public cloud based model. The most obvious change coming with this transition is often the billing model. Providers seem to move to a subscription or consumption based payment scheme, rather than a user license with perpetual maintenance costs. However, with the change of the service delivery model it would also be interesting to understand which other aspects change. A holistic third-party risk management process consists of many aspects, thus requires involvement of various specialists, e.g. legal, supply chain management, etc. It is therefore important to clearly specify the scope of this work and set expectations. This work deep-dives into how information security risks appear, disappear, shift, or duplicate between the service provider and the service consumer in regards to the chosen service delivery model. Thus, the three objectives of this thesis are specified as follows in table 1.1.

Table 1.1: The three objectives of this thesis.

O-ID	Objective
1	Help IT security professionals understand the implications of moving an IT service to the cloud in regards to Information Security Risk Management (ISRM).
2	Analyse the appearance, disappearance, duplication and transfer of information security risks and risk mitigation efforts depending on the service delivery model: on-premises or cloud service.
3	Define comparison criteria which can be used to analyse the impact of a service transition to the cloud from an ISRM perspective.

To meet the set objectives in table 1.1 five research questions were defined in table 1.2.

Table 1.2: The five research questions this thesis seeks to answer.

RQ-ID	Research Questions
1	Which elements should a third-party information security risk assessment include?
2	Which are the differences in terms of information security risks between a cloud based and an on-premises service delivery model?
3	Does the customer profit in respect to information security risk by moving a service to the cloud?
4	Which criteria are most relevant as distinguishing factors for an information security risk comparison between the delivery models?
5	Into which additional risk mitigation measures should a cloud service customer invest?

In summary the aim of this work is to look into how firms could do information security risk management within their third-party risk management process. Furthermore, analyse if there are any differences in information security risks between different delivery models (on-premises vs. public cloud) which should be considered and consequently, if there are any different or additional risk mitigation measures.

1.2.1 Exclusions

While third-party risk management must include subject matter experts from many disciplines, it is not the intention to deep-dive into areas other than information security, and analyse how these are influenced by different service delivery models. Moreover, this work is also assuming that the business case for moving to the cloud has been reviewed, risk assessed and approved by the business. This decision will not be questioned.

1.2.2 Target Audience

The target audience for this paper are information security professionals which need to assess the evolution of risk when adopting cloud services. In the wider scope it also includes any interested IT personnel or IT researcher. Thus, this thesis will not reiterate on the definition of cloud services and deployment models and assume that it is common knowledge within the target audience. Readers not familiar with the terms can review literature like [10] or [11] to gain a basic understanding about cloud deployment and service models.

Chapter 2

Background

2.1 Benefits of moving to The Cloud

In [3] the authors investigated the operational and strategic benefits coming from the consumption of cloud services. They posited those benefits differ between Small and Medium-sized Enterprises (SME) and large enterprises, conducting a survey of 45 individuals in top management positions, they looked at key capabilities of cloud services which are summarised in table 2.1.

Table 2.1: Characteristics and Capabilities of Cloud Computing

C & C	Description
Heterogeneity	The cloud approach enables companies to consume heterogeneous IT resources.
Scalability	Cloud offerings are highly scalable and can add or remove resources quickly based on the customer's needs.
Consumption Based Pricing	Cloud service customers are mostly charged based on a 'pay-per-use' model.
Fully Managed	Cloud services are fully managed by the third party offering it.
Standardised Services	The objective of a cloud vendor is to offer the cloud service to many customers. Hence, these services are more standardised in their technical specifications and interfaces.
Availability	Cloud service providers promise very high availability of their service. They are able to do so because they invest in redundant equipment and pool resources.
Accessibility	Cloud offerings are provided over the internet, allowing service customers to access the service from anywhere.

They separated responses from SMEs and large enterprises. In 2.2 the benefits outlined in [3] are summarised per characteristic and capability. In summary, in general the authors conclude that larger firms are focusing more on exploitative

activities, hence derive operational benefits. Whereas SMEs focus on innovation and exploratory usage of cloud services, allowing them to derive strategic benefits.

Table 2.2: The summarised results of the survey.

C & C	SME	Large enterprises
Heterogeneity	Access to state-of-the-art heterogenous resources which without cloud services would not be possible to build and maintain.	N/A
Scalability	Benefit of scaling their workloads better and make consumption more effective. Also can pursue new business opportunities without making large investments	Services with high variations in demand or unpredictable market conditions benefit from cloud scalability.
Consumption Based Pricing	Ability to remain cost efficient by only paying for what they are using.	Ability to increase cost efficiency by minimizing capital expenditure.
Fully Managed	Consuming cloud services means that SMEs can focus on their core competencies.	Improved cost efficiencies by reducing or eliminating some infrastructure related tasks and streamlining IT processes.
Standardized Services	Support of innovation thanks to interoperability of services.	Streamline business processes and no need to invest resources in developing additional interfaces for solution integration.
Availability	Enables easy global expansion, thus helping to reach new markets with new products quicker and easier.	N/A
Accessibility	New product development and deployment on a variety of devices bringing new business opportunities.	Improved employee collaboration which helps to improve processes.

2.2 Information Security Risk Management in The Cloud

The International Organization for Standardization (ISO) has published a number of standards under the ISO/IEC 27000 framework. On *http://iso.org* one can find over 60 publications within the family. ISO/IEC 27001, the latest version was published in 2013, specifies how an organisation should establish, implement and maintain an information security management system. The standard provides a technology agnostic information security management approach without specifying controls. The ISO/IEC 27002 standard is building on ISO/IEC 27001 and gives guidelines around information security controls. It also highlights the three main sources of security requirements for organisations:

- Risk assessments
- Legal, statutory, regulatory and contractual requirements
- Principles, objectives and business requirements for information handling.

In [12] these were summarised as Risk Assessment; Legal and Contractual Requirements and Business and Technical Requirements as illustrated in figure 2.1. The standard also specifies controls for supplier relationships under clause 15

Figure 2.1: Information Security Requirements Sources as per ISO/IEC 27002. [12]

which an organisation can apply to any supplier relationship also cloud services. However, while the controls in ISO/IEC 27002 are applicable to all organisations and all areas of information technology the International Standards Organisation has released the ISO/IEC 27017 *Code of practice for information security controls based on ISO/IEC 27002 for cloud services* in 2015. With ISO/IEC 27017 they suggest that cloud-specific information security threats and risks exist which require additional controls. These are part of this standard and are to be understood as an extension and not a replacement of the ISO/IEC 27002. ISO/IEC 27017 is also providing guidance if a control is applicable to both the cloud service customer

and the cloud service provider. If they are not, the standard provides separate guidance on the respective control, thus helping both sides to improve information security from their perspective.

In [13] Tanimoto et al. used Risk Breakdown Structure (RBS) to compile a list of user perceived risks arising around cloud services. The list includes risks for the service consumer, the service provider as well as others and is illustrated in figure 2.2. Then for each risk they used the risk matrix method to determine one of

Level 1: Major division	Level 2: Middle division	Level 3: Risks
1. Risks for Company Introducing Cloud Computing	1.1 System	1.1.1 Problem of Cooperation with Existing System
		1.1.2 Problem of Removing Data when Finishing Use of Cloud Service
		1.1.3 Problem of Unique Specification of Service Provider
		1.1.4 Problem with Supervisor of Service Provider
		1.1.5 Problem of Service Provider Leaking, Altering, and Wrongly Using Data
		1.1.6 Problem of Data Being Deleted After Cloud Service Use
	1.2 Operation	1.2.1 Problem of Regulatory Non-compliance by Service Provider
		1.2.2 Problem of Service Provider Limiting Information Disclosure
		1.2.3 Problem of Requirements for Authentication
		1.2.4 Problem of Managing Confidential Information
		1.2.5 Bad Influence when Data of Other Company Using the Same Service are Seized
	1.3 Facility	1.3.1 Problem of Environmental Impact, Such as Carbon-dioxide Emissions
2. Risks for Cloud Service Provider	2.1 System	2.1.1 Problem of Difference between Work Important Matter of Use Company and Cloud Service Provider Specification
		2.1.2 Problem of Unrestorable Specifications when Data Disappears
		2.1.3 Problem of Insufficient Access Privilege Management
	2.2 Operation	2.2.1 Problem whether to Fill Service Level Agreement or Not
		2.2.2 Crisis of Continuation of Service Caused by Bankruptcy, Overspending, etc.
		2.2.3 Problem when Business Continuous Plan is Nonexistent or Insufficient
		2.2.4 Problem when Security Management Organization not Fixed
		2.2.5 Problem of Data Leaking or Disappearing due to Operation Mistake
		2.2.6 Problem to Compliance with Internal Control, Security Audit, Etc.
3. Others	3.1 Operation	3.1.1 Restriction by Revision of Law
	3.2 Facility	3.2.1 Disaster Destroying Data Center

Figure 2.2: Identified risks on the security perception by RBS. [13]

four countermeasures: risk transference, risk avoidance, risk acceptance and risk mitigation. Out of the 23 risks they identified 11 were categorised as risk transference, which means that a third party monitors the assigned risk or the service provider should provide a guarantee that the risk is addressed, 5 were classified as risk mitigation focusing on cloud service specifications, 4 as risk acceptance and the remaining 3 as risk avoidance where the users should adjust or by choosing a cloud service provider. They concluded that a cloud service provider should be able to reduce the customers' perceived insecurity with the proposed counter-

measures. In [14] Tanimoto et al. applied a quantitative approach to demonstrate the risk reduction by the countermeasures.

In [12], the authors assessed the information security risks in the cloud with focus on local government authorities in Australia. They split their research into two studies: a qualitative investigation; and a quantitative questionnaire. For the first study, 21 senior local government staff members were interviewed on information security requirements for cloud computing. The data obtained was grouped into seven themes which are listed in table 2.3 along with a summary of the results. Based on the review, the authors of [12] created a concept consisting of four

Table 2.3: Information Security Requirements of Cloud Services [12]

Theme	Summary of interview results
Data Transmission	Seven out of ten agreed that the cloud enables secure data transfer by using advanced encryption techniques.
Trustworthiness	A little over two thirds agreed that trustworthiness is a factor when it comes to cloud services. Especially IT staff of large providers are perceived to be more risk aware and reliable when it comes to security.
Data Storage	77% of the interviewees stated that cloud service providers and their data centres provide better information security for data at rest.
Redundancy	Less than half of the participants think that the data centres of cloud services have effective redundancy. They also stated that it is a critical requirement. Hence, the lack thereof will influence the decision for a cloud service provider.
Backup	Three quarters highlighted that the back-up systems of cloud provider data centres are effective. It is also important to understand how cloud service providers backup and restore data, and if the data is encoded or if this is something the service consumer has to do.
Data Privacy	Almost two thirds of the participants stated that cloud service providers keep an organisation's data private. The situation has improved over the past years as cloud service providers increasingly build local data centres taking out legal hurdles to host private data offshore.
Government Regulation	83% of the interviewees pointed out that government regulations can drive the cloud adoption by refining regulations to make it easier to use cloud services.

key groups in regard to cloud information security requirements as illustrated by figure 2.3. Three of them were based on the information security requirements sources mentioned in ISO/IEC 27002: Risk Assessment, Legal and Contractual

Requirements, and Business and Technical Requirements. The researches have extended it with a fourth dimension which is Data Security. This fourth group includes the information security requirements for transmission, storage and privacy of data. In their review they came to believe that they high volume data exchange as well as the distributed storage systems used by cloud computing both have security implications. Moreover, they also consider data privacy concerns to be a factor because users refrain from uploading data to the cloud due to the sense of loss of control.

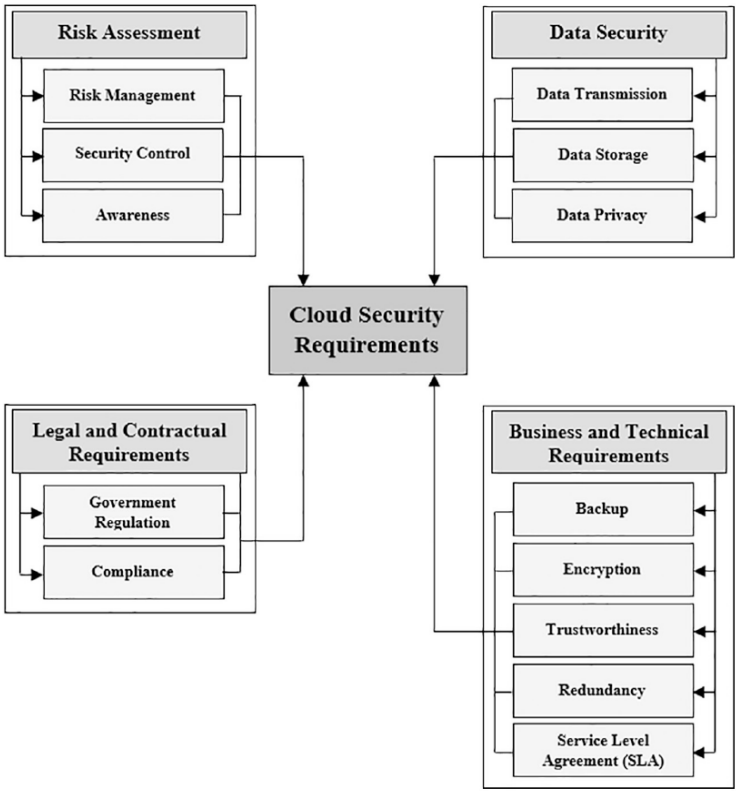


Figure 2.3: Extended cloud information security requirements framework based on ISO/IEC 27002 [12]

In the second part of their study the researchers of [12] used a questionnaire to test and confirm the findings of their exploratory work. The results for each information security requirements group are summarised in table 2.4. The researchers were surprised by their observations about Legal and Contractual Requirements, for both sub-areas the findings were inconsistent with the literature they reviewed. They assumed that this is caused by a lack of awareness and believe that local governments underestimate the importance of state or federal government. The authors concluded that the four components of their conceptual cloud information security framework are significant factors when it comes to determ-

Table 2.4: Results of the quantitative study. [12]

Theme	Summary of interview results
Data Security	For all three sub-areas a significant relationship between them and Cloud Information Security has been observed.
Risk Assessment	Risk Management, Security Control and Awareness were all found to have a significant and positive relationship with Cloud Information Security.
Legal and Contractual Requirements	No significant relationship has been observed between government regulations and Cloud Information Security requirements. The same observation has been made for Compliance.
Business and Technical Requirements	All but Redundancy showed a significant and positive relationship between them and Cloud Information Security.

ine the cloud information security requirements within the Australian regional government context.

Chapter 3

Methodology

In this chapter the methods used to find answers to the research questions are described. Furthermore, there is a statement about non-academic research and how it will be considered for this work.

3.1 Thesis Scope

As mentioned in the introductory chapter this work deep-dives into analysing if and how information security risks are influenced by the chosen service delivery model. Moreover, interfaces between information security subject matter experts and other function areas are highlighted and recommendations are provided towards how information security can support these areas and vice versa. Lastly, this work defines a set of criteria which help information security professionals analyse third-party vendor relationships from their perspective.

3.2 Methodology Introduction

For this thesis multiple qualitative investigation methods were used to find answers to the research questions. The approach was split into two main phases: In a first phase aggregative and interrogative methods were used to increase the understanding of the subject. During the second phase an interrogative method was used to collect empirical knowledge from experts in the field.

3.3 Phase 1

Aggregative methods like literature study were used to gain a general overview about Information Security Management frameworks, Cloud Information Security Risk frameworks, Cloud Benefits and Third-Party Risk Management. An additional objective was to identify potential criteria which can be used as distinguishing factors to determine the impact on information security risks by changing the service delivery model from an on-premises to a public cloud approach. Unstructured

interviews were used to reduce knowledge gaps and get external views on certain subjects.

3.3.1 Consideration of Industry Research

Due to the actuality of the topic, industry research material will be considered for this thesis. This includes reports and whitepapers published by the large consultancies (Deloitte, Ernst & Young (EY), PricewaterhouseCoopers (PWC) and KPMG) or research and advisory corporations like Gartner Inc.

3.3.2 Unstructured Interviews

As an additional source of information to the literature, unstructured interviews were held with industry experts from the field. The interviewees were pseudonymised using an identifier. They are listed in table 3.1 together with their job title, their employer's industry sector as well as the topics they were consulted about.

Table 3.1: List of participants in the unstructured interviews.

ID	Job title	Industry Sector	Topic Discussed
I-U-01	Security Consultant TPRM	Information Technology	Third-Party Risk Management process and IT Vendor Risk Management tools (Security Scorecard & BitSight)
I-U-02	Information Security Officer Governance	Financials	TPRM process, control groups & general cloud information security governance
I-U-03	Senior IT Security Infrastructure manager	Financials	Cloud information security risks
I-U-04	Senior Security Tester	Information Technology	Penetration Testing of Cloud Services

3.4 Phase 2 - In-Depth Interviews

The gained knowledge out of the literature study was further enriched with empirical information gained out of in-depth interviews conducted in a semi-structured style.

3.4.1 Semi-Structured Interviews

Semi-structured interviews were held to get knowledge from key experts on how information security risk management is done in their organisation, how cloud

has influenced the information security risk management process and which key criteria help to decide if there is an information security benefit coming from the move to the cloud. The interviews were all structured in the same way. First there were some questions to determine the experience of the participant, as well as their current job title and employer. The second phase consisted of four open-ended questions to which participants provided in-depth answers. The limited number of questions and their open-ended style allowed to discuss and explore aspects of the participant's answer by asking individual follow-up questions. The questions were to determine the employer's cloud service consumer maturity first and then dive into the information security risk assessment process for third-party engagements, risk evolution caused by the cloud transformation and key criteria to determine the information security benefits of cloud services.

Table 3.2: List of participants in the semi-structured interviews

ID	Job title	Years of IT experience	Years of cloud experience	Industry Sector	Employees
I-I-01	Senior Manager IT Security Infrastructure	36	4	Financials	10,000
I-I-02	Cloud Security Specialist	25	4	Information Technology	100,000
I-I-03	Information Security Officer TPRM	10	7	Financials	10,000
I-I-04	Cyber Security Officer	20	3	Financials	10,000
I-I-05	Chief Information Security Officer	14	2	Information Technology	100
I-I-06	Chief Information Security Officer	25	12	Industrials	10,000

Data Collection & Processing

Prior the interview, interviewees received information about the objective of the thesis, high-level topics covered during the interview and the details how the data of the interviews is documented and processed. A copy of the English version of the information brochure can be found in Appendix A. All interviews were recorded and then transcribed and if required translated to English. The transcript was reviewed for key messages which were summarised and added prior the transcript. The document was then shared with the interviewee for review and approval for usage in the Thesis. Once the confirmation was received the recording was deleted. All available transcripts can be found in the Appendix A. The interviews were held with six TPRM and information security specialists from the industry.

The semi-structured interview participants' identities were pseudonymised by giving them an identifier instead of listing their names. Moreover, the years of experience in IT and with cloud are also listed for each interviewee. Additionally, the sector of the organisation the participant is currently employed has been determined based on the Global Industry Classification Standard [15]. Lastly, an indication of the organisation's number of employees is given in orders of magnitude. The participants are summarised in table 3.2. With the combined knowledge of the participants it was possible to establish what the Information Security Risk Management part of TPRM should cover and identify key criteria which allow a firm to establish the benefits of moving a service to the cloud.

3.5 Methodology per Research Question

Table 3.3: The applied methods per research question.

RQ-ID	Research Question	Method(s)
1	Which elements should a third-party information security risk assessment include?	• Literature study • In-depth interview
2	Which are the differences in terms of information security risks between a cloud based and an on-premises service delivery model?	• Literature study • In-depth interview
3	Does the customer profit in respect to information security risk by moving a service to the cloud?	• Literature study • In-depth interview
4	Which criteria are most relevant as distinguishing factors for an information security risk comparison between the delivery models?	• In-depth interview
5	Into which additional risk mitigation measures should a cloud service customer invest?	• In-depth interview

Chapter 4

Results

4.1 In-Depth Interview Results

As discussed in section 3.4.1 of the Methodology chapter there were key areas which the interviews focused on:

- The maturity of cloud adoption (cloud maturity) of the interviewee's organisation
- Information security risk assessment of third-party services
- Change of risk when services are moved from on-premises to the cloud
- Key criteria which help to determine the information security benefit when a service is moved from on-premises to the cloud

The insights gained through the interviews are summarised in topic-specific subsections including one for any risk mitigating measures which were proposed by the participants.

4.1.1 Cloud Maturity

The participants were asked to rate their organisation's cloud maturity on a scale from 1 to 6: 1 - very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent. The responses varied between 4 and 6 with six participants rating their organisation between 4 and 5. The average of these six ratings is 4.5. One participant rated the employer as having excellent maturity. When asked about the gap to excellent maturity then the three of the five participants with maturity smaller than 6, responded that they need more standardisation and automation of the processes and controls. As participant I-I-04 stated: "*I think we need to standardise our controls further, automate processes and ensure that we live a cloud security culture. We are still in an early stage of the whole cloud topic and still are in the learning curve.*" The remaining participant would like to see more service monitoring capabilities. One interviewee stated that cloud service customers need to have a clear vision about how they want to use cloud. Another responded in a similar way by highlighting that every organisation needs to have dedicated resources to

work on the cloud topic and define a cloud strategy, for example create a cloud working group dedicated for this topic. One participant observed that Financials sector customers have the highest level of scrutiny, whereas other customers only focus on basic compliance. Moreover, two of the participants were asked how the maturity evolved over the past years and both responded that their organisation has gone through a steep learning curve over the last two to three years. Summarising, based on the responses it seems that these organisations have gone through a steep learning process but there is still the need to gather additional experience over the coming years to increase their cloud maturity.

4.1.2 Third-Party Information Security Risk Assessments

The interviewees highlighted the importance of organisations having an understanding the weak points and vulnerabilities of the third-parties they seek to do business with. Ultimately, the risk associated with a third-party engagement should not put an organisation at unreasonable risk, the risk needs to be fully understood and in-line with the organisation's risk appetite. To help compare the risk with the risk appetite, interviewees I-I-01 and I-I-03 suggested that organisations should review possible worst-case (e.g. unintentional data disclosure) scenarios when looking into onboarding a new cloud service. The assessment is done whenever a new service is introduced to the participant's organisations and on a regular basis, for example annually. Some of the participants also stated that an event, e.g. a data breach, caused by or impacting one of their third parties, would trigger an event specific assessment. Throughout the process it is important to monitor the behaviour of the cloud service provider. As participant I-I-03 pointed out, good, transparent collaboration during the assessment is important. This can be an indication that during a crisis, the third party also communicates openly and in a timely manner with their customers. The interviewees named the following sources of information:

- Questionnaires
- Interviews
- Certifications & Reports
- IT Vendor Risk Management (VRM) Tools
- TPRM Service Providers & Cyber Security Assessment Service Providers

Each of these sources can provide insightful information about the level of risk arising from the assessed third-party engagement. Additional details along with comments from the interviewees are described further in the following sections.

Questionnaires

Questionnaires are one of the primary sources of information as per the participants of the interviews. They are used to collect information from both the vendor as well as the customer/business unit, which is requesting to consume the service. Participant I-I-06 explained that they use an initial questionnaire with

their must-have information security requirements to filter out undesired vendors at the very beginning. Similarly, I-I-03 advised that the use of a general TPRM triage questionnaire has also proven to be useful. Follow-up questionnaires will then be added based on the replies to the initial questionnaire itself, as an example, if the engagement includes a cloud service then a cloud security questionnaire needs to be answered as part of the process. Similarly, one participant highlighted that it is of merit to have different questionnaires for the different major cloud service models: SaaS, IaaS & PaaS, each covering model specific aspects. Questionnaires are considered public information as they are being shared with vendors prior to doing business with them. Some organisations even publish them on their website, one example of this is Barclays plc [16].

Interviews

Some interviewees responded that they do interviews as follow-up on the questionnaires. They can be with the third-party or with the customer / business unit and are used to get additional information, clear any potential misunderstanding and discuss findings. Sometimes large cloud service providers let customers do a full audit like I-I-02 described: "*Yes, so what we have done in Germany for example is a pooled audit. Where a lot of financial companies came joined forces to do the audit. Another large financial institution came onsite and audited our data centres. We provided virtual reading rooms to their internal audit, obviously under non-disclosure agreements, where they could look at our reports and processes. They cannot take information away, but they can come and look and scrutinize how we do things and whether there is an acceptable level of risk.*". However, I-I-05 outlined that, while they are able to add a right-to-audit clause into the contract of SME-sized service providers, they struggle to do so with the large cloud service providers. Hence, audits seem to be a privilege reserved for larger/more important customers of the respective cloud service provider.

Certifications & Reports

Another source of information, which was highlighted by the participants, are certifications and reports. I-I-02 advises SME-sized companies to review and trust the certifications and reports done by independent third parties. These provide a good insight on how a cloud service provider operates. The following certifications/reports were named by the participants as a useful source of information to assess a cloud service provider's information technology and information security maturity:

- ISO/IEC 27001 (Information Security Management System) certification
- ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services) certification
- ISO/IEC 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) certification

- System and Organization Controls (SOC)) 1-3 reports
- Penetration Test Reports

The information provided can also influence the size of the questionnaire as I-I-05 explained: "*Certifications impact the size of a questionnaire which we send to a service provider as part of our supplier risk management. If they are ISO 27001 certified, then there will be less questions which they have to answer.*" Thus, increasing the efficiency of the process by avoiding redundancy. Another source of information falling under this category are penetration test reports. Four of the five participants stated that they ask cloud service customers for these. Two of the interviewees would even organise a penetration test of the cloud service in case the cloud service provider is either unable to show a report or the report is not meeting their requirements. Interviewee I-I-04 recommends cloud service customers to treat SaaS services like on-premises hosted internet facing applications. If an organisation's information security policy requires internet facing applications to be penetration tested on a regular basis, the same should be required for SaaS. On the other hand, cloud service providers should consider introducing a bug bounty program, I-I-02 stated that this helps the cloud service provider to increase their information security maturity and it increases the trust shown by customers of the cloud service provider. An organisation with such a program demonstrates a high level of confidence and promotes transparency.

IT Vendor Risk Management (VRM) Tools

Two participants responded that they use an IT VRM tool as an additional source of information about a third party. These tools can provide a comprehensive overview about the information security posture based on publicly available information, e.g. through scanning of IPs or URLs for vulnerabilities. Based on the information collected these tools assign companies an overall rating and then for each category of information an additional rating. These categories are different from vendor to vendor. Examples of categories from two different vendors (BitSight & SecurityScorecard) are: Network Security, Botnet Infections, Application Security, Security Incidents/Breaches, Hacker Chatter, etc. In each category the user can review the findings which can be up to hundreds of results as illustrated in figure 4.1. The ratings can be used to get an initial overview about potential issues or to verify information provided by other sources like I-I-04 highlighted: "*If we see, for example that, the application has many findings in BitSight and the penetration test report is not reflecting this then we would insist to do a pen test with a firm of our choice.*" Another observation about these tools is that they provide a lot of information as illustrated in figure 4.1. These findings require expert knowledge to assess if there is additional risk for the service customer or not. Depending on the number of findings this can be very time consuming and costly.

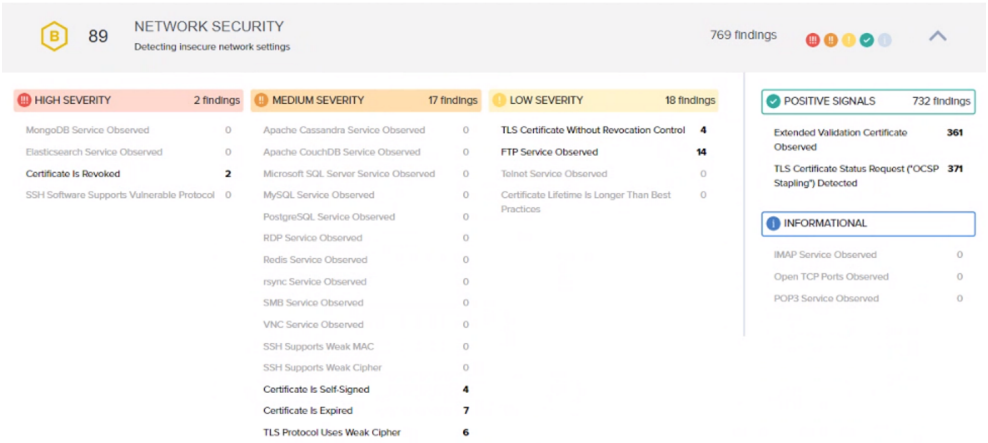


Figure 4.1: Example of findings in Network Security category in the IT VRM Tool SecurityScorecard.

TPRM Service Providers & Cyber Security Assessment Service Providers

The fourth source of information for the information security risk assessment of third parties are service providers which have specialised in third-party risk assessments. Participant I-I-03 explained that there are various service providers, which have specialized in TPRM analysis. An organisation can use the intelligence they collect as input into their TPRM process. Some TPRM service providers cover all aspects of a TPRM. Others specialize in a certain area, e.g. a vendor's cyber security posture. I-I-03 perceived these types of assessments as more valuable compared with IT vendor risk management tools. However, they are also more expensive.

Summary

In this section, the results of the information security risk assessment process for third-party engagements were presented. The interviewees described five sources of information which are used in their risk assessment process. Questionnaires are a tool which is recommended and used by all the interview participants. This low-cost method is used by most in a first phase to get an overview about the third party. In a second phase, some use follow-up questionnaires to deep-dive into identified topics of interest. Another low-cost option to review certain topics in detail are vendor interviews, which can also be used to get an impression of the cloud service provider's employees. Certifications & reports were also mentioned as a good source of information because an external party is reviewing an organisation's processes and procedures against a defined standard. These types of reports are also low cost since they are provided by the cloud service provider to a potential customer for free. A more costly method is to organise a penetration test in case such reports do not exist. IT VRM tools were also mentioned as providing useful information. While they can be used to get an initial feeling about the

information security maturity of an organisation, one needs to deep-dive into the findings of the tool to fully understand the rating and if it presents an actual risk. The license of the tool, the time intensive review of the findings and the requirement to have the skills to understand the findings, make this a more costly source of information. Lastly, there is the option to engage a third party to do a TPRM or a more specific assessment, e.g. cyber security posture. While there is the obvious benefit of getting a report done by a specialised expert, it is also the most expensive source of information. However, depending on the skills of the cloud service customer this might be the only feasible option.

4.1.3 Public Cloud Impact on Information Security Risks

There are key differences between operating a service on-premises and consume it as cloud service and it would be interesting to understand what differences, if any, exist from an information security risk standpoint. The participants were asked about this and based on their replies, the following information security risk areas get a higher than usual focus in the case of a public cloud service engagement:

- Cloud Service Customer Internal Staff
- Data Security & Encryption
- Foreign Governments
- Identity & Access Management
- Customer-Provider Collaboration

The participants described at least one risk for each of these topics. In the following sections these risks are described further.

Cloud Service Customer Internal Staff

The participants raised four risks associated with the internal staff of the cloud service customer (table 4.1). The risk of *loss of control* has been mentioned by four participants. The cloud service provider is providing a managed service which contains aspects a cloud service customer cannot influence. Ultimately, an organisation needs to be clear on how much control they want to give away and also how much control they can give away. One participant raised the *lack of change acceptance* as a risk, I-I-02 highlighting that the IT employees of a cloud service customer can be reluctant to support the journey to the cloud. They might fear that they are no longer needed. Thus it is important that an organisation with a cloud strategy implements strong change management processes which ensure that employees are given a perspective. The importance of it is further underlined by the remaining two risks which relate to an organisation's know-how. It is imperative to build up the required skills set to manage the new technology in the cloud service customer's organisation. The *lack of know-how* can increase the possibility of misconfigured services and potentially unintentional exposure of components or even data. At the same time an organisation also needs to be conscious about how much know-how it needs to retain internally. As I-I-06 stated: "*The third aspect is*

then the know-how. How much know-how do we need to retain to be able to do a new RFI/RFP in the future? How much know-how do we need to take a service back on-premises and operate it ourselves? Do we find the know-how in the market and can we afford it?". The *loss of know-how* caused by the consumption of a managed service can lead to unreasonable dependency on a third party. An organisation needs to have a clear strategy and define what is acceptable to them.

Table 4.1: Risks related to a cloud service customer's internal staff.

Risk	Risk Description	Interviewee
Loss of Control	Consuming a cloud service means letting the cloud service provider manage certain aspects (e.g. infrastructure) of the service without influence of the customer.	I-I-01, I-I-04, I-I-05, I-I-06
Lack of Change Acceptance	Introducing new technology can increase the fear of job loss among internal IT staff. Thus, negatively impact their support of the adoption of cloud services.	I-I-02
Lack of Know-How	Lack of training and missing skills could result in misconfigured cloud services and lead to unintentional data disclosure	I-I-02, I-I-04, I-I-05
Loss of Know-How	Consuming cloud services is ultimately an outsourcing. This can lead to loss of essential know-how and jeopardize the exit strategy.	I-I-06

Data Security & Encryption

Data Security has also been raised as a key risk area. Participants talked primarily about encryption of data at the various stages as well as key management (table 4.2). This area was expected as it was also a key topic in [12] including *Data Transmission*, *Data Storage* and *Data Privacy* topics. This subsection also includes risks and issues which [12] listed under *Business and Technical Requirements*. Five out of six stated that they see a risk that Cloud Service Provider (CSP) have access to customer data in unencrypted form (*CSP decrypted data access*), otherwise the data could not be processed. Cloud providers do react to these concerns, some offer mitigating features like memory data encryption [17]. While this certainly reduces the risk, the data still needs to be decrypted before being processed by the CPU. Consequently, the data is available in unencrypted form to whoever controls the processor. The second (*CSP crypto key access*) and the third (*Weak crypto key generation*) risks were raised in the context of cryptographic key management. Concerns were mostly raised around the scenario where the CSP would fully manage the cryptographic keys. Participants saw the risk that this would give the CSP at least the theoretical possibility to extract and use the keys. Combined with the *Foreign Governments* risk this is perceived to be an even bigger problem. Thus, some regulators did react as participant I-I-04 explained: "*Regulators are dictating to "bring your own key". Meaning that we would generate the key on-premises and*

export it into the HSM of the cloud. In this case we know how the key was generated and that it was not generated using the keygen of the cloud provider. The keys can also be deleted and then the cloud provider cannot use the data either.". Meanwhile all large IaaS providers offer this feature to their customers [18][19][20] and so do some of the SaaS services like Slack [21]. Furthermore, participants recommend to encrypt data on-premises before sending them to the cloud for storage. This makes a customer fully independent of the provider's encryption processes. I-I-02 raised an additional risk around "*Data sovereignty*". Some cloud service customers require data to be available only to an exclusive set of employees, for example when a customer has a globally distributed engineering team they might want to ensure that engineers in country X can see parts of the data and engineers in country Y cannot. Such requirements are mostly driven by laws & regulations, e.g. strict employee data privacy laws like in Germany or banking secrecy laws like in Switzerland. The last risk in this section is related to "*Data portability*". Interviewee I-I-05 perceived this to be a growing risk: "*You also have the issue of data portability. The cloud provider is not interested in enabling you to get your data out of the cloud easily. I think this will become a complex problem once the "cloud first" hype is cooling down and organisations want to move some of the services back on-premises.*" Ultimately, this leads to vendor lock-in. This is indeed a problem which has also been recognised by some cloud service providers, as per I-I-02's statement. Some CSPs try to promote an open model so customers can move workloads between IaaS but to date there are no solutions yet. I-I-06's organisation is mitigating this risk by ensuring that critical services are provided by at least two different providers. While this certainly gives them leverage and flexibility, it is also more costly. Smaller and medium-sized organisations will potentially not be able to afford such a strategy.

Table 4.2: Risks related to Data Security & Encryption.

Risk	Risk Description	Interviewee
CSP decrypted data access	The risk of access to unencrypted data by the cloud service provider.	I-I-01, I-I-02, I-I-03, I-I-04, I-I-05
CSP crypto key access	Cryptographic keys managed by the cloud service provider can also be used by the CSP without knowledge of the customer.	I-I-01, I-I-02, I-I-03, I-I-04 I-I-05
Weak crypto key generation	Vulnerable implementations of cryptographic key generation methods.	I-I-04
Data sovereignty	Risk of unauthorised access to data based on location.	I-I-02
Data portability	Risk of inability to move data stored with a cloud service provider to another cloud service provider or back on-premises and subsequent vendor lock-in	I-I-02, I-I-05, I-I-06

Foreign Governments

Cloud services are distributed globally with point of presences in one to many countries. All major IaaS services operate in multiple countries as figure 4.2 illustrates at the example of Amazon AWS. Depending on the size of a PaaS or a SaaS service they too can have global data locations. If the data is hosted in a country different than the location of an organisation additional laws and regulations can apply. In the context of this additional challenge I-I-04 raised the risk of a "*Foreign Governments*" accessing cloud service customer data by forcing the cloud service provider to hand it over. Although I-I-04's organisation has discussed this scenario with the cloud service provider and included contractual mitigation measures, the participant pointed out that there is still a residual risk. If a government entity compels the cloud service provider to secrecy, then the cloud service customer would not be informed.

Table 4.3: Risks related to Foreign Governments.

Risk	Risk Description	Interviewee
Power of Foreign Governments	A government could force a cloud provider operating under its jurisdiction to hand over data, even in secrecy and without informing the customer.	I-I-04

Figure 4.2: Amazon AWS Global Infrastructure Map showing their current point of presences. [22]

Identity & Access Management

Multiple interview participants also raised identity and access management to be a key topic when services are moved to the cloud. The whole topic is more complex as multiple identities might need to be managed or organisations might choose to use Identity Federation. Cloud service customers also need to consider cloud service provider's access which may be required for maintenance or incident resolution. I-I-05 described the scenario of "*credential theft*" for which the risk is different than for on-premises credentials. As I-I-05 explained: "*When credentials of a person with sufficient rights to deploy infrastructure in the cloud have been stolen, then they could deploy infrastructure, e.g., for crypto mining. This means that you will receive a big bill which can have a substantial impact.*" The interviewee also named potential mitigation measures like two-factor authentication, but they obviously need to be enabled. Another risk, mentioned by several participants, is related to the cloud service provider's administrative access to the customer's instances. Cloud services can provide controls to mitigate some of the risks. The mentioned controls include access approval, access logging, access monitoring including notification services. However, the participants assume that in case of an incident cloud service provider would do anything to restore the service and not wait for authorisation by customers. While the administrative access to a customer's instance is one dimension of the problem, the access to the underlying infrastructure is another, which in most cases is not necessarily under the control of the cloud service customer.

Table 4.4: Risks related to Identity & Access Management.

Risk	Risk Description	Interviewee
Credential Theft	If credentials of an infrastructure administrator are stolen, they could be used to build up hidden infrastructure.	I-I-05
CSP privileged access customer instance	A cloud service provider has privileged access to the cloud service customer's instance and data.	I-I-01, I-I-02, I-I-03, I-I-04, I-I-05
CSP infrastructure privileged access	A cloud service provider has privileged access to the underlying infrastructure which cannot be controlled by the customers.	I-I-01, I-I-02, I-I-03, I-I-04, I-I-05

Customer-Provider Collaboration

It is important to understand what a cloud service customer can expect from a cloud service provider in terms of communication and reporting. Organisations working in heavily regulated sectors like Financials, are required to meet given notification periods for incidents. For example, a financial institution in Singapore needs to inform the Monetary Authority in Singapore about a reportable incident within 60 minutes of the discovery [23]. Thus, two participants raised this as a risk and stressed the importance of clear procedures and a transparent collabor-

ation between the customer and provider. Similarly, five out of six participants, described issues which can be summarised as "*lack of transparency*". To ensure that the cloud service provider operates in a fully compliant environment with all required controls implemented the interviewees recommend auditing the CSP. As I-I-06 "*They do advertise that they have higher information security but when you look into it with an audit – I always add the right to audit to a contract – then we observe that high flexibility comes with reduced information security. It is still on an ok level but not as good as advertised.*" The right to audit is usually added as a contract amendment, which can also include penetration tests. Sometimes cloud service customers want to do a penetration test with an organisation of their choice. For example, to get an independent report in case of discrepancies between a report provided by the cloud service customer and the information security maturity rating in an IT vendor risk management tool. However, I-I-02, I-I-05 and I-I-06 highlighted that it is sometimes difficult to persuade the cloud service provider to accept such clauses. Based on the statements made one can assume that the higher the financial turnover of a cloud service customer the more likely is the acceptance of such a contract amendment by cloud service providers.

Table 4.5: Risks related to Customer-Provider Collaboration.

Risk	Risk Description	Interviewee
Delayed incident communication	If the cloud service provider is not communicating incidents in a timely manner, customers might breach notification periods mandated by regulators.	I-I-02, I-I-03
Lack of transparency	A cloud service provider might not disclose all relevant information, willingly or unwillingly. Issues with processes or lack of controls could go unnoticed and reports could paint a better picture than reality.	I-I-02, I-I-03, I-I-04, I-I-05, I-I-06

Summary

The 15 information security risks raised by the participants of the interview were described in this section. The risks were allocated into one of five categories. On average a risk was raised by 2.87 participants. An important topic appears to be building up new and maintaining existing know-how, thus organisations need to have a clear strategy. Maintaining existing know-how could be underestimated as only one participant highlighted it. Additionally, there were fewer risks raised around data in transit and at rest than expected, the discussions focused more on encryption key management and data portability. Another risk was raised around foreign governments' access to cloud service customer's data. This specific risk was raised by only one participant. Some of the other interviewees discussed more the challenge of having to comply with different laws and regulations like the GDPR in the European Union, however, the topic of Foreign Governments is prominent with larger cloud providers [24][25] and the media [26][27]. Furthermore,

participants are also concerned how CSPs access their customer's instances and the underlying infrastructure. Some CSPs enable their customers to control and monitor any administrative access by the CSP staff. Lastly, cloud service customers need their CSP to be transparent and communicate openly, not only for the sake of internal communication of incidents but also for external communication like regulatory reporting.

4.1.4 Decision Criteria

In the last phase of the interview participants were asked if they can name criteria based on which an organisation can decide whether moving a particular service to the cloud is acceptable or not. A lot of the points raised tie back to an organisation's IT operation and information security maturity (hereafter: IT Maturity). Hence this is perceived to be a key measure to determine if there is actual benefit coming from the move to a cloud based service delivery model. I-I-02, I-I-04 and I-I-06 stated that an organisation can profit from the information security control suite which mature cloud service providers offer out of the box. When asked, the interviewees suggested company size as a simple indicator of maturity. A large cloud service provider with orders of magnitude more employees and financial resources is assumed to be more mature than a small SaaS provider. I-I-04 described the issue as follows: "*When it comes to SaaS however, you have sometimes a vendor putting functionality over security. They want to provide a good product with many features and then invest less into security. From my perspective, there comes bigger risk from smaller SaaS vendors.*" Additionally, to an organisation's number of employees I-I-02 raised the presence of a bug bounty program also as an indicator. Organisations with a bug bounty program are likely to be more mature than organisations without.

Another criterion mentioned by the participants are laws and regulations. Storing or processing data with a third party and/or in another country can be prohibited. Furthermore, an organisation remains accountable for any incidents under certain regulations like the GDPR. For illustration purposes there have been 18 rulings under the GDPR Art. 24 (see section 1.1.1) with fines ranging from €387 up to €8'1510'000 [28].

In addition to laws and regulations complexity has also been named as a criterion. A cloud service on its own might be low complexity but as soon as it has to be integrated in a complex enterprise IT ecosystem the effort required can outweigh the benefits. I-I-06 explained: "*If there are so many interfaces required or accesses across different locations then we review it from an architectural perspective to ensure it makes sense. If the handling of all the interfaces is more complex than running the service in our data centers then we decide not to consume the cloud service.*"

The last criterion is about the criticality of the data or the application. If the data or the application in question are critical for an organisation then they should think twice about moving it to the cloud. To illustrate, the organisation of I-I-05

strictly advises their customers to keep their "golden eggs" on-premises. Another participant explained that all their applications are rated based on their information security requirements, i.e. confidentiality, integrity and availability, and furthermore a business impact assessment is also performed. Together these metrics are defining the overall criticality of the application. The criticality then dictates the architecture type to be used which can exclude cloud services as an option.

Summarising, the participants have stated that they use at least one of the following decision criteria to determine whether the move of an application or data to the cloud is possible: IT Maturity, Laws & Regulations, Complexity, Data & Application Criticality. All of them but complexity can initially be assessed to get an indication if it is worth to continue with the project or if there is too much risk coming from changing the service delivery architecture. The true complexity of a service is likely to only become visible at a later stage of the onboarding process, e.g. during a proof of concept. Thus, complexity could be a good criterion but potentially only at a later stage of the process.

4.1.5 Cloud Information Security Risk Mitigation Measures

During the interview, the participants also described various risk mitigation measures which their organisation implements to reduce risk. The suggested mitigation measures for each the risks described in section 4.1.3 can be found in table 4.6. Participants suggested that organisations implement redundancies and backups outside of the cloud as part of their Disaster Recovery concept. Should a service provider accidentally delete data like it happened to the customers of the largest telecommunication and Internet service provider in Switzerland [29], declare bankruptcy and take the systems offline or delete a customer's data on purpose, e.g. due to unpaid bills, then an organisation would at least have a copy of their data. Participants also raised the increasing dependency on their internet links and stated that they ensure that their connection to the Internet is high availability by implementing redundancy. Depending on the criticality of the service organisations sometimes choose to implement dedicated physical network connections to their cloud providers. Considering malware injection, intrusion by an attacker and data leakage organisations try to implement network-based controls to steer and analyse the traffic exchanged between the customer and the CSP to mitigate the aforementioned risks. Data encryption is used by all interviewees to mitigate any data access related risks and they have developed different approaches to it. Some always prefer the option to "Bring-your-own-key" which has the advantage that neither the CSP nor a Foreign Government can read the data. If such an option is not available the data would be encrypted on-premises or only be sent in an anonymous or tokenised form to the cloud service, which has the downside that some of the features might not work anymore. I-I-06 stated that for them it is a case-by-case decision: "*Which also requires additional audits to ensure the provider is managing the access to the key correctly. We want to see who has access to it, who accessed it in the past, who used it and when was it used, etc. This*

is then reviewed on a regular basis and is a different mechanism compared to when we have our own PKI and deliver the key. If something is going wrong things might get difficult. It also means that our teams need to be ready 24/7 to provide the key. So, for us it is a case-by-case decision which way we go. Applications with a high criticality are not allowed to go to the cloud anyway." Some participants would also like to monitor the vendor's access, but they highlighted that the customer depends on the provider implementing the required monitoring, logging and audit features. One participant stated that in the absence of such controls they would at least like to see a SOC report describing how the cloud service provider operates, however in the end there will always be some residual risk, hence the customer must trust the CSP. Not only the SOC certification was perceived as addressing some of the risks but any evidence of certification is considered proof of a level of maturity. Another raised risk was credential theft for which the participant said that they always try to enable two-factor authentication to mitigate the risk. Furthermore, an organisation has to ensure that their staff have an adequate level of know-how before moving a service to the cloud. I-I-06 also suggested to use multiple providers for the same service, by doing so the customer gains flexibility and leverage in case of issues or negotiations. Should the customer not be in a position to mitigate risks on its own then the interviewees proposed to discuss these with the cloud service provider and see how they could potentially help reducing risk, e.g. by implementing additional features. CSPs are keen to support in case of such enquiries, because they have an interest in improving their services as I-I-02 highlighted, on one hand to win the potential customer and on the other to get an advantage over competitors which then again might attract additional customers. If the CSP is not able to reduce any open risks, then it has also been suggested to reduce the scope of the engagement and only consume certain parts of a service. For any remaining risks which cannot be addressed technically, cloud service customers try to mitigate them contractually, which cloud service providers might not always allow depending on the size of the customer. In the end, all participants stated that there is always residual risk which requires trusting the provider and their abilities.

4.1.6 Summary

In this section 4.1 the results of the interviews were presented. The participants shared valuable information about their experience from the field. While they are still hesitant to move certain services to the cloud they all believe that cloud service providers take the concerns of their customer seriously. CSPs implement risk mitigating features and build expand their points of presence to other countries to overcome legal hurdles. In the end it seems that organisations are going into the right direction but still need to gain additional experience and become more mature.

Table 4.6: Risks described in section 4.1.3 including their proposed mitigation measures.

Risk	Proposed Mitigation Measures
Delayed incident communication	Contract Amendment
Lack of transparency	External Reports (e.g. Penetration Test)
Power of Foreign Governments	Contract Amendment
Credential Theft	Two-Factor Authentication, Role-Based Access Control
CSP privileged access customer instance	Contract Amendment, Access Monitoring Features
CSP infrastructure privileged access	Risk Acceptance
Loss of Control	Risk Acceptance
Lack of Change Acceptance	IT Strategy, Cloud Solution Trainings
Lack of Know-How	Cloud Solution Trainings
Loss of Know-How	Retention of know-how
CSP decrypted data access	Encrypt Data On-Premises, Anonymise Data, Bring-Your-Own-Key
CSP crypto key access	Bring-Your-Own-Key
Weak crypto key generation	Bring-Your-Own-Key
Data Sovereignty	Cloud Service Provider Feature
Data Portability	Cloud Service Provider Feature, Data Backup

4.2 Criteria Analysis

Through the qualitative information collected with the interviews, four criteria were raised by the participants. Those can potentially serve as distinguishing factors whether a service should be moved to the cloud or not. In this section each criterion will be described further and analysed for its plausibility and feasibility. To assess if a criterion is feasible for an organisation, they need to understand the financial effort required to get the data (Cost), the availability of the data (Availability), the effort required to review the data (Effort) and the required level of expertise to understand it (Know-How). In some cases, a criterion might be more feasible for larger organisations than for SaaS-sized organisations, e.g. if one is too expensive to obtain, if the data is only shared with high-volume customers, if it is too much effort to review the data, or too complicated to understand the data. The assessment result is rated as Low, Medium, or High and the threshold for each rating is described in table 4.7.

Table 4.7: Description of ratings for each of the feasibility assessment criteria.

Criterion	Low	Medium	High
Cost	<200 USD	200 USD < cost > 2,000 USD	>2,000 USD
Availability	Data is hard to collect or only available to an exclusive group	Data is only available upon request	Information can be found through internet search or obtained from a third party in an easy way
Effort	It takes less than 1 hour to analyse and assess the data	It takes several hours but no longer than a day to analyse and assess the data	It takes multiple days to analyse and assess the data
Know-How	No knowledge about the subject matter is required to derive the right conclusions.	Requires basic subject matter know-how to derive the right conclusions.	Requires expert subject matter know-how to derive the right conclusions.

4.2.1 IT Maturity

During the interviews multiple indicators were named which are related to the IT Maturity of an organisation, thus the first criterion is IT Maturity. The indicators, which organisations use to assess the maturity of a cloud service provider are: Certifications, Employees, IT VRM Tool Rating and Reports. In addition, one indicator was named which helps an organisation to assess if they are ready to consume a cloud service or not: Internal Cloud Know-How. Both the IT Maturity as criterion as well as the proposed indicators will be analysed for plausibility and feasibility.

Plausibility

In [30] maturity was defined as a set of characteristics, attributes, indicators, or patterns that represent progression and achievement in a particular domain or discipline. Thus, if organisation A is more mature in information security than organisation B, then organisation B could gain an information security benefit from consuming a service provided by organisation A, concluding that this is a plausible criterion. The indicators are analysed in table 4.8.

Table 4.8: Plausibility assessment of the proposed IT Maturity indicators.

Indicator	Plausibility Assessment	Conclusion
Certifications	The purpose of a certificate is to provide written confirmation by an independent organisation that something or someone meets a set of requirements [31]. Thus, an organisation which has been certified against a standard can be more mature than another in the area of certification. For example, if an organisation is certified against a standard out of the ISO 27k family, they are likely to have better information security maturity than an organisation which is not [32].	Plausible
Employees	An organisation's size can give an indication about the size of its the IT and the number of IT security professionals an organisation employs. A large organisation has more resources which can implement and maintain security controls and are also likely to benefit from economies of scale. Thus, they are likely to be more mature in information security than a small organisation. However, it is also important to consider the industry an organisation operates in. I-I-02 stated that large organisations working in the Financials sector are more mature than large organisations in the industrials sector. This could be because of the heavily regulated environment as well as because of the potentially higher ratio of IT employees to total employees. From experience, a bank's IT employee ratio is much larger than that of an Heavy Electrical Equipment.	Plausible
IT VRM Tool Rating	IT VRM tools assess IT vendors' information security posture. These tools include technical as well as soft factors for which the information is available mostly publicly. A view examples: Verification if DKIM records are present; Type of TLS/SSL certificates (self-signed or not) used and their status (active, revoked or expired); TLS/SSL configuration of web servers to rule out that weak cipher suites can be used; Open network ports; Verification if DNSSEC is configured; Were any credentials exposed publicly?; Is there any chatter about the organisation in hacker forums? Any findings which are an indication of bad security decrease an organisation's rating. Thus, a low rating indicates poor information security maturity.	Plausible
Reports	Reports written by an external organisation, e.g. a penetration test report, can provide valuable insights when assessing an organisation's information security maturity. The number of and the type of findings give an indication about the maturity of an organisation's people, processes and products. If multiple reports from different points in time then this could also give an indication about the evolution of the organisation's maturity.	Plausible
Internal Cloud Know-How	If a customer's IT personnel lacks know-how then moving a service to the cloud could be prone to misconfiguration. Almost all attacks on cloud services were possible because of customer misconfiguration like publicly exposed databases or over-privileged accounts [33]. Misconfigured services remain a big problem with a high risk of catastrophic data breaches [34][35]. Ensuring that employees have an adequate level of know-how reduces mistakes [36]. Thus, an organisation with employees which have not been trained on cloud services, is more likely to suffer from falsely configured cloud services. Therefore, they are putting themselves at risk and should consider to run a service on-premises instead.	Plausible

Feasibility

Organisations struggle with assessing maturity as it requires expert knowledge to do so [32]. Moreover, they are better at assessing their own organisation than at assessing a foreign organisation [37]. So, it seems that the simpler the criterion is the better for the assessment. Thus, to assess the feasibility of the IT Maturity criterion one needs to assess the feasibility of the suggested indicators.

An organisation's *Certifications* are usually displayed on an organisation's website for everyone to see, e.g. [38][39] [40]. As previously established, it is a plausible indicator for maturity, hence organisations are keen to show their certified abilities to existing and potential customers and for sure they will gladly share it upon request. Hence, in case certificates exist their availability is expected to be High. Since they are treated as public information the information is free of charge. The effort potentially lies with reviewing the certificate or in case of suspicion verify it with the issuer. Thus, cost and effort are rated as Low. One needs to understand the scope of certificates to decide on their relevancy. However, for an initial assessment a company with certification can be considered more mature than one without. Consequently, the required know-how for this indicator is Low when looking at as a tick in the box exercise. Of course, when going deeper and reviewing the actual audit reports it is beneficial to be more knowledgeable on the corresponding topic.

An organisation's number of *Employees* or an indication thereof, can often be found in the Internet, e.g., on the organisation's website, on Wikipedia, etc. Thus, the data required is also Low cost with High availability. The effort to compare the number of employees between two organisations is Low. One potentially needs to understand that IT departments do not grow linear with the number of employees of an organisation. The ratio depends a lot on the IT needs of an organisation hence it varies heavily [41]. For example, a large manufacturing organisation with 10,000 employees will have much fewer IT employees than a large cloud service provider with 4,000 employees. Consequently, the manufacturing organisation will probably have lower maturity than the cloud service provider. On the other hand, one does not need to be an expert to conclude that a medium-sized organisation can benefit from a large cloud service provider. Concluding that know-how varies between Low and Medium depending on the size of the organisation their industry influences the indication and prevents plain comparison of the numbers.

IT Vendor Risk Management Tools provide a paid service hence are more costly than the previously assessed indicators. While many vendors do not publish prices the basic costs are a few thousand USD and can quickly grow to a few ten thousand USD or more [42]. Although, this might be affordable for a large organisation it seems very expensive for an SME. Which is why the costs are rated as Medium to High. There are a number of vendors on the market but since it is a paid service the data is only available to paying customers. Thus, the availability of the data is rated as Low. Effort-wise it can be low if one only looks at the ratings. However, to not only get a feeling but a good understanding an organisation needs

to review in detail which findings led to the rating. There can easily be several hundreds and up to thousands of findings. Grouping reduces the efforts but it is still perceived to be Medium to High effort. As an initial assessment it might be fine to only compare ratings but to get real value out of it one needs to dig deeper. Hence the effort associated with this indicator is estimated to be Medium to High. Regarding required Know-How to understand the data comparing two numbers is easy. However, as mentioned to get value out of it the data needs to be thoroughly analysed which requires expert knowledge about technology and security controls in order to interpret the findings correctly, thus, know-how is rated as High.

Reports of certifications can be found on some organisation's websites [43] but, certification reports are rather rarely made available publicly.. More delicate reports like the outcome of a penetration test are only available upon request. Thus, the availability is considered to be Medium. Cloud service providers bear the cost for the creation of such reports. Although, some participants in the interview also highlighted that if no penetration test report exists they would organise one and pay for it on their own. In one of the unstructured interviews the cost of a professional penetration test of a SaaS was stated to be between USD 8,800 and USD 26,500. The price is mostly driven by scope and complexity of the application. One can also find cheaper engagements for half the price with reduced scope [44] [45]. Concluding, that existing reports are Low cost and if reports need to be created, they are High cost. The effort to review the report ranges from Low to Medium and is depending on how detailed the review is conducted and the size of the report. As these are specialist reports the reader generally requires expert knowledge to understand and interpret the details. They usually contain a Management Summary, but these often also require a certain level of subject matter specific know-how. Thus, the required Know-How for this indicator is estimated to be Medium to High.

Internal Cloud Know-How is Low cost as it is an internal information. It is always available (High) as an organisation has access to its own resources. The associated effort is also Low. An organisation without any cloud services also has no know-how. More experienced organisations might want to do a more sophisticated self-assessment on a regular basis. While this is likely to be medium to high effort once completed the data can be easily obtained once a new cloud service is assessed. Thus, being low effort. There is not a lot of know-how required to understand the assessment result, hence this is also low. Depending on the internal know-how an organisation might choose to contract a third party to assist with the onboarding and operation of a cloud service. The results of the assessment are summarised in table 4.9.

Table 4.9: Feasibility assessment of the proposed IT Maturity indicators.

Indicator	Cost	Availability	Effort	Know-How	Conclusion
Certifications	Low	High	Low	Low	Feasible
Employees	Low	High	Low	Low-Medium	Feasible
IT VRM Tool Rating	Medium-High	Low	Medium-High	High	Feasible for large organisations
Reports	Low-High	Medium	Low-Medium	Medium-High	Feasible for organisations with IT security know-how
Internal Cloud Know-How	Low	High	Low	Low	Feasible

4.2.2 Laws & Regulations

Legal constraints were named as a criterion whether something can be moved to the cloud or not. Its plausibility and feasibility will be assessed further in this section

Plausibility

Laws can dictate that some data needs to stay with an organisation or within a geographical area. The banking secrecy law in Switzerland [46] is still considered a show-stopper to move any client identifying data out of the country. Even though it is possible under certain circumstances as described in [47] the majority of banks are still reluctant to move such data to cloud services without presence in Switzerland. Another example is the public archives act of Norway, storing data outside of Norway would be in violation of it [48]. Thus, data archives based on public cloud services are currently not a feasible option. Lastly, because of the threat of hefty fines by some regulations, e.g. GDPR [28], organisations might be hesitant to move services to the cloud. In this scenario the criterion would not be a hard but a soft showstopper. So, there are laws which dictate how and with whom data can be shared be it because of privacy or other reasons. Furthermore, laws and regulations exist which define the cloud service customer as accountable for the data, even though the cloud service provider is accountable, e.g. GDPR. Considering all of the above the criterion is deemed to be plausible.

Feasibility

Laws & Regulations are an instrument of the public. Thus, most of the time, they are available (High) over the internet in a digitised form and can usually be obtained at no cost (Low). Reading, understanding and interpreting laws is difficult

as the legal language has its own specialities [49]. Additionally, they can be complex and contain many articles which require multiple hours of reading. There might be articles explaining them in a simplified way like in [50] but these are most likely not including all the details of the law itself. Furthermore, for a large organisation which is operating in multiple countries the effort is much higher because they need to understand the applicable laws of the countries they operate in. Once the laws and regulations are understood the assessment effort is reduced. However, especially SME companies might struggle with getting to this point. Larger organisation with big legal departments have it easier. Moreover, one requires a basic understanding of the subject as well as the law to read and understand laws and regulations. Consequently, know-how is also rated as Medium. Concluding, that this is a feasible criterion for most organisations.

Table 4.10: Feasibility assessment of the proposed Laws & Regulations criterion.

Criterion	Cost	Availability	Effort	Know-How	Conclusion
Laws & Regulations	Low	High	Medium	Medium	Feasible for most organisations

4.2.3 Complexity

Integrating any new service, running on-premises or in the cloud, into an organisation's IT ecosystem can be very complex. If a lot of interfaces are required the service architecture could become too complicated. Limiting the features consumed or running the application on-premises could reduce complexity.

Plausibility

Onboarding a new cloud service to an organisation means that one needs to have an authentication concept. On-premises this means integrating it for example with the Active Directory directly or via a RADIUS. If the application is used to process existing data, e.g. get data from a data lake, then interfaces for data transfer are required. Once the data is processed the application might need to send it back or to a different system, or trigger a process in another application. In case one of these is a cloud service the communication is not internal and crossing the internet. Subsequently it needs to be managed and secured, potentially requiring additional know-how, systems or devices, e.g. an API Gateway [51]. Or it requires another third party in the process, e.g. an identiy provider to help with SAML authentication. In short, increasing the overall complexity and subsequently the cost [52]. An organisation might not be willing to bear this additional cost or not be able to handle the additional complexity. In an extreme example the introduced complexity could even break a system or a process. For example, if additional latency is introduced, by the time the traffic has been sent over the internet to a

cloud service, gets processed and then sent back on-premises, the data might no longer be of value [53], concluding that this criterion is plausible indeed.

Feasibility

Understanding the complexity of something is low cost, as an organisation can use internal resources to do so. There is a dependency on information of the cloud service provider. For example, authentication mechanisms, API, processing, example architectures, etc. This is required to understand how the service needs to be integrated. Such information is not always available online but requires engaging the cloud service provider. Thus, the availability is rated as Medium. The effort to gather all the data required to be able to assess the complexity is estimated to be High. It requires creation of a service architecture overview including the wider IT architecture. The level of know-how needed to assess the data is also considered High, as only experts understand the technical dependencies in detail.

Table 4.11: Feasibility assessment of the proposed Complexity criterion.

Criterion	Cost	Availability	Effort	Know-How	Conclusion
Complexity	Low	Medium	High	High	Feasible for most organisations

4.2.4 Data & Application Criticality

Organisation might choose to keep data on-premises because they do not want to entrust third parties with running core business applications or store critical data. To be able to use this criterion an organisation needs to assess their data and their applications in terms of their criticality. Organisations might consider different data for their criticality assessment. Many use confidentiality, availability and integrity, the three information security principals. Furthermore, the organisation's cloud strategy should define the criteria for applications and data which can be moved to the cloud. Obviously, this should consider an organisation's risk appetite. In the end, comparing the use case against the cloud strategy should immediately indicate which IT architecture types are an option. If the requirements are not met then organisations might not want to move a service to the cloud.

Plausibility

Many organisations rely on critical data or applications in order to do business. A few selected examples include:

- Hospital's storing medical records
- Bank's client data
- Manufacturer's product research data
- Nuclear power plant control system

- Low-latency trading system
- Specialised manufacturing control system

An organisation can refrain from outsourcing such services or data to a third party's systems, because any issue has massive business impact. An example, if a data breach leads to publishing account balances, client names or transactions then this could ruin a bank's reputation. Consequently, customers loose their trust and regulators could fine the institute or even worse, revoke their banking license. Even if the bank would have a contractual right to a penalty of one Billion USD such an event is still likely to drive them out of business. Another example, a critical industrial control system controller which is steering a production line is hosted in the cloud. In the same moment as when a change should have been implemented on the controller, the organisation's internet accesses are flooded by a two hour DDoS attack. Consequently, the production line needs to be stopped resulting in massive financial losses. There are many more examples of critical services or data which in case of an issue can have a catastrophic business impact or even put a whole organisation at risk, thus they want to keep them on-premises which automatically mitigates some of the cloud-specific risks, thus, the criterion is plausible.

Feasibility

The key for this criterion is that all applications are assessed for their criticality regarding the business process and the data they store or process. This is a major effort. Furthermore, an organisation needs to have a cloud strategy defining which types of applications can be moved to the cloud. Once both tasks have been completed the review of a use case should be trivial. The cost is depending on the number of applications because an organisation might need to buy or develop a management system, thus, the cost is ranging from Low to High. The availability of the data is High, as an organisation has all the data it needs for the assessment. This criterion is considered to be Medium effort because of the high initial work required to set it up. Assessing a particular use case can be done within hours. An employee needs to be able to understand the cloud strategy in order to assess the available architecture options. This requires some technical knowledge but most likely not expert level, thus, Know-How is rated as Low.

Table 4.12: Feasibility assessment of the proposed Data & Application Criticality criterion.

Criterion	Cost	Availability	Effort	Know-How	Conclusion
Data & Application Criticality	Low-High	Medium	High	Low	Feasible

4.2.5 Summary

In this section the criteria named by the interview participants were further analysed and deemed both plausible and feasible. All of them can help an organisation assessing if there is benefit coming from the move to the cloud or if it is a high risk undertaking.

Chapter 5

Discussion of Results

In this chapter the answers to the research questions are summarised and the research process is reflected upon.

5.1 Discussion of Research Question 1

Research Question 1 was asking about the elements included in a third-party information security risk assessment. The participants named five sources of information:

- Questionnaires
- Interviews
- Certifications & Reports
- IT Vendor Risk Management Tools (IT VRM Tools)
- TPRM Service Providers & Cyber Security Assessment Service Providers

The process is illustrated in figure 5.1 and combines the aspects raised by the participants. The interviews revealed that the assessment always starts with a triage questionnaire ①. The answers are used to determine which additional information needs to be requested and to filter out unsuitable third parties in an early stage of the process. In this phase the TPRM Team would also send questionnaires to the requester of the service and conduct interviews to establish a common understanding of the scope and objectives. At this stage the TPRM team also reviews the vendor's rating in an IT VRM tool, assuming the TPRM team has access to such a tool. In the next phase ② the TPRM Team would send follow-up questionnaires to the third party with the objective to obtain additional information on topics not covered in the triage questionnaire or to clarify some of the answers to the triage questionnaire. To increase the efficiency of the follow-up questionnaires some organisations remove sections based on certifications the third-party might have, e.g. if the vendor is ISO/IEC 27001 certified then questions regarding the third party's Information Security Management System (ISMS) would be reduced or even removed. Additionally, the TPRM team might also organise interviews to dive into any topics of their choice, e.g. discuss IT VRM Tool findings.

As part of the next phase ③ a third party would share any relevant reports, e.g. audit or penetration test reports. The TPRM team would review these and if required follow-up with additional questionnaires or schedule more interviews. ④ This process or any part of it can also be outsourced to a TPRM service provider. Similarly, organisations sometimes also engage a specialised third party to assess a particular aspect of a third party, e.g. a Cyber Security Assessment Provider to provide a report on a potential third party's cyber security posture. Once the process is completed any identified risks will be assessed and discussed with the business to agree on mitigation measures and where required accept risks or reject the third party as an option. Concluding, this iterative process needs to be very dynamic to be able to react to any findings. Slightly surprising was to hear that some large organisations use external providers and rather buy a third party cyber assessment than using their very capable internal resources to conduct it. Overall an organisation's resources dictate which sources of information are used, as smaller organisations use less than larger organisations.

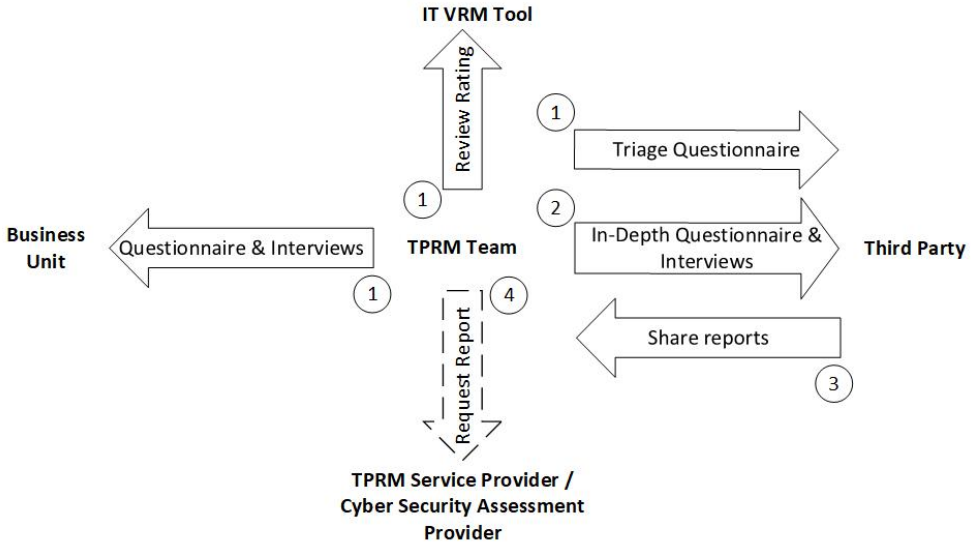


Figure 5.1: TPRM process specific elements and assessment steps.

5.2 Discussion of Research Question 2

The second research question focused on the differences in terms of information security risks between a cloud based and an on-premises service delivery model. A total of 15 risks were raised which were categorised in five information security risk areas as illustrated in figure 5.2. Based on reviewed literature like [12] [54] and from my professional experience it was no surprise to see the discussion focusing on data security at some point. When organisations are moving services to the cloud they want to ensure that only they are able to access clear-text information.

Organisations are conscious that in some cases there is a theoretical possibility that a cloud service provider has access to information which is not encrypted but this is accepted for the applications and data which are moved to the cloud. Furthermore, organisations are concerned about vendor lock-in because exporting data out of a cloud service and moving it to another or back on-premises is very difficult or even impossible, thus mature organisations are expecting this to become a bigger issue in the future. While the risk of a foreign government accessing the data of an organisations through a cloud service provider was raised by only one participant, it is definitely something which all organisations should discuss and form a risk opinion on. This risk definitely applies to data stored in a foreign country there are however legal frameworks which can also make this a concern if an organisation is using a cloud service in a country provided by a foreign organisation, e.g. the U.S. Cloud Act [55]. Another area of risk with increased focus in cloud engagement is the internal staff and their readiness for the cloud journey. The loss of control is a risk which has already been highlighted in the early stages of cloud [56] and continuous to be a key topic. It was very interesting to hear that the skills set lost by adopting cloud services is also perceived as a risk although many organisations seem not to have this on their radar yet. However, this is not surprising as most organisations seem to be still struggling to get the required skills set for securely configuring and operating a cloud service. Depending on an organisations current position on the cloud journey one of the aforementioned risks is more relevant than the other. The risks raised around Identity & Access management were also expected. Although it is astonishing that credential theft was only mentioned by one participant, despite it definitely bringing additional challenges in a cloud service delivery model. IT has also been stressed that the collaboration with the cloud service provider is very important. An organisation might not only depend on it for the sake of the reputation of its IT departement, e.g. incident communication and resolution times, but in heavily regulated environments a good communication between the parties helps to avoid fines [23]. In conclusion, all the raised risks are relevant when moving to the cloud but it seems that while the majority of the risks are perceived similarly amongst organisations, the focus for some risk areas areas is depending on their cloud maturity.

5.3 Discussion of Research Question 3

Research Question 3 was raised to investigate if the customer profits in respect to information security risk by moving a service to the cloud. Related work already investigated this on a macro level and determined that large organisations can gain operational benefit whereas SMEs gain strategic benefits [3]. Participants have established that consuming cloud services can increase an organisation's information security maturity, regardless of their size. However, while SME organisations are perceived to benefit from technology which they cannot afford or lack the know-how to operate themselves, large organisations profit from the cloud security baseline, thus, this observation is in-line with the findings of [3].

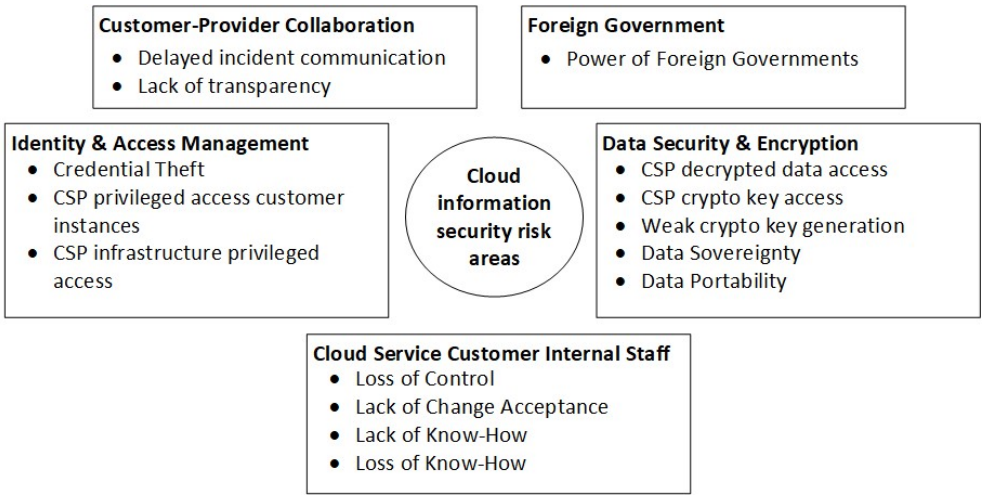


Figure 5.2: Cloud Information Security Risks with increased focus.

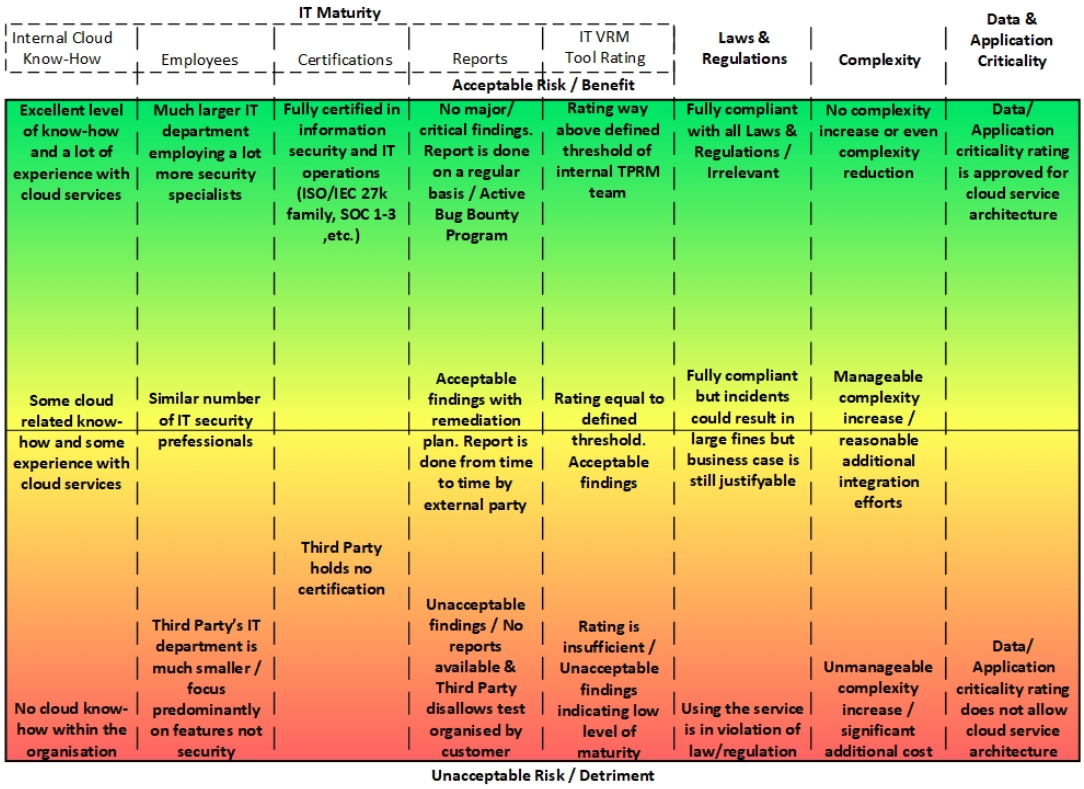
5.4 Discussion of Research Question 4

The objective of research question 4 was to identify relevant criteria which are used as distinguishing factors for an information security risk comparison between the delivery models. Four criteria were mentioned as being used to determine if a potential cloud service can be used or if the service should be run on-premises: IT Maturity, Laws & Regulations, Complexity, Data & Application Criticality. Participants named five indicators as data input for the assessment of the IT Maturity criterion: Certifications, Employees, IT VRM Tool Rating, Reports, Internal Cloud Know-How. Both the suggested criteria and the IT Maturity indicators were reviewed and deemed both plausible and feasible. However, while one criterion might be able to lead to a rejection of a third party or a cloud-based service delivery model it should never be only one criterion which approves the same. Organisations should define thresholds for each criteria, in-line with their risk appetite, based on which a service or a third party can be assessed, as illustrated in Figure 5.3. When applied, organisations might want to implement a score-based system to ensure multiple medium risks are also flagged as unacceptable if they breach a pre-defined threshold and moreover to ensure that any risk mitigation measures positively influence the risk rating.

5.5 Discussion of Research Question 5

The fifth research question investigated into which additional risk mitigation measures a cloud service customer should invest in. Numerous measures were raised to address the different cloud-specific information security risks by the participants. However, the feasibility depends on an organisation's resources and some cannot be implemented by SMEs, for example the larger a cloud service provider and the

Figure 5.3: Proposal of Decision Criteria assessment chart including an indication of possible thresholds.



smaller a customer the less likely it is that the CSP will allow contract amendments. Another mitigation measure proposes that organisations engage two providers for the same service. Although this definitely helps to mitigate the risk of vendor lock-in and moreover provides the organisation with some leverage for negotiations it is considered to be expensive, especially for SMEs. In regard to data security and encryption multiple risk mitigation strategies were explained including their advantages and disadvantages, it seems like organisations have made up their minds early in the cloud adoption process, as to what is acceptable and what is not. Furthermore, cloud service customers have recognised that it is of paramount importance to ensure the professional development of their IT staff in order to reduce the risk of security incidents. Lastly, a cloud service customer cannot test all security controls. I have experienced a case where a large cloud security infrastructure provider had a feature which allowed customers to control the CSP's administrative access to their instance. At some point our organisation was informed that the respective feature had a built-in option which allowed the CSP's staff to circumvent the configuration to gain access to the instance anyway. It has been interesting to hear that participants feel that at some point an organisation simply needs to accept the residual risk. Thus, organisations need to have a

clear strategy about which application and which data can be moved to the cloud and which cannot.

5.6 Discussion of Research Process & Future Work

The results of this thesis meet the set objectives at the beginning. The literature review and the unstructured interviews with various experts in the field provided a good knowledge base. Subsequently, this was very useful in preparation of the interviews and supported the semi-structured approach by enabling me to ask tailored follow-up questions and where required facilitate a discussion on a topic. The participants of the semi-structured interview were a good mix of maturity levels, industries and organisation sizes which ensured that multiple points of view were captured in this work. While the key messages of the participants were aligned in many aspects, their diverse backgrounds allowed to explore different nuances of the risks, e.g. driven by the size of an organisation or by their level of maturity. Therefore, it was possible to identify relevant risks, criteria and mitigation measures which can help organisations to focus on the most relevant aspects when onboarding a new cloud service. In terms of future work, it would be interesting to get additional interviews to build and expand on the observations made as part of this work. In addition, a quantitative verification of the collected data by means of a survey could help to further underline the findings of this work. Lastly, a quantitative assessment of the elicit criteria would be useful to better understand how they hold up as an instrument in the real world.

Chapter 6

Conclusion

This work aimed at investigating the potential differences in TPRM and ISRM processes when organisations are assessing cloud services, as well as which key cloud-specific information security risk areas exist, and moreover if organisations have identified distinguishing factors which can be used as criteria to determine if there is benefit coming from moving a service to the cloud.

Experts in the field confirmed that the TPRM and ISRM processes have not been significantly influenced by this new service delivery model. Organisations add sections to questionnaires specifically designed to cover aspects only relevant for cloud services and more resourceful organisations sometimes contract third parties to do an external assessment of the cloud service provider's cyber security posture.

In terms of cloud-specific information security risks participants raised 15 risks which were assigned to one of the following risk focus areas: Customer-Provider Collaboration, Foreign Government, Identity & Access Management, Data Security & Encryption and Cloud Service Customer Internal Staff. While organisations have similar concerns about risks regarding Data Security & Encryption, any other risks vary depending on an organisation's cloud maturity, size, and industry sector. For example, organisations with low maturity seem to be more focused on building up the required skill set to securely configure and operate cloud services whereas more mature organisations focus also on the retention of know-how to operate services on-premises.

While several technical mitigation measures exist, for 20% of the raised risks contract amendments were proposed to reduce the risk. However, this is a privilege which is only available to large customers of a cloud service otherwise the providers enforce a take-it-or-leave-it culture. Based on the observations I posit that with cloud services there is always residual risk which cannot be mitigated and needs to be accepted.

Regarding distinguishing factors which can be used to assess a cloud service a total of four decision criteria were named: IT Maturity, Laws & Regulations, Complexity and Data & Application Criticality. Furthermore, five indicators were identified to assess a third party's IT maturity: Internal Cloud Know-How, Employ-

ees, Certifications, Reports, and IT VRM Tool Rating. Almost all the information required to assess these criteria and indicators are either public or internal to the cloud service customer, only Reports and the IT VRM Tool Rating have external dependencies. If applied these criteria can give a good indication about the level of risk associated with a cloud service and if it is acceptable or not. By doing the due diligence organisations can avoid consuming cloud services from vendors with lower maturity than their own IT organisations and thus profit from third parties with better security. However, it is imperative for organisations to define a cloud strategy in-line with their risk appetite, which clearly defines the types of services which can be moved to the cloud. All interviewed experts recommend against moving critical data or applications close to an organisations key business processes to the cloud because of the devastating business impact an incident might have.

I posit that my research is providing valuable insights for organisations trying to onboard cloud services. The combined views of experts in the field provide a holistic picture of key risks and mitigation measures used by organisations in various industry sectors. Thus, it is possible to generalise the combined findings and apply them also to organisations in other sectors. The findings obtained through this research are expected to help organisations with risk assessing cloud services and determining if there is benefit in regard to information security risk.

Bibliography

[1] NRICHteam, 'History of morse,' *University of Cambridge*, vol. https://nrich.maths.org/2198, Accessed: 01.04.2020, 2004. [Online]. Available: https://nrich.maths.org/2198.

[2] P. Hallam-Baker, *Announcing alpha test of ptg mail-daemon server*, Mar. 1994. [Online]. Available: https://groups.google.com/g/comp.archives/c/vpWqUAmg8xU?pli=1.

[3] L. S. Gunupudi and R. Kishore, 'The differential benefits of cloud computing for small and medium versus large firms,' in *Information Systems Outsourcing*, Springer, 2020, pp. 235–256.

[4] KPMG, 'Third party risk management outlook 2020,' KPMG International Cooperative, Tech. Rep., 2020. [Online]. Available: https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/08/third-party-risk-management-outlook-2020.pdf.

[5] Deloitte, 'Third party risk management managing risks in your extended enterprise,' Deloitte & Touche Enterprise Risk Services Pte Ltd, Tech. Rep., 2017. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sg-risk-third-party-risk-management-brochure.pdf.

[6] C. Audet, 'Stay ahead of growing third-party risk,' *Gartner*, 2019.

[7] PricewaterhouseCoopers AG, *Excellence inthird party riskmanagement(tprm)*, 2017.

[8] Parliament of Australia, 'Prudential standard cps 234 information security,' vol. 10, no. 1, pp. 39–41, Nov. 2018. [Online]. Available: https://www.legislation.gov.au/Details/F2018L01745.

[9] Monetary Authority of Singapore. 'Mas enhances guidelines to combat heightened cyber risks.' Monetary Authority of Singapore, Ed. (18th Jan. 2021), [Online]. Available: https://www.mas.gov.sg/news/media-releases/2021/mas-enhances-guidelines-to-combat-heightened-cyber-risks (visited on 12/02/2021).

[10] P. Mell and T. Grance, 'Draft nist working definition of cloud computing,' *Referenced on June. 3rd*, vol. 15, no. 32, p. 2, 2009.

[11] T. Dillon, C. Wu and E. Chang, 'Cloud computing: Issues and challenges,' in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 27–33. DOI: 10.1109/AINA.2010.187.

[12] O. Ali, A. Shrestha, A. Chatfield and P. Murray, 'Assessing information security risks in the cloud: A case study of australian local government authorities,' *Government Information Quarterly*, vol. 37, no. 1, p. 101 419, 2020.

[13] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato and A. Kanai, 'Risk management on the security problem in cloud computing,' in *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering*, IEEE, 2011, pp. 147–152.

[14] S. Tanimoto, R. Sato, K. Kato, M. Iwashita, Y. Seki, H. Sato and A. Kanai, 'A study of risk assessment quantification in cloud computing,' in *2014 17th International Conference on Network-Based Information Systems*, IEEE, 2014, pp. 426–431.

[15] MSCI Inc. 'The global industry classification standard (gics®).' MSCI Inc., Ed., MSCI. (), [Online]. Available: https://www.msci.com/gics (visited on 20/03/2021).

[16] BARCLAYS. 'External supplier control obligations.' BARCLAYS, Ed. (), [Online]. Available: https://home.barclays/who-we-are/our-suppliers/our-requirements-of-external-suppliers/external-supplier-control-obligations/ (visited on 14/05/2021).

[17] Google. 'Encryption at rest in google cloud.' Google, Ed. (), [Online]. Available: https://cloud.google.com/security/encryption/default-encryption (visited on 21/05/2021).

[18] Microsoft. 'Bring your own key (byok) details for azure information protection.' Microsoft, Ed. (11th Sep. 2020), [Online]. Available: https://docs.microsoft.com/en-us/azure/information-protection/byok-price-restrictions (visited on 21/05/2021).

[19] Google. 'Using customer-supplied encryption keys.' Google, Ed. (), [Online]. Available: https://cloud.google.com/storage/docs/encryption/using-customer-supplied-keys?hl=en (visited on 21/05/2021).

[20] A. Mnev. 'How to byok (bring your own key) to aws kms for less than $15.00 a year using aws cloudhsm.' Amazon, Ed. (12th Mar. 2021), [Online]. Available: https://aws.amazon.com/de/blogs/security/demystifying-kms-keys-operations-bring-your-own-key-byok-custom-key-store-and-ciphertext-portability/ (visited on 21/05/2021).

[21] Slack. 'Slack enterprise key management.' Slack, Ed. (), [Online]. Available: https://slack.com/intl/en-gb/enterprise-key-management (visited on 21/05/2021).

[22] Amazon. 'Global infrastructure.' Amazon, Ed. (), [Online]. Available: https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls (visited on 22/05/2021).

[23] Monetary Authority of Singapore, Ed., *Instructions on Incident Notification and Reporting to MAS*, 22nd May 2021. [Online]. Available: https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/Instructions-on-Incident-Notification-and-Reporting-to-MAS--Nov19.pdf.

[24] M. Punke. 'Aws and the cloud act.' Amazon, Ed. (29th May 2019), [Online]. Available: https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/ (visited on 22/05/2021).

[25] Microsoft. 'Government access to data.' Microsoft, Ed. (), [Online]. Available: https://news.microsoft.com/cloudforgood/policy/briefing-papers/trusted-cloud/government-access-data.html (visited on 22/05/2021).

[26] S. Ackerman. 'Tech giants reach white house deal on nsa surveillance of customer data.' The Guardian, Ed. (27th Jan. 2014), [Online]. Available: https://www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data (visited on 22/05/2021).

[27] M. Staedeli. 'Us-behörden können neu die herausgabe von daten auf ausländischen servern verlangen.' Neue Zürcher Zeitung, Ed. (15th Dec. 2018), [Online]. Available: https://nzzas.nzz.ch/wirtschaft/cloud-act-us-behoerden-herausgabe-von-daten-ld.1445117?reduced=true (visited on 22/05/2021).

[28] CMS, Ed. 'Gdpr enforcement tracker.' (), [Online]. Available: https://www.enforcementtracker.com/ (visited on 22/05/2021).

[29] S. Huber. 'Accidental data deletion in mycloud: The most important facts and faqs.' Swisscom, Ed. (12th Jul. 2019), [Online]. Available: https://www.swisscom.ch/en/about/news/2019/07/faktencheck-mycloud.html?login&nevistokenconsume&error=NOT_LOGGED_IN (visited on 28/05/2021).

[30] M. J. Butkovic and R. A. Caralli, 'Advancing cybersecurity capability measurement using the cert®-rmm maturity indicator level scale,' 2013.

[31] International Standards Organisation (ISO), Ed. 'Certification.' (22nd May 2021), [Online]. Available: https://www.iso.org/certification.html.

[32] C. Schmitz, M. Schmid, D. Harborth and S. Pape, 'Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities,' *Computers & Security*, p. 102 306, 2021.

[33] N. MacDonald, 'Innovation insight for cloud security posture management,' *Gartner Research*, 2019. [Online]. Available: https://www.gartner.com/en/documents/3899373/innovation-insight-for-cloud-security-posture-management (visited on 23/05/2021).

[34] K. Torkura, M. I. Sukmana, F. Cheng and C. Meinel, 'Continuous auditing and threat detection in multi-cloud infrastructure,' *Computers & Security*, vol. 102, p. 102 124, 2021.

[35] J. Cable, D. Gregory, L. Izhikevich and Z. Durumeric, 'Stratosphere: Finding vulnerable cloud storage buckets,' 1st Apr. 2021.

[36] F. D. Kum, R. Cowden and A. M. Karodia, 'The impact of training and development on employee performance: A case study of escon consulting,' *Singaporean Journal of Business Economics and Management Studies*, vol. 3, no. 3, pp. 72–105, 2014.

[37] K. E. Emam, L. Briand and R. Smith, 'Assessor agreement in rating spice processes,' *Software Process: Improvement and Practice*, vol. 2, no. 4, pp. 291–306, 1996.

[38] Google. 'Compliance offerings.' Google, Ed. (), [Online]. Available: https://cloud.google.com/security/compliance (visited on 23/05/2021).

[39] Uniscon GmbH. 'Idgard sicherheit.' Uniscon GmbH, Ed. (), [Online]. Available: https://www.idgard.de/sicherheit/ (visited on 23/05/2021).

[40] Green Datacenter AG / green.ch AG. 'Certificates.' Green Datacenter AG / green.ch AG, Ed. (), [Online]. Available: https://www.green.ch/en/about-green/company/why-green/certificates (visited on 23/05/2021).

[41] R. Roewekamp. 'Ein it-mitarbeiter betreut 105 anwender.' IDG Business Media GmbH, Ed. (5th Feb. 2010), [Online]. Available: https://www.cio.de/a/ein-it-mitarbeiter-betreut-105-anwender,2217433 (visited on 23/05/2021).

[42] UpGuard, Ed. 'Bitsight vs securityscorecard 2021 comparison and review.' (), [Online]. Available: https://www.upguard.com/compare/bitsight-vs-securityscorecard#:~:text=%20Pricing%20and%20support%201%20BitSight%20-,here.%20UpGuard%20pricing%20starts%20at%20$5k/year...%20More (visited on 23/05/2021).

[43] Google. 'Compliance reports manager.' Google, Ed. (), [Online]. Available: https://cloud.google.com/security/compliance/compliance-reports-manager (visited on 23/05/2021).

[44] @HIgh Bit Security, Ed. 'Standard penetration test cost card.' (), [Online]. Available: https://highbitsecurity.com/penetration-testing-cost.php (visited on 23/05/2021).

[45] J. Johnson. 'How much does a web application penetration test cost?' T. Security, Ed. (), [Online]. Available: https://www.triaxiomsecurity.com/how-much-does-a-web-application-penetration-test-cost/ (visited on 23/05/2021).

[46] Schweizerische Eidgenossenschaft, Ed., *Bundesgesetz über die Banken und Sparkassen, Art. 47*, 8th Nov. 1932. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/51/117_121_129/de (visited on 23/05/2021).

[47] C. Laux, A. Hofmann, M. Schieweck and J. Hess, 'Nutzung von cloud-angeboten durch banken,' *Laux Lawyers AG*, 14th Feb. 2019. [Online]. Available: https://www.lauxlawyers.ch/wp-content/uploads/2019/03/Cloud-und-Bankgeheimnis.pdf (visited on 23/05/2021).

[48] Ministry of Local Government and Modernisation, Ed. 'Cloud computing strategy for norway.' (), [Online]. Available: https://www.regjeringen.no/en/dokumenter/cloud-computing-strategy-for-norway/id2484403/?ch=4 (visited on 23/05/2021).

[49] A. Marmor, 'The pragmatics of legal language,' *Ratio Juris*, vol. 21, no. 4, pp. 423–452, 2008.

[50] Deloitte, Ed. 'Mega-thema datenschutz: Neue regulierung in einem brisanten kernbereich der digitalisierung.' (), [Online]. Available: https://www2.deloitte.com/de/de/pages/risk/articles/datenschutz-digitalisierung.html (visited on 23/05/2021).

[51] F. Montesi and J. Weber, 'Circuit breakers, discovery, and api gateways in microservices,' *arXiv preprint arXiv:1609.05830*, 2016.

[52] J. Akella, H. Buckow and S. Rey, 'It architecture: Cutting costs and complexity,' McKinsey, Ed., 1st Aug. 2009. [Online]. Available: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/it-architecture-cutting-costs-and-complexity# (visited on 23/05/2021).

[53] J. Hasbrouck and G. Saar, 'Low-latency trading,' *Journal of Financial Markets*, vol. 16, no. 4, pp. 646–679, 2013.

[54] D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire and P. R. Inácio, 'Security issues in cloud environments: A survey,' *International Journal of Information Security*, vol. 13, no. 2, pp. 113–170, 2014.

[55] U.S. Department of Justice, 'Promoting public safety, privacy, and therule of law around the world:the purpose and impact of the cloud act,' 1st Apr. 2019. [Online]. Available: https://www.justice.gov/opa/press-release/file/1153446/download?utm_medium=email&utm_a=govdelivery (visited on 21/05/2021).

[56] P. Géczy, N. Izumi and K. Hasida, 'Cloudsourcing: Managing cloud adoption,' *Global Journal of Business Research*, vol. 6, no. 2, pp. 57–70, 2012.

Appendix A

Interviews

Appendix A contains additional information about the interviews held as part of the Master Thesis. A copy of the interview information brochure shared with the interviewees prior the interview and described in chapter 3 has been added. Additionally, the transcript of every interview can also be found in this appendix.

NTNU

Norwegian University of Science and Technology

Interview Information

Manuel Fluri; M.Sc. Thesis Information Security Management; 2021

Working Title: Information Security Risk Management analysis for traditional and cloud service models

Research Project Interview Information

Research Project Objective

- Gain a better understanding of how information security risks change with the service delivery model (cloud vs. on-prem)
- Identify distinguishing criteria on which an organisation can assess the impact on their IT maturity when moving a service from on-prem to the cloud.

Interview Objective

- Collect data by interviewing key experts. Focus of questions will be:
  - Information Security Risk Assessments for Third-Party Engagements with focus on differences between a classical and a cloud service delivery model
  - The diffrence in terms of information security risks between the classical and a cloud service delivery model
  - Key criteria which could help to assess if there is a benefit from an information security perspective if a service is moved from on-prem to the cloud

Interview outline

- **Interview Duration:** ~60 minutes
- **Question Type:** Open questions which allow to explore ideas and go into detail if required.
- **Question content:** Will be aligned with "Interview Objective"-section above.

Data collection & usage

- The conversation will be recorded with a phone
- After the interview the recording will be used to compose a transcript
- The transcript will be shared for review and approval with the interviewee
- The recorded version will be deleted after the approval has been received
- Each interviewee will be pseudomised using the following set of information: a reference ID; job description; years of experience; type of interviewee (industry or academic)
  - For participants of type industry the sector of their employer will be named as per the global industry classification standard

Identifier	I-I-01	Generalised Job Title	Senior Manager IT Security Infrastructure
Years of experience in IT	**Years of experience in cloud computing**	**Academic/Industry**	**Area of lecturing/Industry sector**
36	4	Industry	Financials

Key Messages:

- There is not enough experience with cloud services yet to have a common understanding of how relevant certain risks are. Different people have a different understanding which influences the mitigation measures as best practices have not been established yet.
- An organisation needs to identify the weak points and vulnerabilities of a third-party it is doing business with.
- Information Security Risk Management for cloud services should consider doing worst-case impact assessments.
- An organisation needs to be clear about how much control they are willing to and also can give away.
- While cloud service providers are ensuring that different tenants have no access to each other, the CSP will always have access to the data of all tenants. Moreover, the CSP has always means to decrypt data encrypted using the CSPs technology, e.g. to restore a backup or through keys stored in the memory.
- The IT maturity of a firm is a key measure to determine how big the benefit is when a service is moved to the cloud.

Who	Statement
MF	Where would you place your company in terms of cloud maturity? Maturity scale 1-6 (1 – very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent)
I-I-01	Sufficient
MF	Why 4 and not 6?
I-I-01	I think there is relatively little experience with cloud services in the industry still. The technology itself is quite mature. But from a security perspective there is no common understanding yet, about what should be done on the cloud. There is a need for clear standards and guidelines specifying this. A concrete example: Is an external IaaS cloud a third-party environment or is it a part of the internal environment? Now, while best practices exist, there are still a lot of different views from different people when discussing the topic. A common view has not been formed yet.
MF	In general, between IT and the business or just within IT?
I-I-01	Within IT. Looking at today's on-prem data center environment a common view has formed between application development and infrastructure security departments. But when it is coming to cloud services the positions of the parties are still far apart. Application development teams would like to treat cloud as an internal environment without additional risk. Where IT security teams warn about the lack of control in the environment and see additional risks which need to be assessed. Once these positions are more aligned to each other it will also be easier to conduct proper risk assessments. The alignment is something which requires time. Similarly, to when virtualisation of servers was a new topic. Back then the application development teams had massive reservations in the beginning. Infrastructure teams were pushing for the move and highlighting the benefits. Meanwhile, these views have aligned and there is a good understanding about what can be virtualised and what should not.

MF	Would you consider these risks to be hygiene risks raised by a lack of understanding?
I-I-01	There are always optimists and pessimists regardless of the risks, depending on somebody's experience. Once a common base of experience has been established then the positions align. If you look at both cloud and virtualisation then for virtualisation it was infrastructure teams who were pushing for it and application teams had more reservations. With cloud it is the opposite the app dev teams are more optimistic, as things are simpler, quicker and cheaper from their perspective. Infrastructure teams on the other hand are more sceptical as they see additional risks and costs and a lot of additional things which need to be done. But this will align over time with additional experience.
MF	How would you assess Information Security risk for new services?
I-I-01	With information security risks it is about imagining the unimaginable. One needs to think about "what could possibly go wrong?". Based on this, one needs to assess the relevancy of the risk. Out of this a best practice can be established. Within the own data center there are over 20 years of experience. People did develop a common sense of which risks can be taken and which cannot over this time period. For cloud environments this has not happened yet. One needs to be able to differentiate between what are vendors trying to sell to you and what are facts. Vendors always claim that they are secure and deliver to the requirements. Especially IT security vendors, and this is not cloud specific, cannot imagine being a target of an attack. Thus, becoming a risk for their customers. Which is why an organisation needs to identify the vulnerabilities of a third-party. A key question then is also how can this be controlled?
MF	This would be part of a third-party risk assessment.
I-I-01	Yes and it would also cover other aspects like supply chain risks. In the end it is about giving away control to a third-party. The key questions which an organisation needs to ask themselves are: • How much control do we want to give away? • How much control can we give away? Ultimately, the accountability stays with the organisation but there is a loss of control. Which means that one needs to trust the third-party.
MF	Who should define how much control is given away? Respectively, which vendor to trust?
I-I-01	This is a question of how much risk an organisation is willing to take. And also, very difficult to assess correctly because of the lack of experience and understanding of what is reasonable. One example, NASA built the space shuttle. From experience we know that out of roughly 135 starts, 2 went catastrophically wrong. How should this be assessed in the beginning when there was no experience? It is very difficult, which is why we need more experience for a reasonable assessment. What can help is a gap analysis between something running on-prem and something moving to the cloud. Here one needs to differentiate between a SaaS and an IaaS. I am talking mostly about IaaS. For IaaS one needs to ask themselves where things are changing compared to on-prem and consequently if the changes are for the better or the worse. In a cloud environment the infrastructure is shared with other organisations. On-prem the infrastructure is dedicated to the organisation. Meaning that when the borders between organisations are not airtight from a technical perspective, somebody else could look at your data or tamper with it. On the other hand, cloud providers invest a lot of money to ensure that this does not happen. The question now is how big is the risk? To answer this question, one needs to think about the potential damage. And from my perspective there are two questions an organisation needs to answer when moving something to the cloud. The first one is: Can we live with loss of service and/or data from one second to the other? Here a firm has the

	possibility to introduce mitigating measures like a good backup strategy or redundancy strategies. A cloud service provider could declare bankruptcy and then the service is gone. Or there could be an error by the CSP impacting its clients. For example, the case when Swisscom deleted their private customers' cloud storage.
MF	You make a very good point. Backup is one of the key benefits highlighted for cloud services because the cloud service provider is taking care of them for you.
I-I-01	Absolutely right. The second question is: Can you live with your data being made public?
MF	Which is going back to your initial statement that an impact assessment of worst-case scenarios is important.
I-I-01	Correct and one cannot categorically assume that this would not happen if things were being done on-prem. Which is also why it is important that one also understands the benefits of a cloud service. And the benefit coming from a cloud service depends on the situation of an organisation. Looking at an example: picture an SME organisation where IT is mostly about accounting and order processing, both running on one server. Backup strategy includes changing tapes which is forgotten 50% of the time and patching is also never happening. For a firm like that there is a lot of benefit in moving to a cloud service. However, if you are a firm with a state-of-the-art IT environment, with a clear backup strategy, good border security, clear patching processes, etc. Then there might be more risks than benefits from moving to a cloud service. Hence, I think moving to a cloud service depends a lot on the IT maturity of a firm. For an SME there are more benefits than a large financial institution which has invested a lot of money in their IT.
MF	How are risks changing when moving to a cloud?
I-I-01	Cloud providers will always tell you that something is safe and that the customer has its own cryptographic keys, etc. However, to a certain degree this is an illusion. It might be true for other customers accessing your data but in the end the cloud provider needs to be able to work. For example: The cloud provider is encrypting your backup. Then the cloud provider needs to be able to restore your data which means he has the key. Even if you need to type it in as password, it is in the memory afterwards. Meaning he has the means to decrypt your data. Another point is that while proper access management helps to separate access between customers, the cloud provider has access to everything. So, the danger lies not with another customer getting access to your account but that the cloud provider is hacked, giving the hackers full access to all customers' data. This is fully under the control of the service provider. There are no technical measures to protect yourself. Also, when a provider offers a password vault and claims nobody else has access to it, then this is not true. The cloud provider has access to it. In the end it is all software and somewhere in the memory. It might be not trivial to get access to it but the cloud provider is working with the data so there is technical access at least. This is a discussion we have over and over again. Somebody claims the data is encrypted in transmission and also at rest. Hence nobody can access it. This is factually not correct. Moreover, all virtualised environments are running on a hypervisor. There is a reason why it is called hypervisor, it means it sees everything. The hypervisor sees, steers and controls everything. This needs to be understood. However, a lot of people do not understand the difference to the on-prem environment. The key difference is that with on-prem virtualisation the organisation controls the environment and the boundary. In the cloud an organisation controls the boundary of the tenant but not the boundary of the cloud. Let's make an example: you have a virtualised environment in the cloud and one on-prem. On-prem, at least in theory, you can see that somebody is coming over your boundary and attacking the hypervisor. You can also control which data is sent to the internet. When you go to the cloud then you

	have this on the tenant level but you have no visibility on the cloud level. Also the cloud provider sees the traffic but he is unable to decide if the traffic is good or malicious because of a lack of context. Thus, there is not only loss of abstract controls like reviews but also loss of control of certain traffic and attacks. Neither cannot be understood by the customer due to a lack of visibility. Of course, cloud providers are doing a lot to protect themselves and they are most likely doing a good job. But it is an area where the customer has to trust the cloud provider that he is doing a good job. Which leads to another question: how can the customer monitor & control the cloud provider in this regard? A cloud service consumer will not be able to audit a cloud provider. They rely on certifications of the cloud provider, but this is still not a zero risk guarantee.
MF	Which also requires contractual measures to ensure that the cloud provider allows reviews and shares the report.
I-I-01	Yes, and also that he is adhering to the agreed requirements. The cloud service provider can tell an organisation that they do background checks on their employees. How are you going to verify this? In the end it means you need to trust the service provider or trust a certification a provider has and needs to recertify periodically. However, fundamentally there is always residual risk. Which an organisation can choose to accept to a certain degree. Also raising the question if a tenant should be treated as a simple extension of your internal infrastructure or should it be treated as a third-party environment. The latter requiring controls between the internal infrastructure and the tenant to limit the blast radius if something is going wrong. Imagine a hybrid application architecture, with components hosted in the cloud and on-prem. Then the question is: What is the collateral risk which is being introduced to services which are consciously not moved to the cloud? Because you are interconnecting two environments one of which you do not fully control and where something can go wrong. Obviously, something could go wrong on your side but for this you are fully responsible There is the possibility to introduce contractual safeguards. But even if you can sue them for one billion USD, it does not help you if you have been thrown out of business by a regulator or loss of customers.
MF	And that protection would not help you if the cloud provider would declare bankruptcy and the hardware is sold then as part of the bankrupt's assets
I-I-01	Yes. Obviously, that something like this happens with a big firm like Amazon, Microsoft or Google is probably unlikely. With these the risk that they get hacked is more probable and with that the whole security is undermined. This is the holy grail for any hacker as they would gain access to all the data. Hence, it is probably fair to assume that they are being attacked more often, because there is massive benefit for anybody getting in. Even if they do the best, something can always go wrong like for example with the SolarWinds case. Supply chain attacks can also impact on-prem infrastructure but the upside with hacking a cloud provider is much bigger. It also raises another issue the one of not knowing how the service provider operates and what he uses to provide the service. So there might be risks of which you as the customer do not know about. Introduced by the use of technology by the cloud service provider invisible to the customer. And these risks are unfortunately not theoretical but there are enough examples where these things went wrong.
MF	You already mentioned an organisation's maturity and the number of employees as key decision criteria for an organisation if they should move to a cloud service. Do you see any other criteria?
I-I-01	It depends on the case. When looking at SaaS a lot of times people do not want to do something themselves. One has to look at the drivers then: Is it cheaper? Do we not have the skills?, and what is your core business? For things outside of the core business it could be better to buy it as SaaS rather than doing it yourself. When it is

	then about core business processes then one needs to be very clear how much control does one want to give away and what is the worst-case scenario if something goes wrong? Another challenge with data is that unlike a car, you do not realise it is gone and they cannot be brought back. And an organisation who has data which should not be made public should not put them in the cloud.
MF	Are there any other criteria? You have mentioned SolarWinds. Would you buy software from them?
I-I-01	I do not think any vendor is immune to cyber-attacks. There could be a key logger in Microsoft Word sending out all the data. So there needs to be a base level of trust. It is also important to monitor the firms if they take their lessons learned. Also, it was not a trivial attack if I recall correctly but a complicated supply chain attack against one of their software suppliers. The question is how an organisation can contain the blast radius of such an event. If Word or Outlook were hacked, then one has not much of an option than using another product. In some cases, there are mitigating controls, e.g. using network based scanning of the data exchange. But one will not be able to get the ultimate guarantee.
MF	And exchange was also very prominent in the news.
I-I-01	Yes exactly. The concept which is now becoming the standard is zero trust. Meaning that one only allows what is required to what requires it. Minimizing the attack surface. Any type of segmentation, network based, or application user rights helps minimizing the attack surface. Systems not requiring a function should not be able to access it. This methodology should also be applied to cloud services and it also helps to reduce the impact of an incident in the cloud to on-prem. We mostly talked about cloud as IaaS but there are obviously other use cases like VDIaaS which brings different risks. So, it also depends on the use case. And again, I think we still have a low maturity when it comes to consuming cloud services and what are the best practices. There is progress, like a standard released by the bank of England which defines certain things, but it is still something ongoing. I think it is important for an organisation to understand where an organisation is in terms of maturity and when a cloud service is consumed, does it bring benefits to the maturity.
MF	We have reached the end of the interview. Thank you very much for agreeing to participate.

Identifier	I-I-02	Generalised Job Title	Cloud Security Specialist
Years of experience in IT	**Years of experience in cloud computing**	**Academic/Industry**	**Area of lecturing/Industry sector**
25	4	Industry	Information Technology

Key Messages:

- Cloud platforms provide a comprehensive security ecosystem to their customers.
- Customers in the financial sector have the highest level of scrutiny whereas other industries are usually only focusing on basic compliance.
- Cloud providers might allow large organisations to do their own audits even on-site.
- SMEs should trust certifications like SOC or ISO27001 when they were done by independent auditors.
- Cloud providers should consider being transparent and for example introduce a bug bounty program and allow people to penetration test their systems whenever they like.
- Customers need to understand what they can expect from their cloud provider in terms of compliance with regulations, e.g., notification periods for incidents which are subject to reporting to a regulator.
- The IT and IT security maturity of SMEs can significantly benefit when going to the cloud. The cloud provider takes care of important IT processes like backup and restore. Large organisations with poor processes can also benefit.
- Cloud providers work with customers to address their needs to reduce risk, like data sovereignty.
- Cloud service customers need to adapt their processes when buying cloud services and assess certain areas differently than e.g., a classical outsourcing.
- Cloud service customers should look at the technical security, data security & key management, commercial aspects, and compliance of a cloud service.
- Cloud service customers need to have a clear vision about how they can benefit from using the cloud to drive innovation and digitization.
- Some IT personnel might be afraid of losing their job when moving to the cloud. The classical IT roles will evolve with the transition to the cloud but most likely not disappear.

Who	Statement
MF	Where would you place your company in terms of cloud maturity? Maturity scale 1-6 (1 – very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent)
I-I-02	Do you mean as a consumer or a provider of cloud security?
MF	Would be interesting to get your view on both.
I-I-02	I think our security is excellent so I would rate it in the highest quadrant. It was one of the reasons why I joined this organisation which has been serving customers of cloud services for over 20 years. The scale of the organisation and what they had to defend is huge. With offering cloud services, we offer that same level of security to other customers. Let us take DDoS as an example, we had a customer last year who was hit with 6M packets per seconds as an attack. The advantage for them being on the Google Cloud was that we were able to absorb the attack and were able to protect them. If you are hosting on our cloud, then you benefit from our very large-scale defences of the platform as part of your infrastructure. Another example if we observe that the TCP three-way handshake is not completed then we drop the traffic

	even before we give it to the company. Also, from a content delivery point of view, if you are a global company, you can also profit from the multiple entry points due to our global presence. And I think we also have been a pioneer in security. We have developed a lot of open-source solutions which we offer to customers. Like a zero-trust solution, to help customers get rid of VPNs. Previously there was a mindset that people can only access certain data from the intranet. The pandemic has forced to rethink these concepts. It has been designed so that it does not matter if somebody is inside or outside the company. We authenticate and authorise them based on their platform, their location, the patching level of their system, whether they have the 2FA authenticated, etc. These are a few examples to show why I believe we have excellent security for our customers.
MF	Do you consume third-party cloud services, or do you have everything in-house?
I-I-02	Yes, we do, for example SAP or Salesforce
MF	Meaning, you basically use an external service whenever you are not willing to develop something yourself.
I-I-02	Yes, I think this is a good way to describe it. If something is the best tool in the business, then we are also using these.
MF	How should information security risks be assessed when using third-party services? Looking from both perspectives at it: one being a Cloud Security professional helping your customers to assess and mitigate risks but also when your organisation is consuming cloud services.
I-I-02	One thing to mention is that often it starts with the compliance aspects of the service. When I think about some of our customers, e.g. a large institution in the financial sector, one of the things they want to know from us is which external certifications have we received. It depends a lot on the industry. Manufacturing and retail are not always so focused on compliance issues compared to finance. They want to see if we got the right certifications. For example, the ISO/IEC 27001 and 27017 and look at the report. Also, the SOC reports are quite important because the auditors there come and look at how we deliver the services. So, that is the compliance side of things which is often the first step. The second step is then to look at technical side of things. What customers want to understand is what are the layers of security our cloud is build on. We often talk about the hardware base that we build on including our data centers. Often, they want to know where are the data centers and do they have 24/7 guards, do they have cameras, have we done penetration testing, which risks did we consider with the location, etc. And with financial industry customers we usually go down to the n^{th} level of detail. The level of scrutiny is really down to the server rack where my data is kept. So, the hardware is the lowest layer. On top of that we have our service, sort of our engine running the cloud service. On top of that we then have storage. By default, we encrypt all the disks, and it is not optional for our customers. We then talk about Identity and Access Management and we typically link it with the customer's active directory usually in Azure or on-prem. We synchronise the users into the cloud. We also need to look at the network, how do they connect to the cloud? Could be a VPN for a small company up to a dedicated inter-connect with multiple failure parts. And lastly the actual services we provide. So, as I said it is a combination of the compliance issues which are often the very first thing and then come into the technical as the next thing. The other thing I wanted to mention is the encryption: We chunk the data, encrypt each chunk with its own key and encrypt the keys with a key encryption key. The encryption key management is very important for customers. By default, we do the encryption, but more sophisticated customers usually would like to manage their own keys and decide for example when keys are rotated. In some cases, they even want to use a hardware encryption module or external key management. Back to your question and as I said it is often with

	compliance, where customers first want to see which reports do, we have. Secondly, they want to understand the stack we build on, how are the data centre and services secured up to the services they use. And then the key management is very important. So, we discussed data at rest, we also encrypt data in-transit so all VM-to-VM communication is encrypted. We also have implemented a technique to encrypt the memory of the VM in the hypervisor. So for us it was important to close that loop to encrypt data at rest, in transit and also while processing to the extent that one can.
MF	Yes, and also confirming that data security is a key topic when moving data to the cloud. Ultimately, the cloud service provider always has the key at some point in time in your case to decrypt the data to send it from the memory to the CPU's cache.
I-I-02	Yes, that is true and is where your identity and access management is so important. Because if you give a process the possibility to read from a data base, even if the data base is encrypted, the process needs the authorisation to go in through the front door with the keys to get the data, hence be able to access the keys. The data at rest part is while it is static and not in use but the moment you start to process it you have access to it through your programmatic methods. Which means it is also very important to protect and carefully control the service account keys. You could store them in your GitHub repository and accidentally leak them in your source code. So better to have something with proper identity and access management controls which allow you to fetch the keys when you need them, get the data and then loose the credential again. It is a new world and I think there is a bit learning curve for organisation so that they use it in the correct way as well. The possibilities to build a secure environment are there. But if you do something wrong and you misconfigure or misuse it in a way you did not intend; or you make a storage bucket open to a public view that is where the problems come into play.
MF	Do you have customers which actually want to see things, not only the report but e.g. do a visit on-site or audit you even?
I-I-02	Yes, so what we have done in Germany for example is a pooled audit. Where a lot of financial companies came joined forces to do the audit. Another large financial institution came onsite and audited our data centers. We provided virtual reading rooms to their internal audit, obviously under non-disclosure agreements, where they could look at our reports and processes. They cannot take information away, but they can come and look and scrutinize how we do things and whether there is an acceptable level of risk.
MF	I assume this is only available to large organisations and an SME could not do this.
I-I-02	Sure, but this is where the compliance reports are available to everybody. The SOC report was done by Ernest & Young. All the SMEs should be able to trust EY to audit all the controls. They go through relevant aspects of internal controls, policies, communications, procedures, monitoring and then they test certain controls and report on the results. So, for most companies this should be more than enough in terms of evidence that it has been highly scrutinized already. However, larger organisations sometimes want to dig a bit deeper to satisfy themselves in the light of the potential risk.
MF	From your experience do you think your organisation is better than others in terms of information security and transparency?
I-I-02	I think we are very open. In the terms & conditions we explicitly state that any customer is allowed to penetration test our cloud systems at any time. We do not even ask for prior notification, the only thing we ask is that if they do find bugs they report them to our bug bounty program. The company has been proactive in that regard and almost embraced the security researchers and practitioners to help fortify the environment. Obviously, every cloud provider will tell you they have great security, but I think that our cloud security ecosystem is quite interesting. The

	possibility to combine our cloud solutions with our security features like zero trust network access, identity aware proxies, DDOS prevention, etc. customers get an advantage. The security awareness of the organisation is also something which attracted me to work for them.
MF	We already talked about data security as being an important focus area when people move services to the cloud. Do you see any other areas which customers should look into?
I-I-02	I think things around incident response, disaster recovery and business continuity. These are things customer want to know about. Especially at what point will we notify them of an incident. Because there are a lot of reporting requirements for companies, e.g. GDPR or some regulations from regulators like FINMA. We have a lot of white papers, for example on our incident process which contains information like how we triage incidents, at what point we communicate to the customer and how we will work with them to recover. Also, when they are moving to the cloud the concept of disaster recovery and business continuity is very important. Our cloud is made up of multiple regions which each contain different zones. Failover can work within a zone but one could also have infrastructure in a different region and then failover to that in case of a disaster. Business continuity also needs to be a combination of responsibility between the cloud provider and the business. They may decide to switch to a different cloud provider and we have been promoting swapping between cloud providers. Customers are also worried about lock-in, and they want to be able to move between cloud service providers. We try to promote an open model and obviously in the end get more business by giving it away.
MF	How do information security risks change when moving services from on-prem to the cloud?
I-I-02	It depends on the organisation. I just had a call before this one with a large organisation which did an audit of the company. It was found that they are lacking in a lot of areas. So, for some organisations, especially SMEs, there is a big advantage in moving to the cloud. The cloud provider takes care off a lot of important processes, like backups and restore, disaster recovery, etc. For some companies the risk can be lower when moving to the cloud and ironically even for some large organisations. However, large organisations with a mature IT might worry about the loss of control they experience when moving to the cloud and trusting a third-party in doing the processing. Mostly organisations in the financial sector are very cautious about it and ask themselves if it is a reasonable risk to take. We are saying we think it is a reasonable risk. We are also working hard that things like “bring your own key” is available across all our services. It is not available for all our services yet, but we are evolving. And I think that cloud providers realise that they need to address the risks as asked by the customers. They are looking to make the products more suitable and for example also have data residency guarantees. This to ensure that data stays within a region like Switzerland. Not all of our services are able to provide this guarantee yet. But it also breaks sometimes the global concept, for example when a Swiss user is in Singapore and needs to contact the Swiss region to authenticate. Some customers want data sovereignty. For example, that only Swiss engineers could work on Swiss data and an American engineer could not. We have it already in a pilot phase implemented in the U.S. for government departments. This way we can guarantee that only U.S. engineers are working on their data. We also have features to log access of our engineers to the data of a service of a customer and one where access needs to be pre-approved by the customer. When an organisation is using an external key manager then our engineer needs to provide a justification why a key is used for each request. We are trying to give a lot of insight into how the cloud is being used so that organisations can have confidence and are willing to take the risk.

MF	If you think about other firms using cloud services, what should they focus on in terms of risks? For example, there were cases of companies when payments were missed, and data was simply deleted.
I-I-02	I think organisations need to be careful which cloud vendors they select. This is another aspect of cloud security which I worked on at my previous company was this thing of shadow IT. You have people storing internal data in Box or in Dropbox and one team is using Slack the other team is using something else. It becomes very difficult to control which cloud services are actually being used. So, you get these CASB systems which intercept the traffic, and you can see which clouds are being used. The problem is that a lot of organisation have a traditional model to assess vendors and they need to adapt this for cloud services. We had a customer who wanted to test the calling tree which makes sense in an outsourcing model. But you do not have that with a cloud provider. So, you need to come up with a set of criteria that work for your organisation where you look at technical aspects of the cloud service, like availability, what are they offering you in terms of resilience and uptime of the service. And then you also need to look at the data aspects of a service, so especially where is my data stored and can I get my data back. Like the example you mentioned, one should be able to leave the cloud provider and get their data back. Then there is the commercial aspect, will the provider offer to pay a penalties if the service is unavailable? You also want to understand how they have been assessed, like ISO 27000, do they have SOC reports, etc. So these are the kind of things customers usually ask us and I would recommend if you are coming up with a model: look at the technical security, data security, commercial aspects and compliance. What certifications does this provider have? Which can save you a lot of work if somebody is doing it anyway on a regular basis.
MF	Can you imagine a case where you would advise a company not to use a cloud service?
I-I-02	Yes, I would, and it even happens to us. When they have a minimum set of requirements, especially around data residency or contractual commitments. If they are not willing to make those kinds of undertakings than this could be a reason to not select somebody. You made the example of SaaS vendors where it is really easy to just buy something online and use it. But the question is what it could be exposing the organisation to, in terms of continuity. When data is lost on the cloud because of an operational reason or commercial reason, then the question is what the impact on the business is. That is where businesses have to be careful with which cloud providers they use.
MF	Or it could be worse and there could be an unintentional disclosure of data
I-I-02	Yes, for sure. In terms of your GDPR responsibilities for European companies, they are the control of the data so the main responsible. The cloud provider is the processor of the data and of course the processor's security is part of the picture. However, in the end you as the controller are overall responsible. So you do need to choose your platforms carefully.
MF	And depending on the type of data, it also does not help when you have contractual measures like penalties defined. Even if they pay you one billion dollars, it will not help if a regulator is putting you out of business.
I-I-02	Fully agree, yes.
MF	We have talked about how a firm can determine if there is benefit coming from moving to the cloud. So far you have mentioned the size of a company, size of IT department, number of security professionals. Do you see any other criteria?
I-I-02	Well, I think the reason for choosing different cloud providers is the value add that you can get. So, if suddenly in your mobile banking app you have the possibility to integrate with maps or translate and translate it to any language on earth a user

	would like. Or you can apply machine learning insights that maybe are not so fast in the internal environment. So, if there are additional business factors which help you to drive innovation and digitization and your channels that you are using as a business, that should be the goal. If you just take a virtual machine and put it on the cloud, then that is the lowest possible return you can get. You really want to rethink the business opportunity. If you think of the massive infrastructure with the content delivery network, the global caching, the high-speed fibre network is another opportunity which companies have not realised yet. They can do a lot of traffic engineering in the cloud rather than using an expensive wide area network. In the end you want to improve the experience of your customers. Also, the elastic possibility to scale up and scale down, the built-in security, etc. are the kind of benefits which should drive things into the cloud.
MF	What I am also hearing is that there should be a vision to increase the maturity of the IT, when moving to the cloud, ideally on all levels. You have mentioned IT operation factors, regulations, data security and also the size of a firm.
I-I-02	Absolutely, I think the classical roles will also evolve. They will still be monitoring the environment for anomalies and scanning it to ensure nothing is open for the public. The role of a security professional will evolve as the opportunity for the cloud platforms becomes more feasible. It is not that their work is going away because I also think that this is also a problem. I think there probably is a fear amongst the more legacy focused IT staff that they might become less relevant. On the contrary they are just evolving into a different environment and probably a multi-cloud environment. So how you manage security across that is not easy.
MF	I think you make a very good point with roles evolving. You often hear from more senior managers that they can reduce on resources because they do not have to maintain the infrastructure any longer. But you still need competent employees configuring your tenant. I think in the past there were enough examples where unintentional information disclosure was caused by a misconfigured tenant setup.
I-I-02	Yes, absolutely. I think it also changes your software development lifecycle to almost DevSecOps. So that security is built into the development process because software and infrastructure start to blur. It is a learning process for organisations, and one needs to be careful because it can also lead to problems.
MF	Thank you very much for your time.

Identifier	I-I-03	Generalised Job Title	Information Security Officer TPRM
Years of experience in IT	**Years of experience in cloud computing**	**Academic/Industry**	**Area of lecturing/Industry sector**
10	7	Industry	Financials

Key Messages:

- Third-Party risk management is concerned with identifying the right vendor, which will not put the organisation at risk.
- Questionnaires and interviews are the primary source of information for new vendor engagements.
- Automation of the TPRM assessment process would help to make it more efficient and robust.
- There are service providers, which specialize in TPRM analysis and provide intelligence for the process. Some cover all aspects of TPRM and some specialize in a certain area, e.g. a vendor's cyber security posture. These type of assessments provide more information compared to TPRM software like BitSight and SecurityScorecard but are also more expensive.
- There are also third parties, which do the TPRM risk assessment as a service.
- The first step of a new assessment is the triage, which is used to identify areas requiring an assessment. For example, cloud engagements will have added a section covering cloud services the overall questionnaire.
- A lack of control identified based on the questionnaire is further assessed for compensating controls and if it is actually a risk for the service consumer.
- The business needs to decide if the risk is acceptable considering their risk appetite.
- The TPRM process is identical for on-prem and cloud services. There are additional questionnaires covering the controls required for cloud.
- An event like a security breach of a vendor should trigger an assessment of the event and not a full TPRM assessment.
- Access management and encryption including key management are the topics which have an increased focus when it comes to cloud services
- There is also a risk of not using a new technology. This could lead to loss of market shares or bankruptcy.
- Sometimes there is no good option and you need to do business with a vendor, which is weak in information security. A mitigation measure could be to get them to use the service consumer's IT systems.
- Good, transparent collaboration during the assessment is important. This can be an indication that during a crisis, the third party also communicates openly and in a timely manner with their customers.
- A flat security policy, which considers global requirements, is better as it avoids onboarding services, which might be compliant in one region of the world but are not in another.

Who	Statement
MF	Where would you place your company in terms of cloud maturity? Maturity scale 1-6 (1 – very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent)
I-I-03	I do not know to be honest.
MF	What about TPRM maturity?
I-I-03	I think we are average. There are not too many different ways to do it. I would say we are a 5.
MF	What is required so that you would give a 6?

I-I-03	I think we would need more automation of the process. There are suppliers on the market, which sell you their assessment data. The approach most financials sector organisations take is to do everything on their own. So far, we collect data our selves through questionnaires and interviews. But, there is a good chance that somebody already assessed this vendor, and we could buy that data. We are using some of it today, but it is an expensive service, so we only use it when we assess critical vendors. But ideally, we would be able apply it to all of our assessments to improve the assessment framework.
MF	So do you mean services like BitSight and SecurityScorecard?
I-I-03	Yes, that is one type of service. However, these only provide you with data they get from scanning the vendor's infrastructure and collect publicly available information. But they cannot go into a vendor's network for example. There are other vendors who do full assessments and engage with the third parties and do the full due diligence. One of the vendors which is offering this is CyberGRX and they focus only on Cyber. Another one would be Truesight, which focus on all TPRM aspects. The depth of their cyber assessment is only high-level, compared to CyberGRX.
MF	This is really interesting. How would it work then when I wanted to introduce a new vendor? Do you reach out to them to get them to do an assessment or to provide the results of a previous assessment?
I-I-03	We first do a triage to find out what will the vendor do and what is the criticality of the service from an IT and also the overall perspective. If there is no IT dependency from the engagement, then we would not do an IT assessment. A good example for that are consulting services, when they do not work with our data. But if we exchange information like send data to a vendor or the vendor gets access to our IT systems then we do the assessment. There are different types of assessments, but we try to align them. We first send a questionnaire to the vendor which is tailored to the engagement based on the outcome of the triage. So, if a cloud service is used then there will be additional questions tailored to the usage of a cloud service which will be sent to the vendor. Once the vendor sends the answers back. Then a risk assessor is reviewing all the answers. The vendor has also the opportunity to explain things using free text fields. It is pretty easy to identify lack of controls based on the answers. The assessor discusses any findings with the vendor to understand if there are any compensating controls. For example if a vendor is not able to implement 2-factor authentication for access to our data then this would be against our expectations. Then we try to assess if it is a risk for us or not. This is depending on the level of data the vendor might have access to, or they have so sophisticated authentication mechanism which provides similar security like 2FA. And it is not always flat discussion which means it is different from vendor to vendor. Depending on the complexity we also do it over e-mail or more complex things over the phone. In the end we need to understand what the gap is and what is the risk for us including how likely is it to be exploited. In the end of the day all these findings will be put into the report. At the end of the assessment, we also have a discussion with the business and the vendor to discuss findings and identify risk mitigation measures. So, find out if the vendor can change or implement something to reduce or fully mitigate the risk. If anything can be done, then this will be reflected in the report. If not, then the business needs to answer the question if they are keen to accept the risk. So they need to understand what is their risk appetite. The discussion about the risk appetite is also an interesting story, this is the responsibility of the 2nd line of defence to discuss it with the business. Once discussed and agreed, the right people need to sign off on the engagement and the risk and the risks are added into the risk management tools.
MF	Who is helping with the risk assessments?

I-I-03	We outsourced the entire service to a third party.
MF	Do they consult then with internal IT security specialists when they have findings?
I-I-03	They have their own Cyber Security experts who are able to understand the basic security concepts and do the assessment. So far, we have not had a case where they asked to consult with somebody internal. Sometimes it happens in the engagement setup phase before the assessment. There are two types of engagements: the easy engagements where the business already know what they want to outsource, they discuss it with a vendor and when they know what they want to do, then the assessment is triggered. The more complex one, and the cloud outsourcing fall into this category, start with discussions to build a concept. Here an information security officer specialised in cloud services would be involved from the beginning. The information security officer would be involved in all the discussions with the business and the vendors to define the concept. Once the concept is finalised they draft the contract and put it into the TPRM system, which then triggers the assessment. It is also possible that the contract and the TPRM are done first and only then they do the concept, but it is not common.
MF	Are there any key differences between TPRM for a cloud service and a TPRM for an application hosted on-prem?
I-I-03	No, not at this level. Third-Party risk management is more concerned about collecting the right vendor which will not put our organisation at risk. It is not about an assessment of the IT product. In simple words if we would buy an application from a vendor then at the TPRM level we would assess things like: how does the vendor handle access management; what are the security processes; do they have security policies, security standards, independent certifications, roll-back plans, proper change management in the organisation; is the staff being trained. We want to ensure that they are mature when it comes to cyber security. We want to avoid buying things from vendor with poor security and poor controls in place. If they are not mature in cyber security they will cause problems at a later stage. We are more interested in this than the IT product itself. There are different assessments for that which are triggered after the TPRM is completed. For example if an application is installed in our network then it needs to be penetration tested first and go through a dedicated application assessment. For cloud we have a dedicated cloud assessment. So, for cloud services we still want to do a penetration test, but we also accept if the vendor has done one as long as it meets our security standard. Once you sign the contract you after the TPRM you cannot just install the application you then need to implement it as part of the project delivery framework which triggers additional assessments based on the type of application and data the application is handling. Otherwise, the application will not be added to the eco systems or firewalls will not be opened.
MF	To summarize, the information security risks are collected and assessed slightly when it comes to the service delivery model, on-prem vs. cloud but the process mostly overlaps, right?
I-I-03	Well, it is all about the controls. We follow the NIST control catalogue and depending on what you assess the controls are different. So, for cloud there are different controls applicable than for on-prem. For example, who is holding the keys for encryption? This question is only triggered for cloud services.
MF	Are there any other differences like that?
I-I-03	If you are interested, I can provide you the questions. The document is public as we send it to all vendors, regardless of whether we do business with them or not.
MF	Yes please. Are there different questionnaires, i.e., one for cloud and one for the rest?

I-I-03	In the past there were different questionnaires based on the triage questionnaires. But today we have one big one with various subsections, so if cloud is used then a subsection of questions regarding cloud needs to be answered.
MF	Do you also use event-based triggers for a third-party risk assessment? So, if there is news from a threat intelligence, for example.
I-I-03	Yes, we do, but it would then be event specific and not trigger a full assessment.
MF	Did you ever take any actions or even terminate because of such an event?
I-I-03	No, not as far as I know. We got lucky so far and did not have serious impact because of such events. When something like this happens, the vendor takes it very seriously and communicate openly with us. They provide us a report showing what happened, what the impact was, and which measures they implemented to prevent future incidents. We then do a risk assessment and if there is no further risk then we do not take any actions. But we record the incident and for a future risk assessment the likelihood factor for risk findings could be increased.
MF	How do you think risks change when services are moved from on-prem into the cloud?
I-I-03	As long as we keep the things in-house then we depend on our controls. If we depend on our controls, we feel secure. If move a service into the cloud, there is a dependency on the third party for all things which we do not control. In the finance sector enterprises have this way of thinking that when we are responsible for something than it is treated as it should be. If we have to hand it over to someone then we are not sure anymore. Public cloud is shared by multiple customers and something can happen. So, there is this additional layer of dependency which makes it less secure.
MF	Which additional risks do you discuss when things are moved to the public cloud?
I-I-03	When it comes to the control effectiveness then it is pretty much the same things. Sometimes a vendor is doing something better and sometimes they are worse. It is hard to generalise, and you probably need to go through the controls and see how the vendors perform.
MF	I am looking for key areas or talking point which get more weight, like key management which you have mentioned before?
I-I-03	I would say access management. This is a main challenge besides encryption.
MF	Which information security criteria do you see as distinguishing factors which somebody can use to decide if it is a good idea to move a service to the cloud?
I-I-03	The decision is not being taken on the IT Security level, because you would probably not go to the cloud. When there is a discussion about cloud outsourcing then in the project team there is also somebody from the CISO department participating in the discussion and advising on the Cyber Risk. There is also somebody from 2nd line of defence advising on the operational risk. They consider a lot of factors including the risk of not using new technology. Like for Kodak who did not invest into digital photography and had to declare bankruptcy.
MF	Were you ever involved in a case where the group advised against doing business with a 3rd party?
I-I-03	Yes, this happens. But it only happens from the cyber security perspective and the decision is with the business in the end. What needs to be taken into account is whether or not there is an alternative. It happens often with law firms. The standard law firm is generally small and only has one or a small number of lawyers. These firms usually do not well when it comes to information security, as they are a simple company. The big law firms on the market do much better. Now, because of the nature of what they do they have access to very sensitive data. As we are a global organisation, we need to do business with lawyers in the entire world and rely on services from law firms across the globe. Depending on the region, you sometimes do

	not find a big player in that market and rely on a small law firm. This sometimes creates problems as they do not have basic security in place but due to the lack of alternatives, you do not have much of a choice. From a cyber perspective we could onboard them to our IT systems and give them access to an internally hosted virtual machine as a mitigation measure. We do whatever we can to avoid sending data to them and rather have them working in our environment with our controls. If you look at the large security breaches caused by third party vendors in the last years some of them were caused by law firms, like the Panama papers. Here the law firms did very critical things, which were leaked to the public. When something like this happens then there is a discussion about what we can do. I experience the decisions are then to limit the scope of engagements or anonymize data before they are sent out or onboard the vendor to our IT system. I see these kinds of things happening every month. I do not remember that we ever terminated a contract, but we did not sign some contracts in the past because of the lack of cyber security controls. We also try to assess if it is easy or hard to work with a vendor on cyber security. If we have a vendor who is reluctant to disclose information or is not agreeing to implement mitigation controls then we highlight this to the business as a risk. During a crisis situation it is critical for us that we get information from the vendor and the behaviour during the assessment is being considered to assess how difficult it might be.
MF	Did you ever had to push back on any of the third parties due to regulations or legal requirements?
I-I-03	This would be later in the process. We do try to keep a flat security policy/ security controls requirement. So, hypothetically, if in APAC there would be a requirement to implement 2FA then we would also apply this to all other regions. With this, we want to avoid that a vendor might be compliant in one region a non-compliant in another. In addition, every legal entity has their own governance committee, which ensures compliance of a new vendor and the service with local and regional laws and regulations. Each committee has their own information security officer.
MF	Do you also do impact assessment of hypothetical scenarios? For example, if the data would be disclosed unintentionally.
I-I-03	Yes, something like this happens but from the business process perspective. They will need to do a disaster recovery assessment and one of the scenarios is unintentional data disclosure. This is also something which is done by 2nd line of defence. Another important aspect of TPRM is the requirement to have an exit strategy describing how to get out of an engagement. This also covers if they need to terminate an engagement and should include a checklist for the process.
MF	Thank you very much for your time and your replies.

Identifier	I-I-04	Generalised Job Title	Cyber Security Officer
Years of experience in IT	**Years of experience in cloud computing**	**Academic/Industry**	**Area of lecturing/Industry sector**
20	3	Industry	Financials

Key Messages:

- When it comes to cloud services, both the service consumers and the service providers are still on a learning curve. This does not mean that the three big CSPs (Azure, AWS and GCP) have not already reached a mature level. They already have several years of experience in public cloud, but they are learning more and more about the various regulatory requirements that the financial industry must comply with.
- It is useful to have questionnaires for the different cloud types (SaaS, IaaS, PaaS)
- Certifications or reports like SOC are an important source of information beside the application owner and the vendor.
- TPRM tools like BitSight or SecurityScorecard can be a useful source of information.
- The data collection and analysis process for the risk assessment should be automated as much as possible.
- Access management, data security (encryption & key management) and foreign authority are key areas, which need to be looked at when consuming a service from the cloud.
- The challenge with access management is not only with application access but also with administrative access to the underlying infrastructure, which is not necessarily under the control of a cloud service consumer.
- While there are shared responsibilities in the cloud the service consumer stays accountable towards regulators.
- There is always residual risk that the cloud service provider has some level of access to the customer's data and possibly even without the customer knowing.
- Cloud service customers should ensure that clauses are added to the contract to mitigate or reduce some of the residual risks.
- The large IaaS provider take security and the concerns of customers serious and have many competent IT security staff working on it. Smaller sized SaaS providers sometimes focus more on providing features than on security.
- SaaS services should be treated the same way as DMZ applications, which are facing the internet.
- SaaS services should be penetration tested on a regular basis.
- IaaS should be treated as an extension of an organisation's premise with some limited controls in between. If the Customer Public Cloud environment is considered as an extension of the organisation's premise, the corporate’s network boundary also shifts, which then must be protected in the same way as on-premises. If it is treated like a third party area the number of controls required to secure it will erase any benefits coming from using the cloud.
- SME organisations are more likely to benefit from an increased information security maturity from SaaS services. However, it is advisable that they get expert help to ensure the services are configured correctly especially for IaaS.

Who	Statement
MF	Where would you place your company in terms of cloud maturity? Maturity scale 1-6 (1 – very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent)
I-I-04	4.5
MF	What would be required to rate it as a 6?

I-I-04	I think we need to standardise our controls further, automate processes and ensure that we live a cloud security culture. We are still in an early stage of the whole cloud topic and still are in the learning curve.
MF	How did it evolve over the 3 years you have been working in this area?
I-I-04	It was very intense. We had a very steep learning curve from working with the IaaS cloud providers and it was interesting to see the differences between Microsoft, Google and Amazon. We took the lessons learned from each into the assessment of the others and were able to identify more and more the strengths and weaknesses of the individual cloud service providers. It also helped to improve our knowledge and our processes. At the beginning, the process was more learning by doing with the applications, which wanted to go to the cloud. The experiences made were useful to shape the process.
MF	How does the process look like on a high-level?
I-I-04	We have created questionnaires for all levels. One for IaaS which we used predominantly to assess the infrastructure of the cloud service provider. The same IaaS questionnaire we use for the so-called core foundation which is on top of the cloud provider from our perspective. The core foundation includes additional security controls which are managed centrally. We also have one for PaaS called PaaS minimal bar. It contains all requirements which we expect a PaaS to fulfil. We are also preparing one for internal applications which want to move to the public cloud. This contains questions which are cloud application specific. Additionally, we also have a questionnaire for SaaS applications. For SaaS we also ask about things on the cloud service provider side where also TPRM is playing a role and we look at how we integrate the SaaS into our environment. Covering things like how we connect to it, identity and access management, etc.
MF	Are you primarily triggered via the TPRM process?
I-I-04	So there are two trigger points, one is the TPRM and the other one is the project delivery framework. The focus of the TPRM is the cloud provider and from a CISO perspective we want to understand the maturity of the cloud service provider in terms of IT security, application development, etc. The project delivery framework triggers an assessment of the solution/service itself.
MF	Are you raising risks mainly through the questionnaire or do you also use other sources, like BitSight/SecurityScorecard?
I-I-04	The TPRM officer uses these tools. We are not going that deep yet for SaaS. We ask if they have a SOC report. For IaaS, so Microsoft, AWS and Google, we held meetings to dive into areas of interest. These were identified based on their replies to our questionnaire.
MF	Did you ever have findings where you said the risk is too high and we do not recommend this service from this vendor?
I-I-04	I do not recall having a case where we said the risk is too high. We did have risks where we said that a service cannot be used in the way we initially intended to. Mostly PaaS services and because they wanted to process confidential data. If they do not meet our requirements, then we tell them that they cannot use the service. The other option is to accept the risk, which also happens but only for medium risks, never high risks.
MF	How would you optimise the process today?
I-I-04	What we are looking into is to automate the assessment for applications. The objective is that the assessment is added to our risk management tool. The application owner then has to go through the questionnaire as part of a self-assessment. Based on the answers we should automatically see the risk gaps against which we then raise a risk action item. In case of a high risk or if there are questions from the application owner then he can ask questions through the tool. Today, we do

	everything manually without tool support. The other thing is that we also automate the deployment of services, for example with a template covering security aspects. This would help to restrict the application owner, for example, to open connections towards the internet. Microsoft offers some of these services. Google is more restrictive and provides a ring-fenced environment within a VPC, so the control is included. This is an example of a difference between cloud providers. If you can automate the deployment, you can also ensure that the baseline security is met.
MF	So, you use the vendor and the application owner as primary source of information or are there any other?
I-I-04	We use the information from BitSight. We also look at certifications or reports like SOC performed by security professionals of external parties, which the vendor has. On the other side, we also run regular penetration tests of our security controls with an external party.
MF	How do you think have information security risks changed when services run on-prem compared to run in the cloud?
I-I-04	When you are running an application on-prem with confidential data then we control everything. We can decide how the architecture is built and who has access to it. With access I not only mean who has access to the application so business users, but also which administrators have which access to the infrastructure. When you move to the cloud the topic of infrastructure access and security controls are a topic of shared responsibility. Some things are being taken care of by the cloud provider and some things are in the responsibility of the cloud service consumer. From a regulatory perspective while there is a shared responsibility, we are still fully accountable and need to control the cloud service provider. Also, from a risk perspective the large IaaS provider have good security controls in place which sometimes even are better than ours. Because they can use the latest technology and have a lot of great security people operating their cloud and support us. As part of the assessments, we identified that there is always residual risk. While the cloud service provider has great security controls in place and is providing these to their customers, there is always a risk that the cloud service provider still has access to the customer's data. Even if we encrypt it or implement other controls, there is still residual risk that the CSP has access to our data. As an example, in case of an incident then the CSP has an interest to resolve it as quickly as possible. So, it could be that the CSP is investigating and as part of that creating a memory dump of a system which is not encrypted. Another aspect is that when multiple CSP operators or multiple attackers on the CSP side would work together then it would also be possible to access data and exfiltrate it. The likelihood is very low, as the CSP also has controls and monitors the access to the infrastructure. The third point concerns "Foreign Authority", so the scenario in which a government entity requests access to data of an organisation. While this scenario has been discussed and CSPs try to be transparent about how this is handled, there is still a possibility that they are compelled to support such a request and that they are not allowed to inform us. These residual risks and also the controls which we require, for example, the option to monitor access of the CSP to our data, reporting in case of maintenance or incident which required access, etc. were included in our contract. In the contract we also defined that in a BAU case an CSP operator would never access our data unless there is an incident. Also, in case of a foreign authority requesting access to our data we have defined the procedure. If the CSP sticks to it is then a different question. But we can only mitigate or limit the impact of these residual risks through the contract.
MF	Is the data encrypted as part of the mitigation measures for some of these risks?
I-I-04	Yes, there is the possibility to use the default encryption of the cloud provider, where the CSP would generate and manage the keys. Then there is the possibility for us to

	generate the key in the key vault and store it in our hardware security module. This means that we then are responsible to manage it, so backup, key rotation, etc. Regulators are dictating to “bring your own key”. Meaning that we would generate the key on-prem and export it into the HSM of the cloud. In this case we know how the key was generated and that it was not generated using the keygen of the cloud provider. The keys can also be deleted and then the cloud provider cannot use the data either.
MF	If you think about the services, you have assessed which gave you a greater headache, SaaS or IaaS?
I-I-04	If I think about IaaS then I have less of a headache. We work intensively with the cloud provider. And of course, one can say if you work intensively then they have additional information especially about which data you send to their cloud and which controls your use. But a violation of that trust would require a great criminal energy, as those who work with us are not those operating the cloud. Obviously, this would also result in massive reputational damage for the CSP. The big three will do everything to avoid this. When it comes to SaaS however, you have sometimes a vendor putting functionality over security. They want to provide a good product with many features and then invest less into security. From my perspective, there comes bigger risk from smaller SaaS vendors. They obviously, also need to manage everything also if they use a IaaS cloud provider. And we are more restrictive depending on the type of data. In case they process our confidential data then we either want to be able to manage the encryption keys or in case of critical confidential data then we either tokenise, anonymise, or encrypt the data on our side before sending it into the cloud.
MF	Are there also other conditions coming out of the assessments? For example, that there needs to be a penetration test of the application?
I-I-04	Yes, we mandate penetration tests for all of our internet facing applications. For cloud services it can be that we do one or that the vendor provides us with the results of a recent penetration test performed by an external vendor.
MF	Meaning that you treat any SaaS like an on-prem application facing the internet?
I-I-04	Yes exactly. And it is also part of the TPRM questionnaire, how they treat their internet facing applications. In most cases the vendor performs penetration tests and then it does not make sense if we also do one. We then request the report and review it to ensure there are no high-risk findings and understand how they address the findings.
MF	Is there not a risk that these firms make the reports look nicer than it is in reality? Sort of a “Don't bite the hand that feeds you” scenario.
I-I-04	Could be yes, but if I look at the firms we work with, then I would say they would not do this. If we see for example that, the application has many findings in BitSight and the penetration test report is not reflecting this then we would insist to do a pen test with a firm of our choice.
MF	Do you also investigate cloud chaining? For example, if a SaaS is using AWS do you also verify how the vendor is using AWS.
I-I-04	No. With the TPRM we verify the software development procedure and the security controls used by the vendor. This gives us a view how mature the vendor is, but we would not look at specific configurations. When we work with Azure on our own then we also know that certain default controls will be there.
MF	Summarizing how the risk changes there are three main topics: access management also with focus on the access of third parties.
I-I-04	Yes access management includes the third party. We cannot monitor the access of the vendor. They need to provide us with the tools to enable us to monitor them. One

	also needs to check the SOC 2 reports to ensure that it was verified. In the end it is always also a matter of trust that they do what they claim to do.
MF	The second topic was data security, so encryption of data at rest, key management also falls under this topic
I-I-04	Yes exactly, we do not do that on the same level for our on-prem services
MF	The third one was foreign authority. So that there is a new risk that a government entity could gain access to data and even without that you are being informed.
I-I-04	Yes. One must consider that the three largest players are all US companies. Hence, there are a lot of request that data centers are also being built in our country. This would help that we can keep our data in country. The other interesting aspect is where the operators of the CSP are located. We did ask them, and they are dispersed across the globe. The cloud providers realise that this is an important topic for us an also other organisation.
MF	Do you think of IaaS as being an extension of your premise or do you treat it as a foreign environment?
I-I-04	We treat it as an extension of our premise, at least to a certain extend. We do implement controls between the two to monitor what is moving in and out, so we have a controlled perimeter. But we have not implemented DLP between on-prem and IaaS. I also believe that it should go into the direction of treating it as an extension of your premise. Because if you treat it as an external environment the number of controls required securing it properly will erase the benefits coming from using the cloud. The challenge is how to assess it. On one hand, we have the questionnaires and the due diligence we are doing and, in the end, there always needs to be a level of trust towards the CSP.
MF	Like you said in the beginning, most of it is still new and you still need to gain additional experience.
I-I-04	Yes, and everything is still developing. Maybe we will have security providers in the future which will help us to gain additional independence and/or better control of the cloud provider. We are still in an early stage of this journey and so are the CSPs, which too are still in a learning curve.
MF	What are key criteria which a firm can use to assess if there are benefits coming from moving a service to the cloud compared to hosting it on-prem?
I-I-04	You probably have to discuss this with the business. I cannot assess the financial benefits.
MF	I meant more the information security benefits.
I-I-04	I would say for any data which is not confidential there are a lot of services where it would be difficult to do it on-prem. Because on-prem you need to integrate with all the eco systems which is not always easy. Also, for machine learning and artificial intelligence services there are a lot of tools where you can build something quickly and which is powerful in the cloud. But as soon as confidential data is involved then there is a big overhead which has to be added to ensure security.
MF	From a security perspective, do you feel that organisations gain a security benefit from moving to the cloud?
I-I-04	I think the level of security is similar. One advantage is that in the cloud one benefits also from the CSP's security. So more modern controls for example. If we do something new internally there is a lot of development required and, in the cloud, you already have that out of the box. For example, infrastructure access, DDoS prevention, etc. this is being taken care of by the cloud provider.
MF	If you think about all types of organisations, so SMEs and large organisations, what would you recommend them in terms of criteria, which they could use to assess if it makes sense to go to the cloud?

I-I-04	It depends on what one wants to get out of it. A small company using a SaaS which meets their requirements then there is probably a lot of benefit compared to doing it themselves. IaaS on the other hand is probably more for medium or large size companies. One needs to have a certain maturity, as it is a lot of effort to maintain an IaaS. So smaller firms are probably better of using SaaS compared to the rest who can move large applications or outsource part of their data center to a cloud provider. Smaller firms probably need to work with a third party who helps them to run their IT or go to the cloud.
MF	Which ties back to the IT maturity of a firm and the IT security maturity, correct?
I-I-04	Yes, so smaller firms probably benefit from using SaaS. But when you have smaller firms which are not security-savvy then they will also not think about security when they start using a SaaS.
MF	Fair point in the end the customer is responsible to configure it. What do you think about laws and regulations as a criterion?
I-I-04	They also play a material role when it comes to what can go to the cloud and what cannot. I would welcome it if regulators would certify the large cloud service providers and approve their usage. Then you would have a certificate and know that they are safe to use. It would also be a selling point towards SMEs if the CSPs could show that the large banks and insurances are using their service.
MF	Thank you very much for your time.

Identifier	I-I-05	Generalised Job Title	Chief Information Security Officer
Years of experience in IT	**Years of experience in cloud computing**	**Academic/Industry**	**Area of lecturing/Industry sector**
14	2	Industry	Information Technology

Key Messages:

- To properly manage the cloud information security risk and even cloud engagements in general a firm needs to dedicate resources and invest into defining a cloud strategy, adapting existing risk management processes and defining the required controls.
- From an information security perspective, identity and access management and data security (encryption and key management) are focus areas.
- What data can be moved to the cloud depends mostly on the laws and regulations but also on an organisation's risk appetite.
- Data portability is an important topic which should be considered from the beginning to avoid vendor lock.
- The answers to the questionnaires provided by the service provider as well as the entity seeking to consume the service; and any certifications or reports the service provider provides are the main source of information for the risk assessment.
- Organisations without cloud and cloud security competency should consider engaging a competent third party to help them with the risk assessment.
- The lack of skilled resources is a major risk when going into the cloud as misconfigured cloud services are a key issue when it comes to unintentional data disclosure.
- Credential theft is a more complex issue in the cloud than on-prem due to the self-service aspect of the cloud and the associated pay-for-use billing model.
- Major challenges when it comes to cloud are to train the resources configuring the complex cloud services and to ensure being compliant with laws and regulations when data is crossing borders.
- While an SME can negotiate adding clauses like a "right to audit" to a contract with an SME cloud service provider, it is impossible to do so with the large CSPs.
- The "golden eggs" of a company should not be moved into the cloud.

Who	Statement
MF	Where would you place your company in terms of cloud maturity? Maturity scale 1-6 (1 – very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent)
I-I-05	I would say 4. For two years we have a managed cloud service strategy to position ourselves as a managed hybrid cloud service provider. With that we would like to offer managed services out of the hybrid-multi cloud environment to our customers. So far, we only offer services out of the private cloud. We know that we are moving to a bimodal IT model. So, on one side there is the traditional, stable, secure IT environment out of the private cloud. On the other side the public cloud should provide us with the agility, flexibility, and innovation, where required. Basically, the large, slow container ship vs. the speedboat. This meant that we had to think about how we want to build our managed services portfolio in the future. One aspect being cloud security, as the threat landscape compared to on-prem is different. There is some overlap for sure but there are also some which are exclusive to public cloud services. There are some public cloud services mostly SaaS which we or some of our customers consume. They are mostly also not integrated into our environment but

	standalone services with a limited number of users and without integration with existing systems. There we are looking to help our customers as IDP, so the whole topic about AzureAD and AzureAD synch. With our customers the focus lies on SaaS. The use cases for PaaS and IaaS do not exist yet. So right now, they are more concerned about Office 365 topics. Meaning they want to have their office or their teams from the cloud. From our perspective the most important topic is identity services. This to enable the customer to use the account he is using on-prem also for cloud services. So, identity federation and single sign-on using SAML or OpenID collect are key topics we are working on. Summarising when it comes to SaaS, I believe we are mature. But we have not had a lot of experience with PaaS or IaaS hence I think we are a 4 in terms of maturity.
MF	So, once you master these you would rate yourself as 6?
I-I-05	I do not believe anyone can ever be a 6. The whole environment is too dynamic, there are always new things. If you look at Microsoft's Azure cloud and the number of features, they constantly release, I think we would need much more people who work exclusively on these topics to achieve a 6.
MF	How did your maturity evolve over the last years?
I-I-05	I think 1-2 years ago we would have been a 2, max a 3. Everybody knew that the topic would come eventually. But due to other projects we were only able to start focusing on it in the last 1-2 three years. Since then, we have founded a cloud expert group and worked with an external partner to define our hybrid cloud strategy. From the strategy we then derived work packages and started to build the basis so that we are able to do the due diligence: This includes clarity about compliance requirements, how the risk management for cloud should look like, what are our data security requirements etc. We worked a lot in the last two years to define our baseline security for cloud.
MF	How do you assess information security risks of a new service?
I-I-05	I do not think there is a big difference in the methodology between assessing risks for services on-prem or the cloud. We still need to ensure that we cover the three-information security objectives: Confidentiality, Integrity and Availability. Some parameters in the risk assessment are different due to the different threat landscape. Typical topics are self-service, visibility, etc. which would be different than for services run on-prem.
MF	So how do you introduce a new service? For example, if a customer wants to introduce a new SaaS, is he then responsible for the risk assessment or are you doing this as part of the project?
I-I-05	This is a good question. We currently have 12 use cases describing how a customer can consume a service from us. 4 of them fall into the SaaS area. The first use case would be an existing customer for whom we host the identity, and he would consume the service through us, so we are the service broker. The customer has the contract with us, and we have the contract with the cloud service provider. The second use case would be that the customer is not an existing customer with his own IDP but is consuming the service over us as service broker. So again, they have the contract with us, and we have it with the cloud provider. The third use case covers the scenario of an existing customer who is directly contracting the SaaS. In this case we would provide the IDP and manage the interfaces between our environment and the SaaS. The last use case is similar to the third one. The customer is again an existing customer contracting the SaaS directly and we would manage the SaaS on their behalf. Then the customer has the contract with the cloud service provider and with us for the operation of the SaaS. For each use case the controls are slightly different. We have a list of 30 controls for any new service being evaluated. We also have a cloud privacy compliance check for which we do a workshop with the customer to

	review what data he wants to move to the cloud. There are also sector specific laws and regulations which require our customer to fill out a data protection assessment. We work with our customer to review the service; What kind of data they want to move to the cloud; Where is the data stored and where are they processed, e.g., in the same country or if it is in a different country do, they have similar data privacy laws; How is the data portability, so how easy is it to export the data. There are also other governance topics which we review like incident reporting of the cloud service provider; Is the CSP ISO 27001 or ISO 27018 certified; Does the CSP provide data around their operations, so that we can do a risk assessment; Do they provide DR plans? Furthermore, we also look at transition topics covering things like how does admin access work, is there integration into AzureAD or an IDP, are their any issues to apply our local access management in the cloud, how is the application managed, how is data managed, up to operational topics like who manages the applications, is it us, a third party or the customer. Another thing we look at is logging activities, especially audit logs. Also is the application penetration tested on a regular basis, do they describe their patching and update process, how do they increase capacity and how do they do DR testing. We try to apply all the things we do internally as part of our risk management to the cloud service.
MF	If I understand you correctly you have 2 primary sources of information: one is the customer and one is the cloud service provider and each is getting a different questionnaire, right?
I-I-05	Yes, correct. Usually, we do the full assessment together with our customers because they do not have a dedicated data privacy officer. This is where we add value for our customer. We support them with filling out the questionnaire and assessing the potential impact from a data privacy perspective. We also try to assess potentially interesting services for our customers in advance and create blueprints which we can provide to them in case they are interested. When they approach us, we can show them that it is safe to use this service from a compliance and regulatory perspective.
MF	As part of your impact analysis do you also consider worst case scenarios like unintentional disclosure?
I-I-05	No not on this level. What we do is a business impact analysis. So what is the system used for, what are the availability requirements and what is the impact of a service outage, what are the RTO RPO requirements, what is the impact if the system would be unavailable for a longer period.
MF	You also mentioned that you look at certifications, which is another source of information. Do you consider some certifications as a must have?
I-I-05	No, we do not have such requirements. Certifications impact the size of a questionnaire which we send to a service provider as part of our supplier risk management. If they are ISO 27001 certified, then there will be less questions which they have to answer.
MF	Is the questionnaire different if a service is using IaaS for their SaaS?
I-I-05	It depends on the cloud service provider. We do look at the large IaaS independently. We had a few risk assessments, and they vary heavily in terms of quality and material provided.
MF	Did you ever identify anything critical so far?
I-I-05	No not yet. But this is mostly because only uncritical data was involved. It will probably be different as soon as customers want to outsource core applications with sensitive information.
MF	Do you also use threat intelligence information as part of your assessment?
I-I-05	No, so far not.
MF	Where are the key differences in terms of information security risks between a service hosted on-prem and the cloud?

I-I-05	There are a few. There is the risk of exposure due to misconfigured services which resulted in exposed APIs or databases. The advantage of the self-service is also a risk. When credentials of a person with sufficient rights to deploy infrastructure in the cloud have been stolen, then they could deploy infrastructure, e.g., for crypto mining. This means that you will receive a big bill which can have a substantial impact.
MF	Are those risks caused by misconfiguration by the cloud service provider or is it more an internal risk of having uneducated personnel?
I-I-05	I think it is the latter. Meaning, one has to train its own staff, so that they can secure these things properly. The protection of the cloud identity is also important. If internal credentials are stolen, then this is not ideal but manageable and the impact can be limited. In case of a hybrid-cloud identity with single-sign access to all the services this is a different topic. Protecting this identity is definitely more important and mitigating measures can be two factor authentication or a risk based conditional access to cloud resources. Then the next topic is regulations and legal requirements which are not fully clear. Each canton has its own set of laws and regulations and it is difficult to navigate through it and comply with all. For example, if one of our customers wants to move to the cloud the requirements range from: if the cloud service provider has a similar data protection than we have in our country then it is ok; over differentiation between the type of data; to strict requirements towards key management. So, it is very difficult to ensure that the service is compliant with all the laws and can be used by all our customers.
MF	Are you ensuring that the data needs to stay in-country or are you okay to have them sent to for example the U.S.?
I-I-05	We have created a matrix helping us to determine – based on the data type (privacy, confidentiality) and data volume – if a particular case can be hosted in a foreign country and which could also be stored out of country. In case of confidential data, we tell our customers that they cannot host the data out of country and even that they should not move such data to the public cloud. The risk of an incident is simply too high. If the customer has the contract with the service provider, then we can only provide our recommendations. If they do something against our recommendation, then they need to sign a risk acceptance confirming that he is conscious of the risk. When we select services for which we act as broker then we ensure that they comply with our recommendations otherwise we would not onboard them to our portfolio. Going back to the risks, I think there is also a financial risk. It is a common say that one advantage of cloud is cost transparency and that one only pays what he consumes. I do agree with this, but we have made the experience that as soon as one requires a customization of a service it gets really expensive. Another topic is data control. We see this with the usage of the office services. While the cloud provider guarantees that the service and the customer's tenant is running in-country or a specific region, in the end, one cannot be sure that none of the log data, backups, archive data or meta data are being sent cross-border. They could be sent to the U.S. for data analysis purposes, and nobody is providing guarantees that confidentiality is ensured if this happens. This could be mitigated by encrypting the data with an own independent encryption solution which would encrypt the data before it is stored for example on Sharepoint Online. The downside of this is that some of the features of the platform could not be used anymore. Another thing is that the complexity of the public cloud is not to be underestimated. One cloud selling point is the high availability but there have been cases of outages. MS Teams was down for a few hours last week. Moreover, with the whole consumption of cloud services over the internet, the WAN connection becomes increasingly important. If there is an outage of the WAN then one loses access to all the cloud services. Lastly, there is the lack of visibility and

	control. The service consumer has no visibility of the cloud architecture or procedures of the cloud service provider. It is always “take it as is or leave it”.
MF	That is where you depend on the certifications and pen test reports which they provide you.
I-I-05	Yes, especially with the big cloud providers. Consuming the service happens on their terms. We do have smaller third parties where we put in a clause which gives us the right to audit them. With the large cloud providers there is no chance to do this. The only thing you get are the ISO27001 reports and maybe attestation of ISAE 3402 and you just must live with this.
MF	You talked about data security. For IaaS you could also encrypt the data yourself or you could use an external key management service. Is this something you discuss?
I-I-05	Yes, this is a topic, but it is still in an early stage. We are looking into installing a Hardware Security Module in our on-prem data center to do key management on-prem and encrypt data in the public cloud.
MF	What are distinguishing criteria to determine if a service can or should be moved to the cloud or if it should be run on-prem?
I-I-05	Primarily, this comes down to legal and regulatory requirements. If the laws do not allow to move certain data to the cloud, then we cannot. We also need to do our due diligence and proper risk management on the data going to the cloud. This as a foundation to take the decision then if the data can be moved to the cloud. For us as a managed service provider it is a “make or buy” decision. This is definitely the case for a lot of SaaS services. In general, I see an advantage in all the security features which the large cloud providers provide to their service consumers out of the box or for a premium. However, the downside of this that you need somebody who understands this massive security platform and understands all the settings. We are currently seeing this with Office365. There are tons of security features, like encryption, Web Application Firewall, Data Leak Prevention, etc. all of these need to be reviewed, a baseline needs to be defined and then need to be maintained. For us it is both a big benefit and a curse.
MF	What you are saying is that while the big cloud providers are definitely better in security than an SME company. However, to fully leverage all the advantages the SMEs need to have the staff to handle it. Not that you end up having a misconfigured environment which worst case opens it up to the public. Which is something which is less likely to happen on-prem because the staff is already familiar with the environment.
I-I-05	Yes exactly. Typical non-info sec criteria are scalability and costs to move a service to the cloud. One advantage is that because deployment is easy and the global presence of the cloud providers, a service can be made available easily from anywhere in the world. Which is also a risk, if the service is not configured properly or a cloud identity gets compromised then this increases the risk. Which is why when there is confidential data, so the golden eggs of our customers, we advise our customers to not move it into the public cloud. The risk is just too high.
MF	There are other IT operation advantages which are proclaimed by the cloud model. One being that you do not need to take care about backup and restore anymore.
I-I-05	I only partially agree with this. We have a client which is using O365 services and yes Microsoft guarantees resiliency and backup. What they do not guarantee though is disaster recovery. Meaning that one needs to ensure that the data is also backed-up to another location to be able to restore it. In the end it comes down how one assesses the risk. If a firm is moving their core systems to the cloud, I would not rely on the cloud provider to do everything.
MF	And with SaaS you also have the issue of bankruptcy.

I-I-05	Yes. You also have the issue of data portability. The cloud provider is not interested in enabling you to get your data out of the cloud easily. I think this will become a complex problem once the “cloud first” hype is cooling down and organisations want to move some of the services back on-prem. How do you get the data out of the cloud if at all? Microsoft 365 is a good example, the services are heavily interconnected, if you store a file in Teams which is based on Sharepoint online which is using OneDrive. I do not think it will be possible to get the data out in the same structured way as they are currently stored.
MF	What would you recommend a small organisation regarding cloud? Would you advise them to move to the cloud or rather buy a NAS and run it, for example, in the small grocery store?
I-I-05	It depends, it can make sense for a small grocery store to consume a SaaS. As long as they think about the risks, the data they put in the cloud and if they can handle it. If they for example know a guy who has an IT background, and they ask him to setup a NAS and maybe a Windows server then I am not sure that this is better than consuming a service from the cloud. I think it is important that if somebody is going to the cloud that they do not rush things but do a proper evaluation of the service providers. Including looking into how they do information security management.
MF	What you are saying is that one should not underestimate the level of knowledge the staff requires to move services securely into the cloud. Is this true because you are trying to do complex things, or would you say this is true for every cloud service?
I-I-05	Yes, I think this is true for all services. The data owner is always accountable for the data. In case of an incident the data owner cannot just point to the cloud service provider. Because the data owner is always responsible for the risk management and ensuring that the data storage is compliant with law and regulations. Which is why I think that cloud service brokers are very important. Even though there is a small additional cost, the service consumer then has somebody ensuring a security baseline, regularly checking the configuration, monitoring the service and reporting on it.
MF	Do you think the whole cloud security topic has helped to improve the maturity of your risk management process? Or did you just take what you have had and applied it to cloud assessments?
I-I-05	The latter, I do not think the process has changed a lot. We just consider different aspects and threats which are cloud specific in the assessment.
MF	Thank you very much for your time.

Identifier	I-I-06	Generalised Job Title	Chief Information Security Officer
Years of experience in IT	**Years of experience in cloud computing**	**Academic/Industry**	**Area of lecturing/Industry sector**
25	12	Industry	Industrials

Key Messages:

- An organisation should understand which services they want to and which services they actually can consume as a cloud service.
- Checklists and questionnaires are a primary source of information.
- Multiple checklists and questionnaires should be used. For example, one with the must-have requirements to narrow down the number of potential cloud service providers.
- It is important to have the right to audit your cloud service providers
- Certifications and audit reports by independent external auditors are a useful source of information and also how frequently they are done.
- Large cloud service providers are generally less flexible and take a take-it-or-leave-it position towards customers.
- Critical applications should not be run in the cloud.
- The information security risk assessment should be redone on a regular basis or in case of a major event like a data breach.
- The criticality of an application should be assessed not only based on the classical information security areas: criticality, availability and integrity. The business impact, data criticality, number of interfaces to other systems should also be considered.
- The size of the risk assessment should be adapted based on the criticality of a service. Critical services should get a more thorough review.
- Worst-case impact assessments should be performed, and mitigation measures should be implemented accordingly.
- It is important that the tools used for the ISMS are meet the needs of the users and are used in the way they are intended to be used.
- It vendor risk management tools like Risk Methods, are providing useful information.
- Legal aspects, business impact, data location, number of interfaces and know-how are key focus areas when a service is moved to the cloud. These can also be distinguishing criteria whether a service can be moved to the cloud or not.
- Retention of know-how to be able to move a service to a different provider or back on-prem is an important aspect which is often not considered.
- Running a thorough information security risk assessment process which is repeated on a regular basis is very resource intensive for large organisations which consume a lot of different services.
- Consuming a cloud service can also lead to an increased information security maturity because they provide certain controls out of the box.
- If an organisation's core business is not depending on IT then consuming cloud services can increase the information security maturity. This is also true for organisation with business processes depending on IT however extended due diligence is required in such cases. Regardless, it is important that an organisation has the required level of know-how to configure the services correctly.
- Outsourcing a process without understanding it usually results in failure.

Who	Statement

MF	Where would you place your company in terms of cloud maturity? Maturity scale 1-6 (1 – very poor; 2 – poor; 3 – insufficient; 4 – sufficient; 5 – good; 6 – excellent)
I-I-06	Based on our experience I would rate us as 5. There are some new services we are looking at like for example Amazon Cloud, which we approach differently. For these we get specific services and do something on top of it ourselves. Here we might be a bit lower, as this is new for both us and the cloud service providers. Though, overall, we are definitely around a 5 rating.
MF	What is missing so you would rate yourself as 6?
I-I-06	From my perspective we need to improve our service monitoring capabilities. I think we are good regarding the bidding process, service ordering and service operations. We can improve our service availability monitoring, so when is a service and its parts available. Furthermore, we can also improve on service forensics and service disruptions. I think these are the areas where we are not yet where we should be.
MF	How did your maturity evolve over the last years?
I-I-06	In the first ten years after 2000s we focused on full outsourcings. So, from entire application landscapes, over housing types of engagements to entire services which were provided by a handful of large providers. The first few years were hard, and we were on a steep learning curve until the first contracts were renewed. The lessons learned influenced then the renewal of the contracts: what worked well and what needs to be done differently. This was the first big maturity increase. Starting 2010 until 2015 we started to look into the different cloud service offerings and the new sourcing models. Understanding how far we want to and how far can we go as organisation was the second big step forward. Key topics were, what is required for the change, what are relevant laws and regulations not only from a national but also a European perspective. From 2015 onwards we also faced evolving scalability and service delivery requirements which required us to re-think our contractual and service delivery location requirements. As an organisation which is close to the government, we have to follow the public tender process and fill the requirements.
MF	How heavily are you influenced by the government's requirements?
I-I-06	Not a lot. The requirements are more around how strictly we have to follow the public tender process. The more something is "service public" the stricter we have to follow this for the full service. We are not allowed split projects or do one after the other. Meaning, we always need to understand the full project from the beginning. This is very difficult and a challenge which has become even greater with the new service delivery models like DevOps and agile project management methods.
MF	Are there also information security requirements included in the tender process? If yes, how specific are these?
I-I-06	Yes, there are some regulatory requirements, but they are not very specific. There are more high-level requirements, for example an organisation needs to have an ISMS. For certain services it is mandatory to deliver them with a specific level of security which also impacts the production.
MF	How should information security risks be raised and assessed for new third-party services?
I-I-06	We use checklists which depend on the financial size of the project and the service. These checklists are sent to the potential service providers as part of the pre-selection phase. They include our information security requirements which need to be fulfilled. If they do, they are admitted to the next phase of the bidding process which allows them to send an offer. Based on the offer they are also required to accept our contract amendments which define service delivery aspects and defines their responsibility further. Here they need to proof that they are able to fulfil the requirements defined in our contract amendments. Lately, we have also started to verify how the service is delivered. With cloud service providers we have a master

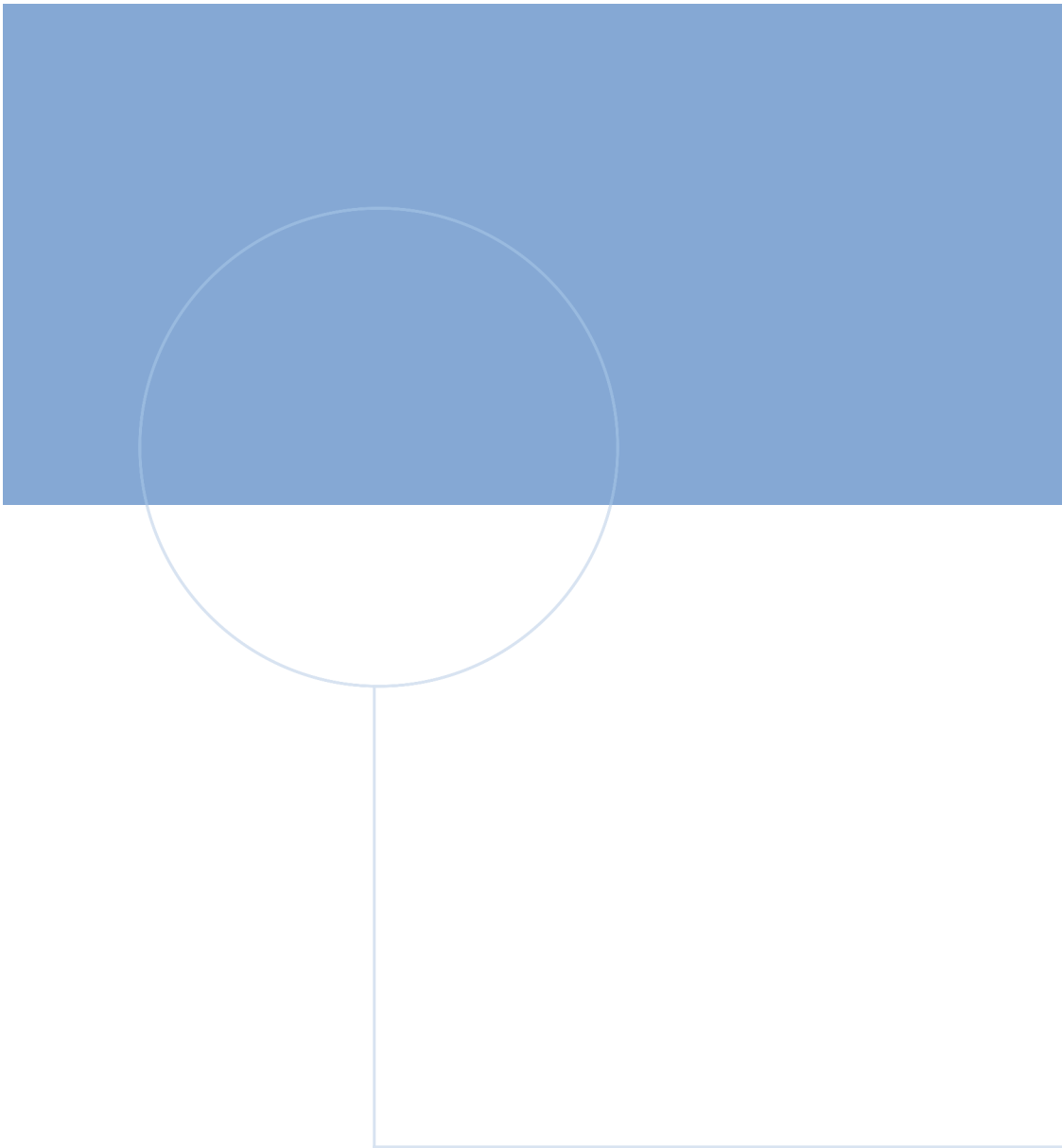
	agreement. Based on this there is then a further contract per service. As part of this we define the individual service reporting, delivery, information security requirements, etc.
MF	You use these checklists / questionnaires as an initial source of information?
I-I-06	Yes correct. We also review audits done by external auditors. If they are disclosed, then we do not verify aspects which have already been covered. But the report must be done by an independent external organisation, we would not accept internal reports. The process is not ideal yet, it would be good if we could automize random testing of certain aspects as a safeguard. We also observe that with our established key providers these processes work very well. With newer providers and with the large providers it is more difficult. Especially, large providers struggle to accept our requirements and are generally less flexible. They have their standard contracts and are mostly not willing to accept special requirements from individual customers. They do advertise that they have higher information security but when you look into it with an audit – I always add the right to audit to a contract – then we observe that high flexibility comes with reduced information security. It is still on an ok level but not as good as advertised. Moreover, very large providers, like Amazon, they have a take-it-or-leave it approach and we are not able to discuss things with them. Consequently, this also means that we would not consider working with such providers or only with a reduced scope. Meaning, that we would not run critical applications or applications with critical data on them. This strategy enables us to profit from cheaper services but at the same time be very conscious about which services are consumed as a cloud service.
MF	Do you run all cloud services through that process? So, large IaaS like Google cloud and also small SaaS which are only used by one team?
I-I-06	Yes, we do.
MF	You also mentioned that you use certifications and reports from auditors. Do you use only standardised reports like ISO 27001 or SOC, or do you also request penetration test reports? Also, if they do not have a penetration test report do you run one yourself?
I-I-06	Both. In a first phase we focus on basic standards like ISO 27001. Do they have a sense for information security? Are they able to manage information security internally and also for customer services? We also request industry certifications, if available. We review the material provided and then ask follow-up questions in case we have any. In case the independent audits do not cover all aspects, which are important to us then we run one ourselves. The outcome is then compared with the provided material to ensure everything is covered. If we are satisfied, we would trust this service for 3-5 years. After this time period we would re-do the exercise. In case, we are not satisfied then we would follow an internal audit plan, based on which we review certain topics from time to time. This can include penetration tests, software code review, etc. Summarising, we definitely do both. We prefer cloud service providers to hire an independent third party to audit their services and to create standardised audit reports. This simplifies our efforts for the review. After a few years we will check with the service providers if they have newer reports which still cover all the services. This to ensure that they are not missing anything.
MF	Are the follow-ups you mentioned done using questionnaires or do you conduct interviews?
I-I-06	We do both. For smaller non-critical services which can be unavailable for some time, we do it with a lower frequency. We do have a good overview of our application and platform inventory. We use this to assess the criticality of the service based on the business impact, data criticality, number of interfaces to other systems, etc. In case of a critical service this a more thorough risk assessment is triggered.

MF	Not only involving the cloud service provider but also the internal business unit which is seeking to consume the service?
I-I-06	Yes, exactly and this is independent of a cloud service. It happens for each application.
MF	Are you also doing worst-case impact assessments for cloud services, for example unintentional data disclosure?
I-I-06	Yes. We also check which services need to be available in a crisis. For example, our incident management platform is a SaaS service. Especially in a crisis situation it is important to have access to the incident management platform to track and update the incidents. If the access is using the standard internet link, then we have a problem if our link has an issue. If we think about these things, we also reflect upon the architecture. In this case we decided to have dedicated direct lines into the cloud service provider's data center which we manage to mitigate this risk.
MF	Do you have any other sources of information which you use for the assessment?
I-I-06	We do have our ISMS which integrates with different modules which feed different types of information into our system. Things like guidelines from the cloud security alliance or from other firms are fed into the system. We then list them as controls and filter and customise them based on our needs. For the findings management we have a different tool. We have a separate DMS for critical things in case we want to be independent of a cloud. So, in case of an incident the data would be available, maybe not in the same form but at least we can access the information. We try to build everything based on our needs using matching modules. Similar to a large carpenter's shop. You would not use a saw to nail something. Which is why we say we need a general management system for everything but for the specific tasks we need the right tools and not use a saw to hit a nail. Different service delivery models, on-prem, cloud, etc. require different tools.
MF	Do you also use IT vendor risk management tools which rate the vendor based on publicly available information?
I-I-06	Yes, we use tools like this. Some also as a Service. We also have our own Cyber Defense Center with a separate Security Operations Center. We also have a team which is doing penetration testing, red teaming, etc. We have our own vulnerability management team which is also scanning provider systems. Depending on the model we also introduce system monitoring tools which give us visibility about the patch level, what data is transmitted to these systems, etc. We are still developing this, especially with the adoption of cloud we had to change a few things. But we have a four-year program which is now at half time, so we are still on our way.
MF	Do you prefer internal capabilities rather than getting external services providers to help with third-party risk assessments?
I-I-06	Both. We do use risk methods for example and also other platforms to do an initial assessment. Risk methods is providing us a view about the vendor, which risks do they have, have they been on the news, have they been mentioned in the darknet, etc. This we then use to plan additional measures, like a vulnerability scan, using different tools. These measures can be executed by an internal team or bought as a service. If the delivery is standardised, then we would consider buying it as a service. If it is close to our business process which requires special know-how, then we would do it internally.
MF	Based on your experience, how do risks change when a service is moved from on-prem to cloud?
I-I-06	I would say the overall risk exposure between the classical models did not increase or change much. They are a bit different and have shifted. In the classical model they systems were on-prem and a bit closer. With cloud services the perimeter has been extended a little. Services run out of another country or M365 somewhere in Europe. We do know where and how they run and in which data center. We had to fix the

	locations as we have a legal obligation to know where it is running. This has changed. Can we consume a service from a different country? For example, from Russia what is the legal situation there? Is the country part of the European Union and thus falling under GDPR? What is the political situation of the state, are they open or not? These are all things we need to think about. And we need to be clear about our strategy, what can we as an organisation close to the government allow ourselves? Are we forced to do something because of a vendor's strategy? For example, M365 we do not need to think about other solutions because I doubt that there will be a possibility to run it on-prem in five years' time. So, an organisation does not need to think about if they accept that or not because of the lack of alternatives. Thus, it is really difficult to talk about if we want to take the risk or not. The second area of risk is about the production of the software. Where and how is it produced? In which form can we accept it? Do we need to ensure data storage in country? We can process data in M365 and store it in-country in case they are critical or confidential. Thus, there are strategic considerations which is a risk assessment based on the reputation of the service provider, costs, is it doable?, latency, etc. The next step then is to clarify which partners can be considered? Only European or can we look globally? This is the production level. After that we look at the service level to decide which type of service we consume, SaaS, PaaS or IaaS. How far do we want to go? As part of the last stage, we look at how it is produced.
MF	You mentioned the data location as one of the focus areas. Are there any other areas which became more important regarding cloud services?
I-I-06	Legal topics, business impact, so if something happens, how bad is it for us, and the third aspect is know-how. How bad is it if, over time, we loose know-how because we lack visibility of how things work in detail and only manage the outcome of a service, Legal topics include: location, contracts, dependencies to states and other requirements like how it is produced (low cost countries, child labour, etc.). The second aspect includes the architecture, location and the business impact. The third aspect is then the know-how. How much know-how do we need to retain to be able to do a new RFI/RFP in the future? How much know-how do we need to take a service back on-prem and operate it ourselves? Do we find the know-how in the market and can we afford it?
MF	I am surprised a little bit, as the other participants all mentioned data security with encryption. Did you not mention this because it is not part of the focus or is it regardless of the service delivery model, cloud and on-prem, a top topic?
I-I-06	This is indeed a top topic in general. It depends on the classification of an application. We thought a lot about which risk is higher: operate our own key management and potentially run into an issue because the provider cannot restore data because he has no access to the key. Opposed to the risk that the provider has they key with limited access to it. Which also requires additional audits to ensure the provider is managing the access to the key correctly. We want to see who has access to it, who accessed it in the past, who used it and when was it used, etc. This is then reviewed on a regular basis and is a different mechanism compared to when we have our own PKI and deliver the key. If something is going wrong things might get difficult. It also means that our teams need to be ready 24/7 to provide the key. So, for us it is a case-by-case decision which way we go. Applications with a high criticality are not allowed to go to the cloud anyway. The application data classification prevents this automatically.
MF	Are you assessing this case by case or do you have a set of requirements which you use to map it then to the key management case?
I-I-06	Both. On the main level we do the mapping. But because we sometimes consume different services from a provider, we bundle them and assign the same strategy. So, for example all SaaS services in a specific area have setup X. This simplifies things for

	us. Of course, sometimes there are then more security requirements than necessary for a service.
MF	Is this mainly driven from the data confidentiality perspective or also availability and integrity?
I-I-06	From all three perspectives. We always use multiple dimensions to classify a service. These include the classical information security dimensions confidentiality, availability and integrity, and also acceptable downtime, 1 hours, 3 hours, 5 hours, etc. Business impact which is using five different categories to specify it. This then influences which architecture types, cloud solutions, etc can even be considered for such an application.
MF	So one can summarise, the more critical the service the higher the possibility that it must be run on-prem?
I-I-06	The closer it is to our business process the more we do internally. Commodity solutions are outsourced more often.
MF	Is this true for applications or also infrastructure?
I-I-06	For both. We also verify that the overall architecture meets our requirements. So if we say that we want to do the infrastructure ourselves and we do not care about the application on top of it. This was one of the bigger mistakes we made in the early days. We only looked at the applications and then realised that they do not have the know-how of running infrastructure. So, they are excellent with application development and operations, but they lack skills to operate the infrastructure. This led to issues and even outages. So, we try to look at this holistically and while the application might be great but the infrastructure not some much. This is obviously more complicated, and we try to look at the whole architecture and to ensure that we consume similar services in the same way. If we consume it as a service, then we do not care where it is running on. SaaS or PaaS then we just need the platform to be ready and the rest we do then ourselves.
MF	Which key criteria do you see as distinguishing factors helping to estimate if it makes sense for a firm to consume a cloud service or host something on-pre? You already mentioned legal topics. Do you see any other criteria?
I-I-06	We mostly focus on the mentioned topics: so legal dependencies, architectural dependencies and know-how. Know-How has become an increasingly important topic to support the exit strategy and bring something back on-prem. Dependencies and interfaces is also a big factor. How many need to access the application and how many interfaces to other systems exist?
MF	So, when there are too many interfaces you would just do it yourselves?
I-I-06	Exactly, if there are so many interfaces required or accesses across different locations then we review it from an architectural perspective to ensure it makes sense. If it the handling of all the interfaces is more complex than running the service in our data centers then we decide not to consume the cloud service. Or we look if it is possible to only consume a partial aspect as a cloud service to reduce the complexity of the interfaces.
MF	Did you ever veto a service because the risk was too high?
I-I-06	Yes, we did have such cases. For business-critical services we ask our teams to do a pilot of a new service. We have had cases where everything checked out theoretically and then during the pilot, we discovered issues. We have a lot of data with a low confidentiality rating. In many cases data availability is much more important and low latency is a key requirement. Issues related to latency only became apparent during a pilot operation of the service. We had a lot of cases where we discovered issues because the service run somewhere on the Amazon cloud and we did not get the data in time.

MF	Do you also look at cloud chaining so where a service is running, or do you only look at the SaaS itself?
I-I-06	Yes, we did in the past. But we have so many applications which are running already and a limited time frame for our assessments. Meaning sometimes we are not able to go as deep and have to prioritise more critical services over lower criticality services. Additionally, sometimes we even struggle to do the regular reviews of services in time. Services with lower criticality are usually pushed back due to lack of resources.
MF	Do you also do event-based assessments? E.g., if one of your vendor's has a data breach.
I-I-06	Yes, as mentioned we use two to three platforms which alert us in case of such issues. Then we look at the details which are provided by the tools and the cloud service providers. This information is sent to our specialists in the cyber defence center which investigate the history and monitor the service.
MF	Was a decision ever influenced by threat intelligence information or even initiate an exit of a service?
I-I-06	No, we never exited a service because of an event. We did have cases where we added requirements based on events to a tender. If the existing provider did not meet the requirements, then we would choose somebody who did. For critical services we always choose two service providers. If one is causing us issues, then we just move the service to the other provider. This gives us the required leverage to influence service providers.
MF	Did you also have cases where your information security maturity increased from consuming a cloud service?
I-I-06	Yes, we did. We struggled to implement some security services which the cloud service provider delivered out of the box and not even optional. So for example by default you get DDoS protection or anti-virus on all systems which cannot be disabled. Internally we do have it sometimes that the anti-virus gets deactivated to gain additional performance. So, it is great that some things are just there when you go to the cloud.
MF	Would you recommend an SME organisation to go to the cloud because it increases their information security maturity?
I-I-06	I think it depends on the organisation. If the core business processes of an organisation are not dependent on IT then it makes sense to consume services from the cloud. If there is a big dependency on IT then I would still recommend it. But it is much more important to do the due diligence around it: how do I set it up? with whom can I work with? how much know-how do I need to have to manage it properly? So, it depends on how big the dependency of the business process on IT is. On a similar thought, OT and IT are getting closer and closer. As an industrials sector organisation, it is important to ensure compatibility with the OT environment if a service is consumed out of the cloud. You can consume the controller function out of the cloud but if the connection of the OT environment gets overly complex then I would not do it. I would recommend any company to build it themselves first. Because you can only efficiently outsource a service to the cloud if you understand the process perfectly. If you think you can move something to the cloud other than a commodity service, which you do not fully understand then it usually fails.
MF	Yes agree. It also means that an organisation needs to have the skills in the IT to configure cloud services correctly.
I-I-06	Yes, exactly.
MF	Thank you very much for your time



NTNU

Norwegian University of
Science and Technology