Protecting Enterprise Data in the Cloud

Thomas Vandermarliere

Supervisor: Prof. dr. ir. Jan Devos
Counsellor: dhr. Chris Kappler (PWC)

Master's dissertation submitted in order to obtain the academic degree of
Master of Science in de industriële wetenschappen: elektronica-ICT

Department of Industrial Management
Chair: Prof. dr. El-Houssaine Aghezzaf
Faculty of Engineering and Architecture
Academic year 2015-2016

UNIVERSITEIT
GENT

Protecting Enterprise Data in the Cloud

Thomas Vandermarliere

Supervisor: Prof. dr. ir. Jan Devos
Counsellor: dhr. Chris Kappler (PWC)

Master's dissertation submitted in order to obtain the academic degree of
Master of Science in de industriële wetenschappen: elektronica-ICT

Department of Industrial Management
Chair: Prof. dr. El-Houssaine Aghezzaf
Faculty of Engineering and Architecture
Academic year 2015-2016

UNIVERSITEIT
GENT

(14 January 2016)

Preface

The goal of my thesis was to combine IT security with my major Cloud Computing. As the subjects offered by the University did not match with my interests, I decided to search for a company who was willing to support me. This search started at the Howest Job Fair in 2015. After sending many emails, two companies gave me the opportunity to work on a thesis together: Cevi NV and PricewaterhouseCoopers (PwC). I decided to go for PwC because I had no prior experience with a company of that size. Even although I did not choose for Cevi NV, I would really like to thank them for offering me the opportunity.

At PwC I was given a lot of freedom in choosing the subject of my thesis. During my research, I got a lot of support. They offered me an office, free coffee and a laptop, but most importantly, experienced, smart and friendly people who were always available to help me. My thanks go out to everyone at PwC who helped me.

First of all special thanks to Chris Kappler for taking time to guide me. Your constructive and detailed feedback has been a great help in writing this thesis.

Also special thanks to: Vincent Haerinck for introducing me to PwC, Kris Boulez for arranging everything and taking time to support me during Chris Kappler's absence and Bram Verdegem who helped me to understand risk assessments better.

I would also like to thank my promotor, prof. Jan Devos, for guiding and supporting me.

Last but certainly not least, I would like to thank my family and friends. I am not able to find the words that can express my gratitude for their support, love, happiness and so much more. Special thanks to my mom Sandra Renders and my dad Dirk Vandermarliere for being awesome parents and for their financial and moral support in everything I have done. Also special thanks to my grandma Suzanne Mini for doing my laundry every weekend during my time as a student.

Ghent, January 2016
Thomas Vandermarliere

Dutch abstract

Protecting Enterprise Data in the Cloud
Bescherming van bedrijfsgegevens in de Cloud

Thomas Vandermarliere

Promotor: Prof. dr. ir. Jan Devos
Begeleider: dhr. Chris Kappler (PWC)

Beschrijving

Deze thesis probeert antwoord te geven op volgende vier vragen. Hoe eenvoudig is het om data te stelen van publieke Software as a Service (SaaS) oplossingen? Wat is het risico van een datalek? Hoe kan een bedrijf zich hiertegen beschermen? Wat kan en moet een bedrijf doen in het geval van een datalek?

Twee use cases worden gebruikt om op een realistische wijze een risicoanalyse te maken over het gebruik van publieke SaaS in een grote onderneming. Een derde use case is toegevoegd om het minder zichtbare risico van de zogenaamde Shadow-IT aan te tonen.

Op basis van een selectie bedreigingen specifiek voor publieke SaaS wordt een risicoanalyse uitgevoerd. Deze risicoanalyse gebruikt een kwalitatieve aanpak om de risico’s te bepalen op basis van de waarschijnlijkheid en de impact van de verschillende bedreigingen.

Aan de hand van de gevonden risico’s worden oplossingen beschreven om deze risico’s te verlagen. Elke opgegeven bedreiging wordt gekoppeld aan een mogelijke oplossing voor de specifieke use cases.

De thesis sluit af met verschillende opties voor een bedrijf om te reageren op een datalek.

Protecting enterprise data in the Cloud

Thomas Vandermarliere
Supervisors: Prof. dr. ir Jan Devos, Dhr. Chris Kappler
Ghent University Campus Kortrijk, Belgium

***Abstract*— This thesis focusses on the issues with public Software as a Service (SaaS) for enterprises. A risk assessment is made on the use of public Cloud SaaS in an enterprise. The two main threats considered in the risk assessment are data breaches and data losses. Two use cases are included to map the issues on real situations. In a third use case an illustration is made of how public SaaS is also a threat to the organization as Shadow-IT. A qualitative scale is used to define the likelihood and impact of the breach. Combining this likelihood and impact creates the risk. For each risk listed possible countermeasures are proposed. Since no countermeasures exist to provide a 100% protection against data breaches, the thesis concludes with options on how to prepare for a data breach.**

***Keywords*—Cloud Computing, Security, SaaS, Shadow-IT**

I. Introduction

CLOUD computing offers possibilities to businesses that were impossible 10 years ago. Flexibility, scalability, as well as cost-efficiency are all advantages that come with the Cloud. However, organizations moving to the Cloud do not always consider the security risks. Recent attacks performed against large companies (Sony Playstation Network, Apple iCloud …) were picked up by the global media. The general public is becoming more aware of what the consequences can be when their data is not well protected by the Cloud services they use. Protecting confidential data is extremely important for enterprises. With the popularity of Dropbox and other Cloud based storage services, confidential company data can go everywhere.

II. Methodology

The risk management process from ISO 31000:2009 [1] will be used as main guidance for this thesis. The thesis is organized into four sections. In the first section the different use cases are summarized, this links to the context establishment from the ISO standard. The second section evaluates the risks of public SaaS, this is the risk assessment. Section three offers solutions for risk treatment. The last section lists options on how an enterprise can prepare for a data breach.

III. Use case scenarios

These use cases are used to map the different new risks of public SaaS to real use case scenarios.

A. Google Apps for Harvard University

Harvard University provides Google Apps to students and faculty staff to facilitate collaboration. Besides Google Apps, the university also uses SharePoint for more confidential documents. Only **non-confidential** student or faculty member data is stored on Google Apps.

B. Dropbox for Foursquare

Foursquare is an IT start-up that grew very quickly. It became apparent that they needed a more robust, reliable solution for sharing files across different locations. They chose Dropbox as the best solution for digital collaboration. It became a centralized repository for **critical assets** and it enables easy access to **client contracts, sales presentations and internal collateral**.

C. Shadow IT: Confessions of a rogue marketer

The use case describes a marketer that used different Cloud services without approval from the IT department. He used the Cloud for file sharing, storage, project management and collaboration services. The reason why he was using these Cloud services was to get his job done as efficiently as possible. This use case is different from Harvard and Foursquare since the public SaaS here was unapproved by the IT department. The term for this is Shadow IT.

IV. Risk assessment

To produce a list of information security risks the guidance in the Special Publication 800-30 [2] by NIST is used.

1) *Identify Threat sources*
2) *Identify Threat events*
3) *Identify Vulnerabilities and predisposing conditions*
4) *Determine likelihood*
5) *Determine impact*
6) *Determine risk*

For the likelihood and impact the following qualitative scale is used.

Table 1- Qualitative values impact and likelihood

VERY HIGH
HIGH
MODERATE
LOW
VERY LOW

To calculate the risk the following table is used to combine the impact and likelihood.

Table 2- Assessment scale

		Impact				
		VL	L	M	H	VH
Likelihood	VH	VL	L	M	H	VH
	H	VL	L	M	H	VH
	M	VL	L	M	M	H
	L	VL	L	L	L	M
	VL	VL	VL	VL	L	L

In this context the likelihood refers to the likelihood that the threat will result in the impact. **Not** that the threat event will be initiated.

V. Result Risk assessment

The main threats data loss and data breaches are split up in more specific threats. Thirteen threats are selected to conduct the risk assessment. Below they are listed with a short description.

The qualitative value for the likelihood and the impact is based on different factors for each threat. To limit the length of the extended abstract, these individual factors are not incorporated in the sections below.

Data loss

1) *Cloud Service Provider (CSP) hardware confiscation*

When other tenants use the Cloud service for illegal purposes the Cloud provider's hardware can be confiscated. This may lead to data loss for other customers.

2) CSP Bankruptcy

A Cloud service provider can go bankrupt, which can result in data loss for the customer.

3) Natural disaster

Natural disasters can destroy the CSP's infrastructure which can lead to data loss for the customer.

Data breach

4) Brute force attack admin credentials

A brute force attack makes multiple attempts to guess the password of the targeted account. The target here is the admin account with access to the management interface.

5) Social engineer admin account

Social engineering relies on human interaction. It tricks people into doing things they did not intent. The target here is the admin account with access to the management interface.

6) Brute force attack user credentials

A brute force attack makes multiple attempts to guess the password of the targeted account. The target here is a specific user account.

7) Social engineer user account

Social engineering relies on human interaction. It tricks people into doing things they did not intent. The target here is a specific user account.

8) Man in the Cloud attack

This attack steals the synchronization token for the Cloud service client which allows the attacker to download the targeted account's data.

9) Cloud side channel attacks

These attacks request data with no actual information from the Cloud service, but the way the response is delivered is leaking secret information.

10) Company data owned by CSP

Some CSPs have a user agreement that defines if data is modified or created on their Cloud service, it becomes property of the CSP.

11) Malicious insider

An employee that uses his or her access to the Cloud service to do malicious actions.

12) Foreign government espionage

Foreign governments that spy on data stored in their country.

13) Malware targeting Cloud

Malware that specifically targets Cloud services.

Table 3- Risk assessment on use cases

		Risk	
Threat		Harvard University Google Apps	Foursquare Dropbox
T1	CSP hardware confiscation	VERY LOW	LOW
T2	CSP bankruptcy	VERY LOW	LOW
T3	Natural disaster	VERY LOW	LOW
T4	Brute force attack Admin credentials	MODERATE	VERY HIGH
T5	Social engineering admin credentials	MODERATE	VERY HIGH
T6	Brute force attack user credentials	LOW	HIGH
T7	Social Engineering User account	LOW	HIGH
T8	Man in the Cloud attack	LOW	HIGH
T9	Cloud side channel attacks	LOW	HIGH
T10	Company data owned by CSP	VERY LOW	LOW
T11	Malicious insider	LOW	VERY HIGH
T12	Foreign government espionage	VERY LOW	LOW
T13	Malware targeting Cloud	LOW	VERY HIGH

The risks for the Foursquare use case are a lot higher in comparison with Harvard university, this is due to the critical data stored on Dropbox. The impact of data loss or data breach is much higher for Foursquare.

VI. Risk Shadow IT

The problem with Shadow-IT is visibility. It is impossible to do a risk assessment on IT services the company is unaware of. Therefore the risk of Shadow-IT depends on how much visibility the enterprise has on unsanctioned IT applications and infrastructure. The risk that public SaaS as Shadow-IT poses is substantial. According to a discovery assessment by PwC and Skyhigh Networks across Europe, the average number of Cloud services per organization is 987. [3]

VII. Countermeasures

*A. **Choice of CSP***

Some of the risks can be mitigated with the choice of CSP. Before choosing a CSP it is very important to do research for every CSP offering Cloud services. It is not easy and often expensive to change to another CSP, this is also referred to as vendor lock-in.

*B. **Existing Security controls***

1) Security policies

Information security policies consist of several documents that describe how the organization handles information security. There are policies that define what the security requirements are for the organization. Specifics about the implementation of these policies is described in procedures. The enforcement of these policies relies on technical or human security controls.

It is very important that senior management supports the security policies and ensures that they are enforced.

2) Data classification

Data classification is a useful way to rank the value and importance of groups of data. Data classes are used by other security controls such as Data Loss Protection (DLP), security policies, access control …

3) Security Awareness

Security Awareness is making employees more aware of good security practices. People are viewed as one of the weakest links in IT security. With awareness programs, employees are encouraged to think about security during their work.

*C. **Security as a Service (SecaaS)***

SecaaS is a Cloud computing model that delivers managed security services over the internet.

1) Cloud Access Security Broker (CASB)

A CASB is a security solution for Cloud services that combines different functionalities. The four pillars of functionality are: visibility, compliance, data security and threat protection. CASBs offer a wide range of functionality including Data Loss Prevention (DLP), Security Information & Event Management (SIEM) and User Behaviour Analytics (UBA).

2) Data Loss Prevention (DLP)

DLP is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. Cloud features have been added in several DLP products to prevent sensitive data to be copied to the Cloud.

3) Security Information & Event Management (SIEM)

SIEM provide centralized logging capabilities for an enterprise. It aids in detecting, analysing and mitigating security incidents.

4) User Behaviour Analytics (UBA)

UBA detects anomalous behaviour for employees. For example if a user starts downloading all corporate data, this may indicate that a hacker is trying to steal all confidential data.

VIII. RISK TREATMENT FOR USE CASES

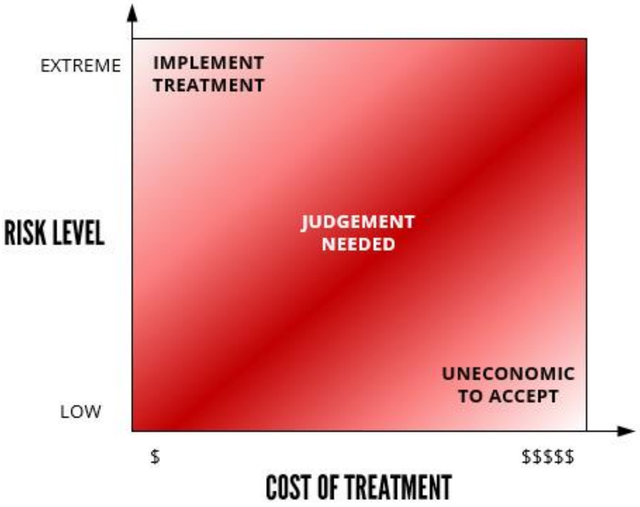


Figure 1- Judgement of risk treatment [4]

A. Google Apps for Harvard University

Harvard University has no serious risk of data loss or data breach caused by Google Apps. CASBs may offer more protection but the cost would be too high compared to the risk level.

B. Dropbox for Foursquare

Foursquare will need to implement treatment to lower the highest risk. A combination of CASB functionalities with security policies and awareness needs to be considered by Foursquare. Multiple vendors of CASBs need to be evaluated so that they match the requirements for Foursquare. These treatments will reduce the likelihood of the threat but as long as critical data is stored on Dropbox, the impact will remain high. CASBs provide a combination of features like DLP, SIEM and UBA. Foursquare can also opt to buy stand-alone solutions in case these offer better services.

C. Shadow-IT

An enterprise can decide to block the shadow-IT that can be detected by investing in solutions to detect unauthorized Cloud services. This will reduce the risk of shadow-IT but this will eliminate the functionality that employees get from Cloud services.

Another option is to make enterprise solutions easier and simpler so that employees are not tempted to go to the Cloud. Security awareness can guide employees to understand the risks of sharing documents with the public Cloud. Cloud Access Security Brokers help gain visibility, assesses the risk for each Cloud service and allows the enterprise to allow trusted Cloud services. DLP software with Cloud functionality can prevent users to share confidential files with the Cloud. Enterprise licenses can be bought for the Cloud services that employees want to use to offer more centralized control and visibility.

D. Conclusions and future work

Cloud Access Security Brokers promise to address many of the security risks that the use of public SaaS creates. It is however a young market and a detailed study is needed to check if the CASBs really address these risks efficiently.

The need for good security management increases because of the shift to global access to Cloud services and the location independent nature of public SaaS.

If an enterprise considers to start using public SaaS for its business, a risk assessment must be made in function to make a good decision.

IX. DATA BREACH

There is no such thing as 100% secure, the risk of a data breach can never be reduced to zero. Knowing how to handle a breach is essential for business continuity. The following sections provide guidance in how an enterprise can handle a data breach.

A. Incident Response Plan

An incident response plan has the primary objective of managing a cybersecurity incident in a way that limits damage and reduces time and costs. SANS defines six steps to handle an incident.

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

B. Reporting requirement Belgium

From 1 January 2016, a new reporting requirement will become active for the European Union. Organizations that suffer a data breach will need to notify the “Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL” and in most cases also the owners of the involved data.

C. CERT.be

Computer Emergency Readiness Teams (CERTs) are organizations with specialized teams of ICT professionals that give support for security incidents. They gather and share information about incidents, give support during incidents, coordinate security responses, support local CERT initiatives and share data and knowledge via publications and events.

D. Federal Computer Crime Unit (FCCU)

The FCCU is the specialized unit in charge of fighting cybercrime in Belgium. In case of criminal cyberattacks the FCCU should be contacted.

E. Insurances

Insurance companies offer insurances to transfer some of the financial risk of a data breach to the insurer. In terms of risk treatment this can be viewed as reducing the consequences. The reputation of the enterprise will still be damaged.

A recent PwC report forecasts that the global cyber insurance market will reach $7.5 billion in annual sales by 2020, up from $2.5 billion this year. [5]

X. BIBLIOGRAPHY

[1] ISO, “ISO 31000 - Risk Management,” ISO, [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm. [Accessed 12 11 2015].

[2] NIST, “Special Publication 800-30 Guide for Conducting Risk Assessments,” NIST, Gaithersburg, 2013.

[3] PriceWaterhouseCoopers, “Managing the Shadow Cloud,” PriceWaterhouseCoopers, 2015.

[4] W. Stallings and L. Brown, Computer Security, London: Pearson Educated Limited 2012, 2012.

[5] D. Gollom, “Cyber insurance market set to reach $7.5 billion by 2020 - PwC report,” PwC, 15 9 2015. [Online]. Available: http://www.pwc.com/ca/en/media/release/2015-09-15-cyber-insurance-market-reach-7-5-billion-2020.html. [Accessed 15 12 2015].

Beschermen van bedrijfsgegevens in de Cloud

Thomas Vandermarliere
Begeleiders: Prof. dr. ir Jan Devos, Dhr. Chris Kappler
Universiteit Gent Campus Kortrijk, België

Abstract— **Deze thesis focust op de beveiligingsproblemen bij het gebruik van publieke Software as a Service (SaaS) in een bedrijf. Deze problemen worden geanalyseerd aan de hand van een risicoanalyse. De twee grootste bedreigingen die opgenomen zijn in de risicoanalyse zijn datalekken en dataverlies. Aan de hand van twee use cases worden de problemen bij publieke SaaS gelinkt aan bestaande situaties. In een derde use case wordt aangetoond hoe publieke SaaS een bedreiging voor de onderneming kan vormen als Shadow-IT. In de risicoanalyse wordt een kwalitatieve schaal gebruikt om de kans en de impact van een datalek of dataverlies uit te drukken. Wanneer deze kans en impact gecombineerd worden krijgt men als resultaat het risico. Aan de hand van de verkregen risico's worden oplossingen voorgesteld om dit risico omlaag te krijgen. Aangezien geen enkele oplossing 100% bescherming kan bieden sluit deze thesis af met opties om zich voor te bereiden op een datalek.**

***Trefwoorden*—Cloud Computing, Security, SaaS, Shadow-IT**

I. Introductie

CLOUD computing biedt mogelijkheden aan bedrijven die onmogelijk waren 10 jaar geleden. Flexibiliteit, schaalbaarheid en kost-efficiëntie zijn allemaal voordelen die de Cloud met zich meebrengt. Aan de andere kant zijn er ook risico's aan verbonden, waar ondernemingen niet altijd aan denken. Recente aanvallen gericht op grote bedrijven (Sony Playstation Network, Apple iCloud, …) komen meer en meer in de internationale media. Mensen beginnen de gevolgen in te zien van wat er kan gebeuren wanneer hun gegevens niet goed beschermd worden door Cloud services die ze gebruiken. Bij bedrijven is het beschermen van confidentiële data van zeer groot belang. Met de populariteit van Dropbox en andere Cloud services is het mogelijk dat confidentiële bedrijfsgegevens hierop belanden.

II. Methodologie

Het risicomanagement proces van ISO 31000:2009 [1] wordt gebruikt als richtlijn voor deze thesis. Het document is opgedeeld in vier secties. In de eerste sectie zijn de verschillende use cases samengevat, dit verwijst naar de context establishment van de ISO standaard. De tweede sectie behandeld de risico's van publieke SaaS voor de use cases, dit is de risicoanalyse. Sectie drie reikt mogelijke oplossingen aan om de risico's te verlagen. De laatste sectie geeft opties op om voorbereidingen te treffen tegen een datalek.

III. Use case scenario's

Hieronder worden de use case beschreven die gebruikt worden om de nieuwe bedreigingen bij publieke SaaS te koppelen aan realistische situaties.

A. *Google Apps voor Harvard University*

Harvard University biedt Google Apps aan studenten en faculteitspersoneel aan om samenwerking te faciliteren. Naast Google Apps gebruikt de Universiteit ook SharePoint voor meer confidentiële research data. Enkel **niet-confidentiële** data van studenten en faculteitspersoneel wordt opgeslagen op Google Apps.

B. *Dropbox voor Foursquare*

Foursquare is een IT start-up dat heel snel gegroeid is. Het werd duidelijk dat ze nood hadden aan een robuuste en betrouwbare oplossing om bestanden te delen over verschillende locaties. Dropbox werd gekozen als de beste oplossing voor digitale samenwerking. Het is de gecentraliseerde opslagplaats voor kritieke bedrijfsbestanden en zorgt voor makkelijke toegang tot klantencontracten, verkoop presentaties en andere interne bestanden.

C. *Shadow IT: Confessions of a rogue marketer*

In deze use case gaat het over een marketeer dat verschillende Cloud services gebruikt heeft zonder toelating van de IT afdeling. Hij gebruikte Cloud voor onder andere het delen van bestanden, opslag, project management en collaboratiesoftware. De reden hiervoor was om zijn job zo efficiënt mogelijk uit te voeren. Deze use case verschild van Harvard en Foursquare in de zin dat het gebruik van publieke SaaS niet ondersteund werd door de onderneming. Dit wordt beschouwd als Shadow-IT.

IV. Risico analyse

Om een lijst op te stellen van beveiligingsrisico’s worden de richtlijnen van de Special Publication 800-300 [2] door NIST gebruikt.

1) *Identify Threat sources*
2) *Identify Threat events*
3) *Identify Vulnerabilities and predisposing conditions*
4) *Determine likelihood*
5) *Determine impact*
6) *Determine risk*

Om de kans en de impact van een bedreiging te bepalen wordt gebruik gemaakt van volgende kwalitatieve schaal.

Tabel 1- Kwalitatieve waarden voor kans en impact

VERY HIGH
HIGH
MODERATE
LOW
VERY LOW

Het risico wordt verkregen doormiddel van de combinatie van kans en impact aan de hand van volgende tabel.

Tabel 2- Assessment scale

		Impact				
		VL	**L**	**M**	**H**	**VH**
Likelihood	**VH**	VL	L	M	H	VH
	H	VL	L	M	H	VH
	M	VL	L	M	M	H
	L	VL	L	L	L	M
	VL	VL	VL	VL	L	L

In deze context bedoeld men met de kans, de kans dat een bedreiging effectief zal resulteren in een negatieve impact. Het is dus **niet** de kans dat er een poging gedaan wordt om een kwetsbaarheid te exploiteren.

V. Resultaat risico analyse

De bedreigingen, dataverlies en datalekken zijn opgesplitst in meer specifieke bedreigingen. Dertien bedreigingen zijn geselecteerd om de risicoanalyse mee uit te voeren. Hieronder zijn ze opgelijst met een korte beschrijving.

Om de kwalitatieve waarde van de kans en impact te bepalen is gebruik gemaakt van verschillende factoren per bedreiging. Om de lengte van de extended abstract te beperken zijn deze niet toegevoegd in onderstaande secties.

Dataverlies

1) *Cloud Service Provider (CSP) hardware confiscatie*

Wanneer andere gebruikers van de Cloud service illegale activiteiten uitvoeren op de service dan is er een kans dat de hardware van de CSP in beslag wordt genomen. Dit kan mogelijks resulteren in dataverlies voor de andere gebruikers van de Cloud service.

2) CSP Faillissement

Een CSP kan failliet gaan met als resultaat dat de gebruikers van de Cloud service data verliezen.

3) Natuurlijke ramp

Natuurlijke rampen kunnen de infrastructuur van de CSP vernietigen waardoor dataverlies mogelijk is voor de gebruikers.

Datalek

4) Brute force aanval op admin account

Een brute force aanval probeert met meerdere loginpogingen het wachtwoord te raden van het doelwit. In dit geval is het doelwit het admin account met toegang tot de management interface.

5) Social engineer admin account

Social engineering is de term die gebruikt wordt bij technieken om informatie te verkrijgen doormiddel van manipulatie bij mensen. Het doelwit is het admin account met toegang tot de management interface.

6) Brute force aanval user credentials

Een brute force aanval probeert met meerdere loginpogingen het wachtwoord te raden van het doelwit. In dit geval is het doelwit een specifieke user account.

7) Social engineer user account

Social engineering is de term die gebruikt wordt bij technieken om informatie te verkrijgen doormiddel van manipulatie bij mensen.Het doelwit is een specifieke user account.

8) Man in the Cloud attack

Bij deze aanval wordt de synchronization token van de Cloud service client gestolen. Hierdoor kan de aanvaller data downloaden van het doelwit.

9) Cloud side channel attacks

Bij deze aanvallen wordt data opgevraagd die geen relevante informative bevatten, maar de manier waarop het antwoord gegeven wordt bevat mogelijks gevoelige informative.

10) Bedrijfsgegevens die eigendom worden van CSP

Bij sommige CSPs staat er in de gebruikersovereenkomst gedefinieerd dat wanneer er data aangepast wordt met hun service, deze aangepaste data eigendom wordt van de CSP.

11) Werknemer met slechte intenties

Een werknemer die opzettelijk Cloud services gebruikt om data te lekken.

12) Buitenlandse overheid spionage

Buitenlandse overheid die spionage uitvoeren op data van andere landen die opgeslagen is in hun land.

13) Malware gericht naar Cloud

Malware die specifiek gericht is naar Cloud services.

Table 3- Risicoanalyse op use cases

		Risico	
Bedreiging		Harvard University Google Apps	Foursquare Dropbox
T1	CSP hardware confiscatie	VERY LOW	LOW
T2	CSP faillisement	VERY LOW	LOW
T3	Natuurlijke ramp	VERY LOW	LOW
T4	Brute force aanval Admin credentials	MODERATE	VERY HIGH
T5	Social engineering admin credentials	MODERATE	VERY HIGH
T6	Brute force aanval user credentials	LOW	HIGH
T7	Social Engineering User account	LOW	HIGH
T8	Man in the Cloud attack	LOW	HIGH
T9	Cloud side channel attacks	LOW	HIGH
T10	Bedrijfsgegevens die eigendom worden van CSP	VERY LOW	LOW
T11	Werknemer met slechte intenties	LOW	VERY HIGH
T12	Buitenlandse overheid spionage	VERY LOW	LOW
T13	Malware gericht naar Cloud	LOW	VERY HIGH

De risico's voor de Foursquare use case zijn veel hoger in vergelijking met die van Harvard University. De reden hiervoor is voornamelijk dat de data die opgeslagen wordt bij Foursquare veel gevoeliger is dan de data bij Harvard. De impact van een datalek zal veel groter zijn bij Foursquare dan bij Harvard. Aan de hand van deze resultaten kunnen de grootste risico's eerst behandeld worden.

VI. RISICO SHADOW IT

Het probleem bij Shadow-IT is zichtbaarheid. Het is onmogelijk om een risicoanalyse te doen op Cloud services waarvan de onderneming niet op de hoogte is ze gebruikt worden. Het risico van Shadow-IT hangt hierdoor voor een groot deel af van hoeveel zicht de onderneming heeft in het gebruik van Cloud services. Algemeen kan men aanemen dat publieke SaaS een substantieel risico vormt voor alle ondernemingen. Een studie van PwC en Skyhigh Networks over heel Europa toont aan dat er gemiddeld 987 Cloud services gebruikt worden binnen de onderneming. [3]

VII. MOGELIJKE OPLOSSINGEN

A. *Keuze van CSP*

Een aantal van de risico's kan beperkt worden door een goede keuze te maken tussen de verschillende CSPs. Het is belangrijk research te doen naar de verschillende Cloud services om een doordachte keuze te maken. Na het maken van de keuze is het in veel gevallen moeilijk om nog te veranderen. De term die hiervoor gebruikt wordt is vendor lock-in.

B. *Bestaande security controls*

1) Security policies

Information security policies bestaan uit verschillende documenten die beschrijven hoe de onderneming moet omgaan met informatiebeveiliging. Er zijn policies die definieren wat de beveiligingsvereisten zijn voor de organisatie. Specifieke details over de implementatie van deze policies staan beschreven in procedures. De handhaving van deze policies hangt af van technische of menselijke security controls.

Het is zeer belangrijk dat het hogere management de security policies ondersteund en ervoor zorgt dat deze effectief worden gehandhaafd.

2) Data classificatie

Data classificatie is een manier om de waarde en het belang van groepen data te rangschikken. Data klassen worden gebruikt door security controls zoals DLP, access control, …

3) Security Awareness

Security Awareness is het op de hoogte stellen van werknemers over goede beveiligingshandeling op de werkvloer. Mensen worden aanzien als de zwakste schakel in IT security. Doormiddel van security awareness worden werknemers aangezet om beveiliging in het achterhoofd te hebben tijdens hun werk.

C. *Security as a Service (SecaaS)*

SecaaS een Cloud computing model dat managed security services aanbiedt over het internet.

1) Cloud Access Security Broker (CASB)

Een CASB is een beveiligingsoplossing specifiek voor Cloud services die verschillende functionaliteiten combineert. De vier pilaren waarop de CASBs focussen zijn: visibility, compliance, data security en threat protection. In de brede waaier van funcionaliteiten kan men onder andere Data Loss Prevention (DLP), Security Information & Event Management (SIEM) en User Behaviour Analytics (UBA) vinden.

2) Data Loss Prevention (DLP)

DLP is een oplossing die ervoor zorgt dat eindgebruikers geen confidentiele data buiten het bedrijfsnetwerk sturen. Cloud functionaliteiten zijn toegevoegd aan verschillende bestaande DLP producten om tegen te gaan dat confidentiële data zomaar naar de Cloud wordt gekopieerd.

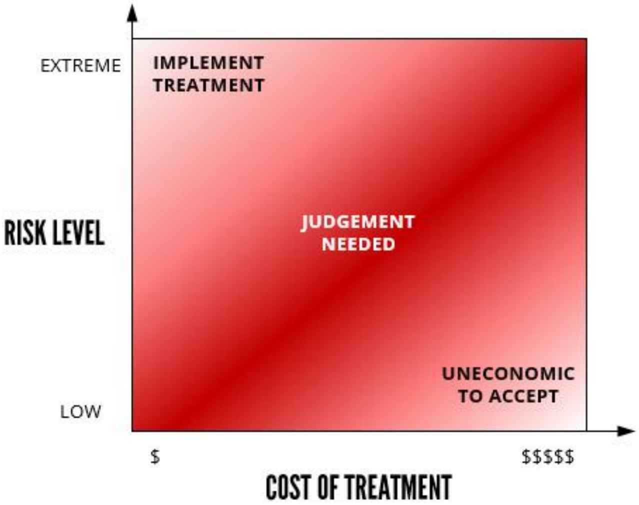
3) *Security Information & Event Management (SIEM)*

SIEM voorziet gecentralizeerde loggingsmogelijkheden voor een onderneming. Het kan helpen in het detecteren, analyseren en vermijden van beveiligingsincidenten.

4) *User Behaviour Analytics (UBA)*

UBA detecteert abnormaal gedrag van gebruikers. Wanneer een gebruiker bijvoorbeeld alle confidentiële data in één keer wil downloaden, wijst dit waarschijnlijk op slechte bedoelingen.

VIII. RISICOBEHANDELING VOOR USE CASES



Figuur 1- Beslissing bij risicobehandeling [4]

A. *Google Apps voor Harvard University*

Bij Harvard University is er geen serieus risico op dataverlies of datalekken door het gebruik van Google Apps. Het gebruik van een CASB zou eventueel extra beveiliging kunnen bieden maar de kost hiervoor is niet verantwoord ten opzichte van het risiconiveau.

B. *Dropbox voor Foursquare*

Foursquare zal moeten kijken naar oplossingen om de hoogste risico's te verlagen. Een combinatie van CASB functionaliteiten met security policies en awareness moet overwogen worden. Verschillende CASB vendors kunnen vergeleken worden om te voldoen aan de vereisten van Foursquare. Deze oplossingen hebben grotendeels effect op de kans van de bedreiging. De impact van een datalek zal hetzelfde blijven zolang er kritieke bedrijfsgegeven opgeslagen worden op Dropbox. CASBs bieden een waaier aan functionaliteiten gericht op Cloud zoals DLP, SIEM en UBA. Foursquare kan er ook voor kiezen om stand-alone oplossingen te implementeren in het geval deze betere services aanbieden.

C. *Shadow-IT*

De onderneming kan ervoor kiezen om Shadow-IT die gedetecteerd kan worden te blokkeren op het bedrijfsnetwerk. Dit zal het risico van Shadow-IT verlagen maar zal er ook voor zorgen dat de werknemers de functionaliteit van deze Cloud services verliezen. Hierdoor is het mogelijk dat ze minder efficiënt hun job zullen kunnen uitvoeren.
Een andere optie is om de oplossingen aangeboden door de onderneming makkelijker en beter te maken zodat werknemers geen nood meer hebben aan andere Cloud services.

Security awareness kan werknemers de beveiligingsproblemen laten inzien bij het gebruik van publieke Cloud services.

CASBs kunnen helpen bij het verkrijgen van inzicht in het gebruik van Cloud services binnen de onderneming en om het risico hiervan in te schatten. DLP functionaliteiten gericht op de Cloud kunnen blokkeren dat confidentiële data naar de Cloud verstuurd wordt.
Voor veel gebruikte publieke Cloud services kunnen business licenties worden gekocht om zo betere beveiliging en gecentraliseerde controle te verkrijgen.

D. *Conclusie en toekomstig onderzoek*

Cloud Access Security Brokers beloven veel van de beveiligingsrisico's bij publieke SaaS aan te pakken. Het is echter nog een jonge markt en een gedetailleerde studie van de verschillende CASBs is nodig om te controleren of ze effectief de risico's verlagen.

De nood aan goed security management wordt verhoogd door de shift naar globale toegang tot Cloud services en de locatie onafhankelijke natuur van publieke SaaS.

Als een onderneming de overweging maakt om publieke SaaS te gaan gebruiken, is het aangeraden om een risicoanalyse uit te voeren die helpt om een doordachte beslissing te maken.

IX. DATALEK

Omdat geen enkele oplossing 100 % bescherming kan bieden, is er steeds een kans op een datalek. Het is daarom belangrijk om als onderneming voorbereid te zijn. De volgende paragrafen geven richtlijnen hoe een organisatie kan reageren op een datalek.

A. *Incident Response Plan*

De primaire doelstelling van dit plan is het reduceren van de impact van een datalek. Het plan zorgt ervoor dat de bedrijfsactiviteiten zo snel mogelijk op een normale manier kunnen worden voortgezet. SANS, een research organisatie, definieert zes stappen om voorbereid te zijn tegen een datalek.

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

B. *Rapporteringsplicht België*

Vanaf 1 januari 2016 wordt er een nieuwe rapporteringsplicht actief binnen de Europese Unie. Organisaties die slachtoffer worden van een datalek zullen verplicht zijn om in België melding te doen bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL), en in de meeste gevallen ook de eigenaars van de gelekte data op de hoogte te stellen

C. CERT.be

Computer Emergency Readiness Teams (CERTs) zijn organisaties met gespecialiseerde teams van ICT professionals die ondersteuning geven bij beveiligingsincidenten. Ze verzamelen en delen informatie over incidenten, geven support tijdens een incident, coördineren beveiligingsinitiatieven, ondersteunen lokale CERT initiatieven en delen data en kennis via publicaties en evenementen.

D. Federal Computer Crime Unit (FCCU)

De FCCU is het gespecialiseerde team die verantwoordelijk is voor het vechten tegen cybercrime in België. Wanneer er zich een criminele cyberattack voordoet moet de FCCU gecontacteerd worden.

E. Verzekeringen

Verzekeringsbedrijven bieden verzekeringen aan om een deel van het financieel risico bij een datalek te verlagen. In termen van risicobehandeling kan dit gezien worden als het verlagen van de consequenties. De reputatie van het bedrijf daarentegen zal wel nog steeds schade oplopen bij een datalek.
In een recent onderzoek van PwC wordt voorspeld dat de globale cyber verzekeringsmarkt zal stijgen naar $7.5 miljard in jaarlijkse omzet tegen 2020 in vergelijking met de $2.5 miljard dit jaar [5]

X. Bibliografie

[1] ISO, “ISO 31000 - Risk Management,” ISO, [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm. [Accessed 12 11 2015].

[2] NIST, “Special Publication 800-30 Guide for Conducting Risk Assessments,” NIST, Gaithersburg, 2013.

[3] PriceWaterhouseCoopers, “Managing the Shadow Cloud,” PriceWaterhouseCoopers, 2015.

[4] W. Stallings and L. Brown, Computer Security, London: Pearson Educated Limited 2012, 2012.

[5] D. Gollom, “Cyber insurance market set to reach $7.5 billion by 2020 - PwC report,” PwC, 15 9 2015. [Online]. Available: http://www.pwc.com/ca/en/media/release/2015-09-15-cyber-insurance-market-reach-7-5-billion-2020.html. [Accessed 15 12 2015].

Contents

Abbreviations

CCSL	Cloud Certification Schemes List
CCSM	Cloud Certification Schemes Metaframework
CERT	Computer Emergency Readiness Team
CIO	Chief Information Officer
CSP	Cloud Service Provider
DLP	Data Loss Prevention
ECSA	EuroCloud Star Audit
ENISA	European union Agency for Network and Information Security
FCCU	Federal Computer Crime Unit
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IR	Incident Response
IT	Information Technology
OS	Operating System
PaaS	Platform as a Service
PII	Personally identifiable information
SaaS	Software as a Service
SEA	Syrian Electronic Army
SIEM	Security Information & Event Management
SPI	SaaS, PaaS, IaaS
UBA	User Behaviour Analytics
UTM	Unified Threat Management
VM	Virtual Machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network

List of Figures

List of Tables

Thesis description

Cloud computing offers possibilities to businesses that were impossible 10 years ago. Flexibility, scalability, as well as cost-efficiency are all advantages that come with the Cloud. However, organizations moving to the Cloud do not always consider the possible security risks.

Recent attacks performed against large companies (Sony PlayStation Network, Apple iCloud ...) were picked up by the global media. The public is becoming more aware of what the consequences can be when their data is not well protected by the Cloud services they use.

The increased demand for enhanced data security has spurred innovation and led to some creative solutions but it has also created confusion and misleading vendor claims as what is truly feasible from a data protection standpoint.

For enterprises protecting their confidential data is extremely important. With the popularity of Dropbox and other Cloud based storage services, confidential company data can go everywhere when these apps are not monitored or blocked. This thesis focuses on the security issues for the use of public Cloud Software-as-a-Service (SaaS) within an enterprise.

Goal

The main focus of this thesis is how Enterprise Data in the Cloud can be protected. An overview will be provided on the various, existing methods to use Cloud services in a secure manner. As 100% protection against attacks can never be achieved, this thesis will also cover what to do when a breach occurred.

First goal: How easy can Cloud services be compromised?

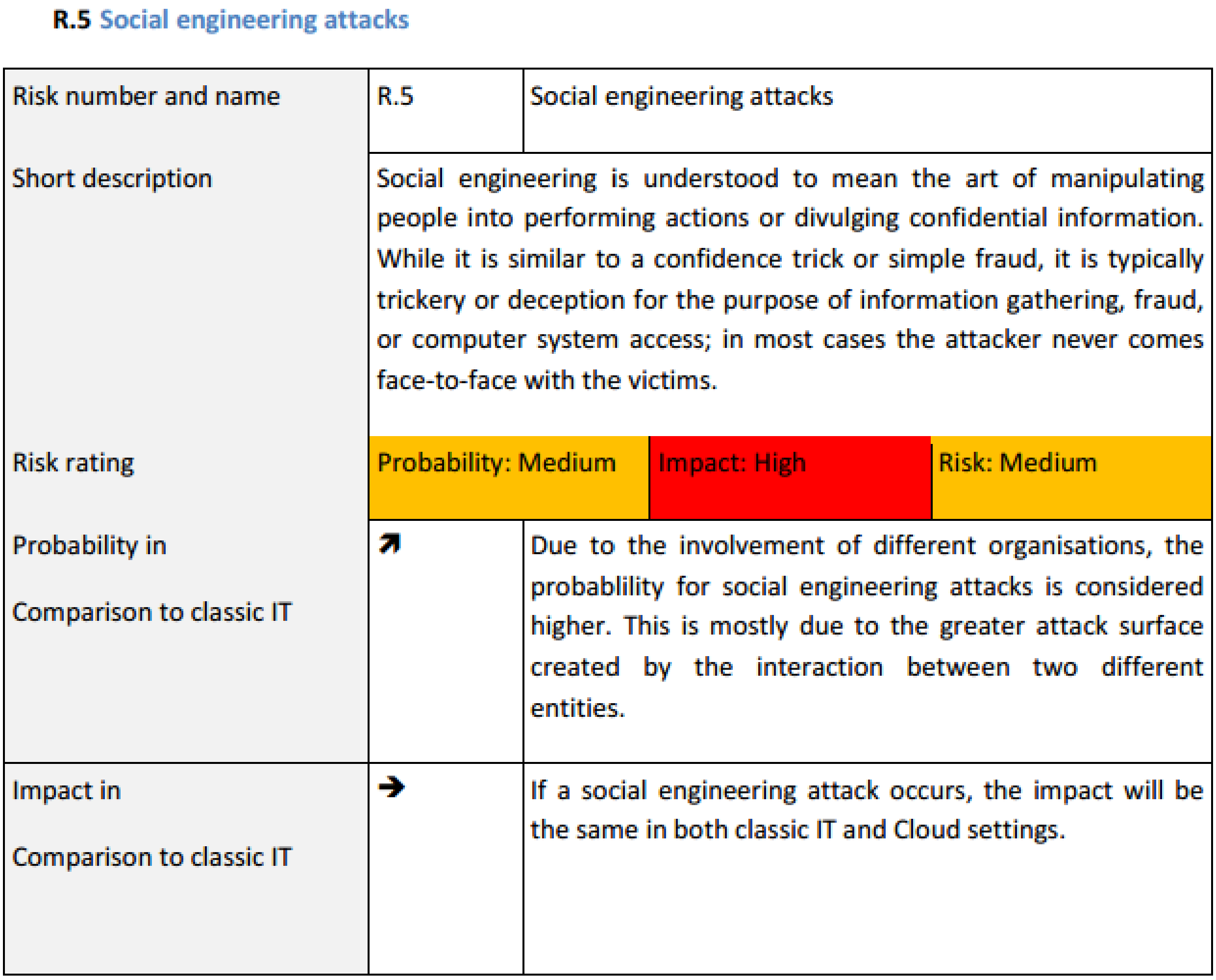
Public Cloud services bring ease of connectivity for the users, this also means adversaries have more attack vectors. Not only external hackers are a threat, internal employees can also be a threat. The employees of the CSP that manages the Cloud can also represent a threat to the enterprise.

It is critical for an enterprise to know these different threats and attacks.

Second goal: What is the risk of a breach?

A breach is the result of a successful attack, combining the likelihood and the impact of the different threats results in the risk.

Example from ENISA



R.5 Social engineering attacks

Risk number and name	R.5	Social engineering attacks	
Short description	Social engineering is understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, it is typically trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.		
Risk rating	Probability: Medium	Impact: High	Risk: Medium
Probability in Comparison to classic IT	↗	Due to the involvement of different organisations, the probablility for social engineering attacks is considered higher. This is mostly due to the greater attack surface created by the interaction between two different entities.	
Impact in Comparison to classic IT	→	If a social engineering attack occurs, the impact will be the same in both classic IT and Cloud settings.	

Figure 1 ENISA (2012), Cloud Computing: Benefits, risks and recommendations for information security

Third goal: how to protect Cloud services for an enterprise?

Protecting confidential enterprise data is important. That is why organizations need to know how to protect themselves. With new Cloud threats, new Cloud protection techniques appear. Cloud Access Security Brokers can help with protecting valuable assets.

Fourth goal: How to handle a data breach?

There are no solutions to be 100 % secure so an enterprise needs to know what to do when a data breach occurs.

1 *Literature and technological research*

1.1 Defining Cloud

The NIST Definition of Cloud is:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model is composed of five essential characteristics, three service models, and four deployment models." [1]

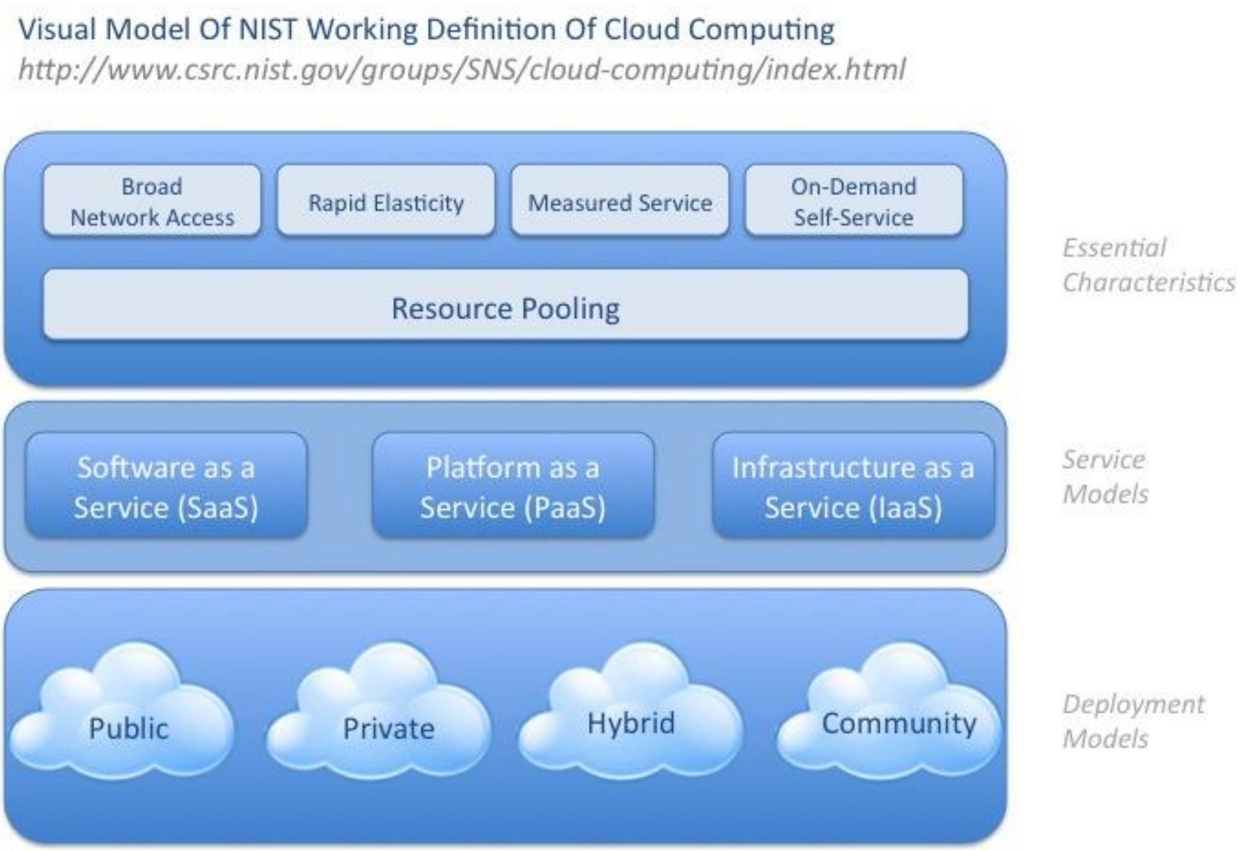

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models

Figure 2 Visual Model of NIST working definition of Cloud Computing

1.2 Service models

In Cloud computing the most prominent service models are:

- **Software as a Service** – SaaS
- **Platform as a Service** – PaaS
- **Infrastructure as a Service** – IaaS

1.2.1 SaaS: Software as a Service

SaaS is the service model that provides both the server hardware and software to organisations without the need to maintain an IT infrastructure.

Most of the responsibilities are for the provider with the SaaS service model. It is not necessary to have in-house personnel to manage the Cloud infrastructure.

A well-known example of SaaS is Dropbox. Dropbox is a service that offers online storage and services.
There is no need for any technical configuration to start working with Dropbox.

1.2.2 PaaS: Platform as a Service

With PaaS, the Cloud Service Provider (CSP) gives the customer more freedom in the choice of computing platform they want to use. This means that the customer must have adequate computer specialist to manage the platform. The extra freedom means also that the customer is responsible for the security of the applications that they run.

An example of PaaS is a MySQL server, the CSP offers the infrastructure and platform but the customer must manage the database.

1.2.3 IaaS: Infrastructure as a Service

The IaaS service model offers the customer the most control over the provided infrastructure. It is necessary for the customer to have people with extensive computer expertise.

The IaaS customer is responsible for all the security aspects of the system except physical security.

IaaS is the most expensive service type and is used by large corporations. Most of the costs for IaaS go to the management of the infrastructure rather than the leasing costs for the servers.

An example of IaaS is the Amazon EC2 service. With EC2 the customer can create virtual machines in an easy and fast way.

1.3 Organizational control

With each different Cloud service model there is a different kind of organizational control. The following table provides an overview of who is in control of what:

Table 1 Organizational Control [2]

On site	SaaS	PaaS	IaaS
⬛ Data	🟨 Data	⬛ Data	⬛ Data
⬛ Apps	🟦 Apps	🟨 Apps	⬛ Apps
⬛ VMs	🟦 VMs	🟦 VMs	🟨 VMs
⬛ Storage	🟦 Storage	🟦 Storage	🟦 Storage
🟨 Network	🟦 Network	🟦 Network	🟦 Network

LEGEND

⬛ Business control

🟨 Dual control with CSP

🟦 CSP control

The fact that there are different kinds of organizational control has effect on the responsibilities for security. With an on-site infrastructure, most of the responsibility falls on the organization itself. However, with SaaS, almost all responsibility lies with the Cloud Service Provider.

1.4 Cloud security Models

When leveraging Cloud services, the Cloud consumer and the CSP have a shared responsibility for securing the Cloud services.

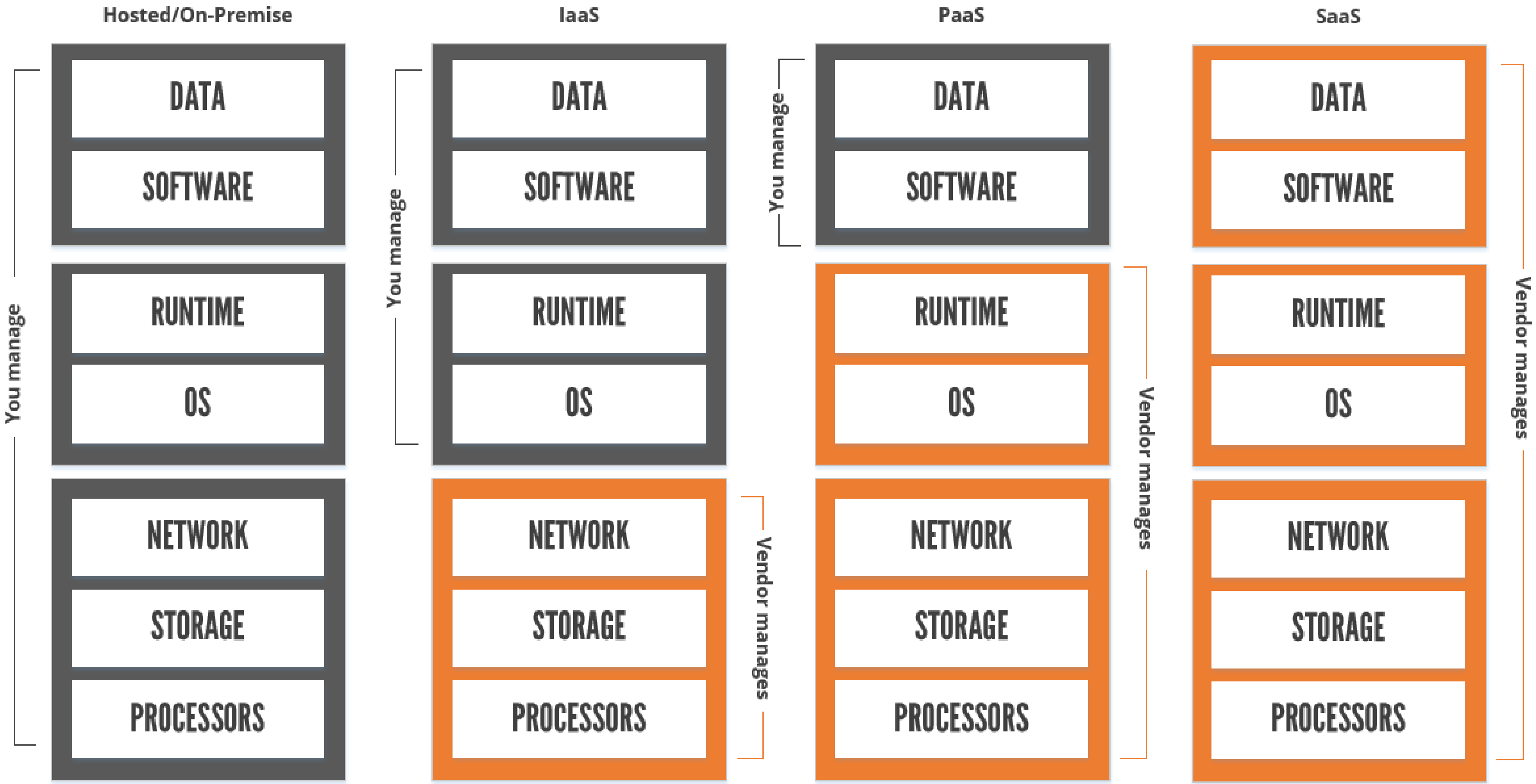


Figure 3 - Cloud Security Models [3]

1.5 Deployment models

Next to the three service types in Cloud Computing there are several deployment models. These define where the Cloud services run and to whom they are accessible. There are four deployment models: Public, Private, Hybrid and Community Cloud.

1.5.1 Public Cloud

The public Cloud is the most open deployment model. It is accessible by anyone that has a connection to the internet. Any of the three service models (SaaS, PaaS and IaaS) can be used with the public Cloud.

The public Cloud is very popular for private consumers, a lot of these Cloud services offer a free account. Dropbox, OneDrive, Google Drive, Outlook are some examples of public Cloud services.

Enterprises also use public Cloud services, for example: Amazon AWS, Google Apps, and Salesforce.com.

One of the greatest concerns for the public Cloud is security. A survey study on major technical barriers affecting the decision to adopt Cloud services [4] refers to security as the most critical factor that indicates the cases of non-adoption.

The perceived security of public Cloud is often very low compared to the real level of security. Public Cloud providers have better security in many cases than in-house solutions. Public Clouds are hardened through continual hacking attempts. The bug bounty programs of Cloud service providers like Google or Amazon have made their public Cloud services very secure.

Advantages of Public Cloud

- Simplicity and efficiency
- Cost-efficient / only pay for what you need
- Reduced time
- No maintenance

Disadvantages of Public Cloud

- Lack of control
- Lack of visibility
- Reliable on internet connection
- Perceived weaker security

1.5.2 Private Cloud

Private Cloud is a Cloud deployment model that is accessible to the organization only. This can mean that the infrastructure is owned by the organization but is not necessary. It is also considered private Cloud when a CSP provides dedicated servers to an enterprise. The private Cloud can be split up in four types: typical private Cloud, managed private Cloud, hosted private Cloud and virtual private Cloud (VPC).

1. **Typical Private Cloud**

The infrastructure is owned by the organization and has an in-house IT workforce to manage the private Cloud. There is a higher level of security than with a public Cloud.

2. **Managed Private Cloud**

With managed private Cloud, the infrastructure is also owned by the organization but a third party manages it.

3. **Hosted Private Cloud**

In this model a Cloud Service Provider (CSP) provides dedicated servers to the organization. It is also referred to as leased private Cloud. It is more expensive because the CSP cannot use the dedicated server during idle times.

4. **Virtual Private Cloud**

This private Cloud can be viewed as a public Cloud with VPN access. The hardware will be shared among other customers of the CSP but the access is secured via a VPN. It is the cheapest type of private Cloud but still more expensive than public Cloud.

Advantages of Private Cloud

- Greater control
- More control over security
- Higher performance
- Deeper compliance
- Customizable

Disadvantages of Private Cloud

- Higher cost
- On-site Maintenance (if owned by enterprise)
- Capacity Ceiling

1.5.3 Hybrid Cloud

A hybrid Cloud is essentially a combination of a public and a private Cloud. This is ideal for organizations that want to take advantage of the scalability and cost-effectiveness that a public Cloud can offer while keeping some of the applications within a private Cloud.

1.5.4 Community Cloud

A community Cloud is a Cloud shared by a particular sector or a group of organisations with a shared interest.

For example, a community Cloud for the health care sector could focus on HIPAA compliance and the associated need for patient data protection and privacy. [2]

1.6 Cloud Actors [5]

In Cloud computing there are essentially five major actors according to the NIST Cloud computing reference architecture:

- **Cloud Consumer** – Person, or organization that maintains a business relationship with, and uses services from Cloud Providers
- **Cloud Provider** – Person, organization of entity responsible for making a service available to Cloud Consumers
- **Cloud Broker** – An entity that manages the use, performance and delivery of Cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers
- **Cloud Auditor** – A party that can conduct independent assessments of Cloud services, information systems operations, performance and security of the Cloud implementation.
- **Cloud Carrier** – The intermediary that provides connectivity and transport of Cloud services from Cloud Providers to Cloud Consumers

Cloud Provider is also referenced to as Cloud Service Provider (CSP).

[redacted] Current use of Cloud

According to a survey of the SANS institute with a participation of 485 IT professionals the current state of Cloud Computing is as follows. The survey was released on September 2015. [6]

1.7.1 Deployment Model

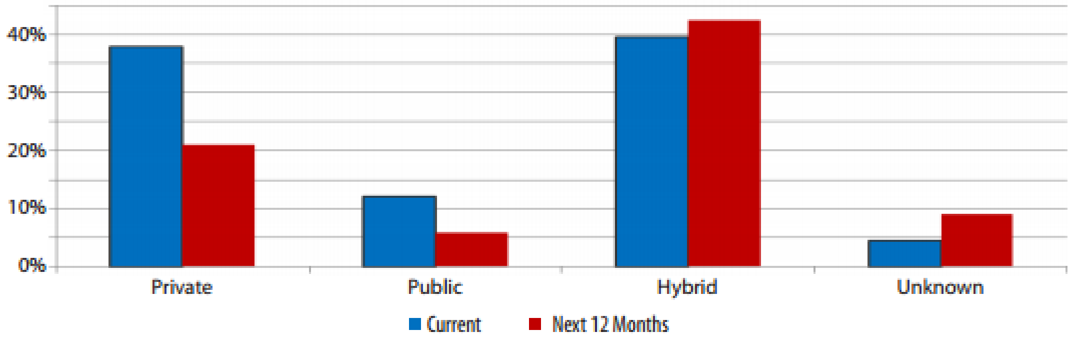


Figure 4 Primary Cloud Architecture Models in Use [6]

The Hybrid deployment model is the most commonly used among survey respondents with 40% currently deploying and 43% planning to move in that direction in the next 12 months.

Next up is the Private Cloud with 38% current deployment and 20% planning in to move in that direction in the next 12 months.

1.7.2 Service model

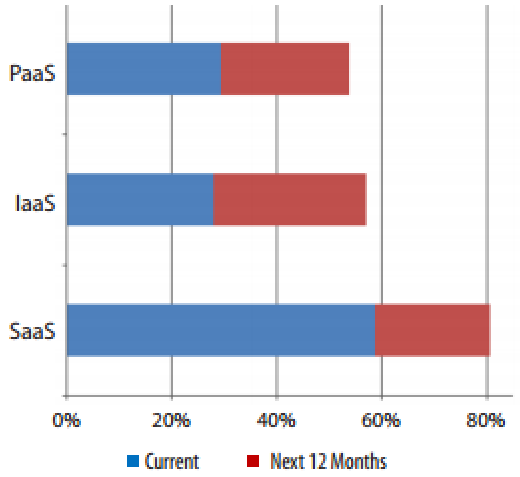


Figure 5 Current and Planned Cloud Models [6]

SaaS is the most adopted Cloud service model with 59% of the correspondents using it currently and 21% planning to implement it within the next 12 months.

1.7.3 Who is using Cloud?

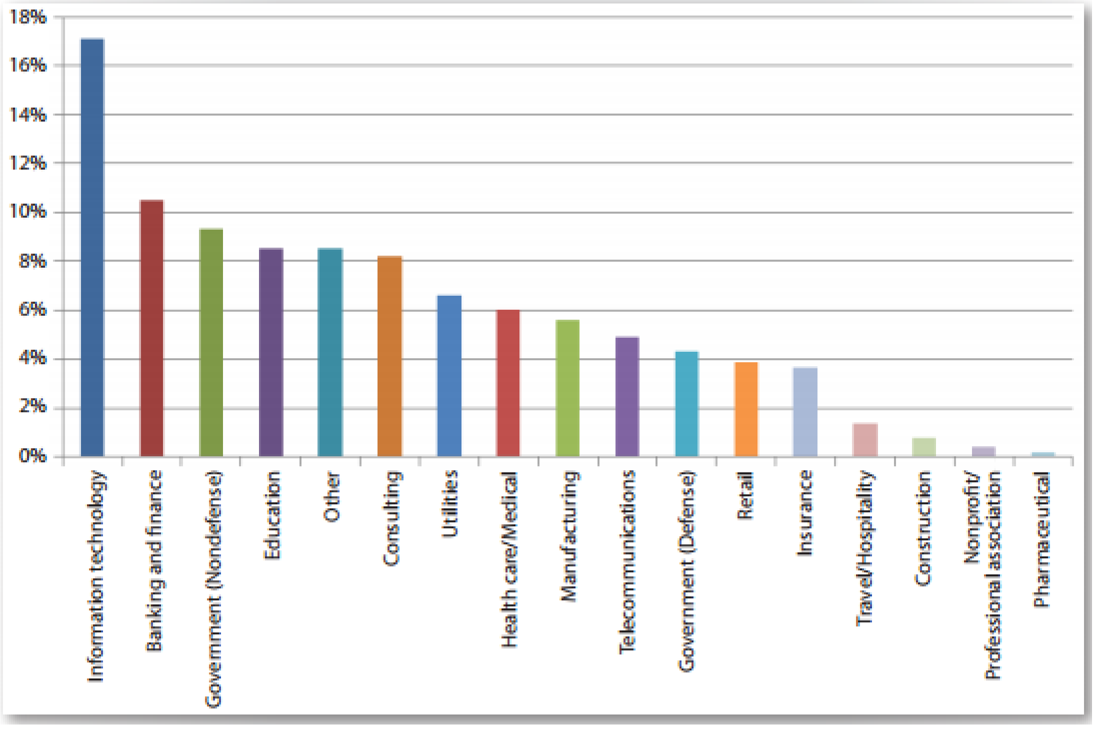


Figure 6 Respondent Roles [6]

The IT sector is the largest Cloud adopter, followed by Banking and Finance.

1.7.4 Conclusion current use of the Cloud

According to the SANS survey the most used deployment model is **Hybrid Cloud** with **Software as a Service** as the most used service model and the largest sector using the Cloud is the **IT sector**. This was the situation on September 2015.

1.8 Cloud for Enterprises

This thesis focuses on protecting enterprise data in the Cloud, so it is important to know how enterprises are using the Cloud. What service model are they using the most and what deployment model? What are the biggest concerns and barriers to adopt Cloud computing specific to large enterprises?

1.8.1 Deployment Model and Service Type

There are different surveys online with information about which service and deployment model is used the most for enterprises.

<table>
<tr><td>Source</td><td>Deployment model</td><td>Service type</td></tr>
<tr><td>Book: Cloud Computing Basics [2]</td><td><b>Private Cloud</b></td><td>All 3 service types but mostly <b>IaaS</b></td></tr>
<tr><td colspan="3">In this book, they make a difference between small and large companies so it is safe to say that the most used case for enterprises according to this book is <b>Private Cloud IaaS.</b></td></tr>
<tr><td>Survey: Orchestrating Security in the Cloud [6]</td><td><b>Hybrid Cloud and Private Cloud</b></td><td><b>SaaS</b> is mostly used but <b>IaaS</b> has the largest area of predicted growth</td></tr>
<tr><td colspan="3">In this survey, there is no distinction between small and large companies. <i>“Survey respondents represented a mix of small and larger organizations, with 38% having 1000 or fewer employees, 24% with over 15000 employees, and the remainder having between 1000 and 10 000.”</i> [6]
This means that this study represents a mixture of companies and not only large enterprises.</td></tr>
<tr><td>Survey: State of the Cloud report [7]</td><td>Wider adoption of <b>public Cloud;</b> deeper adoption of <b>private Cloud.</b> Mostly <b>Hybrid-Cloud.</b></td><td>/</td></tr>
<tr><td colspan="3">RightScale is a company that offers solutions for using Cloud more effectively in your organization. Therefore, we can assume that this report is not vendor neutral. The percentage of enterprise respondents to this survey is 33% but in the report there is a clear distinction between enterprises and small companies.</td></tr>
<tr><td>Citation: The state of Cloud platform standards: Q2 2015 [8]</td><td><b>59% private Cloud</b>
<b>53% public Cloud</b></td><td>/</td></tr>
</table>

“59% prioritizing building a private Cloud and 53% prioritizing adopting public Cloud from a service provider” [8]
This is based on a survey conducted by Forrester. The survey is not available for the public, and information about the survey is only available after additional payment. With 3190 number of respondents from all over the world, this survey can be considered as one of the largest surveys around this topic. [9]

1.8.2 Platform

VMware’s vSphere Hypervisor is used for almost every enterprise’s virtualized environment and a strong share of private Cloud products and public Cloud and managed hosting services. [8]

Common private Cloud platforms include OpenStack, VMware vCloud Suite, and Apache CloudStack. [10]

1.9 Virtualization

Virtualization is a technology that is very important for Cloud Computing. It allows running multiple Virtual Machines (VM) on a hardware platform. Applications, services and Operating Systems (OS) are abstracted from the hardware on which they run.

The fact that VMs operate independent from the hardware it is hosted on allows to move them around on different servers. They share the hardware with other VMs so they require a middleware layer to support such operations, this is done by Virtual Machine Monitors, called hypervisors.

Advantages of virtualization:

- Cost and downtime reduction
- Ease of management and administration
- Scalability

Disadvantages of virtualization:

- Security
    - Isolation failures between VM’s through vulnerabilities / zero-days
    - Side channel attacks.

1.10 Multi-Tenancy

Multi-tenancy in its simplest form implies use of same resources or application by multiple consumers that may belong to same organization or different organization. In a public Cloud there is multi-tenancy because the hardware is shared among different customers. [11]

1.11 Risks of Cloud Computing [2]

With the adoption of Cloud services, the organizations must be prepared for some of the risks it introduces.

1. **Lack of control over the infrastructure** – The level of control depends on what type of Cloud is used.

2. **Security and privacy control** – When using any Cloud service that is not hosted on premise the organization's data can be located anywhere on the world, with different privacy regulations.

3. **Service management by the Cloud service provider** – Who are the privileged users at the service provider who have access to the customer's applications and data?

4. **Compliance** – Before using a certain Cloud service provider, check if the CSP complies with the necessary standards (HIPAA, PCI-DSS)

5. **Cloud outages / service availability**

6. **Data Breach** – With the public Cloud, it is easier for attackers to gain access to company data

7. **Dependant on CSP** – When CSP shuts down, all company data could be lost (e.g. MegaUpload)

8. **Data lock-in** – When using a certain Cloud service, it is often hard to move to another provider

9. **Lack of access to log files of CSP** – CSP's are reluctant for third party audits of their infrastructure management and policy enforcement.

1.12 Cloud Security concerns

According to the SANS survey "Orchestrating Security in the Cloud" [6] the top concern with data processing in Clouds is maintaining compliance. The results of the survey are displayed in the figure below.

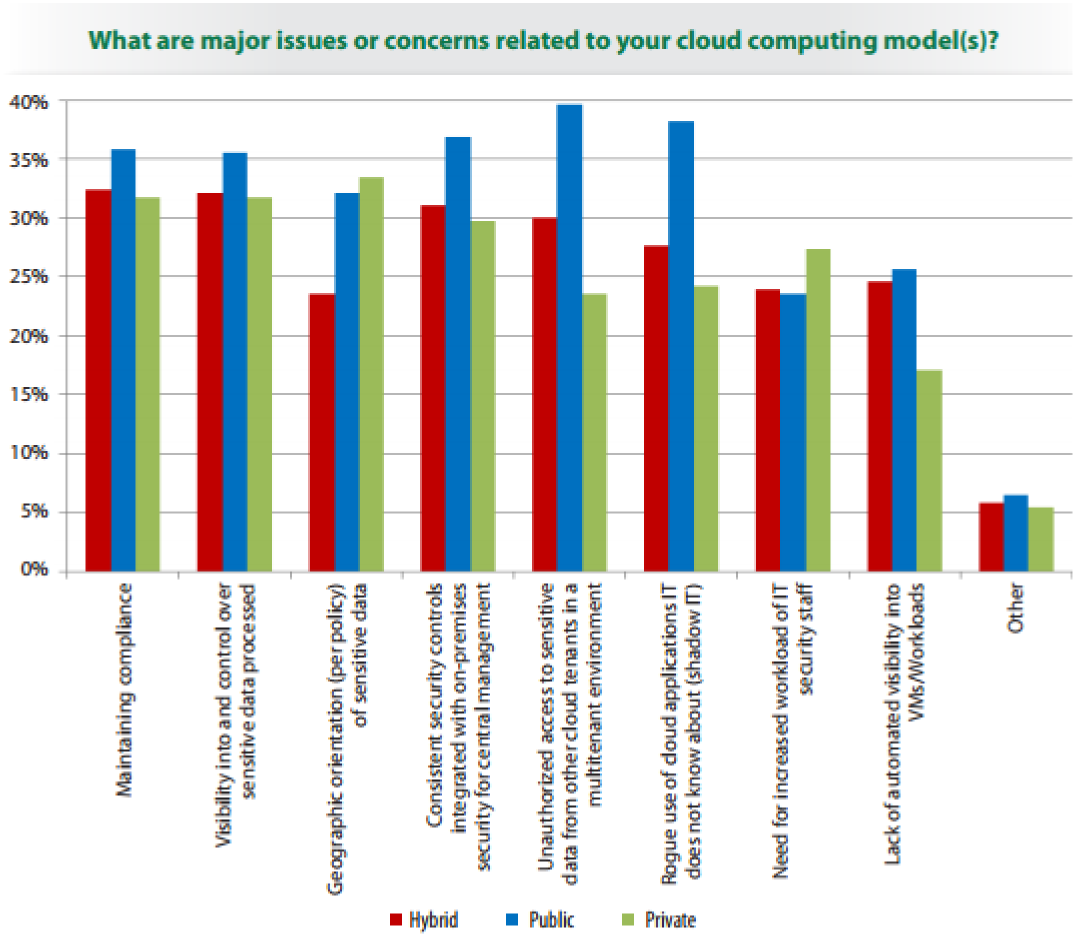


Figure 7 Major Security Concerns in Cloud Deployments [6]

For the public Cloud the biggest concern is the risk of exposing sensitive data. Organizations using private Cloud services are more concerned with the geographical location of their sensitive data, which likely coincides with the multitude of regions they operate in and the regulations they need to comply to.

Other Cloud Security Concerns include:

- **Lack of control** – As explained above in "Organizational Control" various Cloud models allow different levels of control. With the SaaS service model, the organization has minimal control over the Cloud service.
- **Lack of visibility** – Most Cloud service providers (CSPs) will not give away all their internal operations and controls.
- **Inability to test** – Testing the security of a CSP is in most cases restricted since the environment is multi-tenant. Customers are forced to take the word of the CSP regarding the security.
- **Response Preparedness** – When an incident occurred it is often difficult to do forensic analysis, it goes back to the lack of visibility into internal Cloud provider operations. Access to log files and other forensic artefacts is often prohibited.

1.13 Security as barrier to adopt Cloud Services

In the article “A survey study on major technical barriers affecting the decision to adopt Cloud services” [4], one of the main concerns of adopting Cloud services was security. The basis for this article are different studies conducted by large consultancy and IT service companies.

Respondents perceived security concerns as the most critical in the healthcare context.

Government organizations are also sceptical against public Cloud since they are entrusted with public’s information. Therefore, agencies tend to move their systems to a more controlled and secure private Cloud.

“Data protection emerged from the consultation and the studies launched by the Commission as a key area of concern that could impede the adoption of Cloud computing.” [12]

1.14 What is security? [13]

1.14.1 Information systems security (ISS)

ISS focuses on protecting information regardless of form or process. It is often defined with the CIA triad. CIA stands for Confidentiality, Integrity and Availability.

- **Confidentiality** – The goal of ensuring that only authorized individuals are able to access information
- **Integrity** – Ensures that information has not been improperly changed
- **Availability** – Ensures information is available to authorized users and devices

1.14.2 Information Assurance (IA)

IA focuses on protecting information during process and use. The CIA triad is therefore expanded with 2 more pillars.

- **Authentication** – The ability to verify the identity of a user or device
- **Nonrepudiation** – The assurance that an individual cannot deny having digitally signed a document or been party to a transaction

1.14.3 Threats, Vulnerabilities, Risk

When talking about security the terms threat, vulnerability and risk are often used, therefore it is important to have basic understanding of these terms.

- **Threat** – A human-caused or natural event that could impact the system
- **Vulnerability** – A weakness in a system that can be exploited
- **Risk** – The likelihood or probability of an event and its impact

[redacted] Cloud Rating Score for Cloud Service Providers

In a document written by Taiye Lambo (2012) named “Why You Need a Cloud Rating Score” [14] he suggests that a scoring system is necessary to understand the security protections offered by the different CSP’s. This score should make it easier for IT managers and executives to decide between the different CSP’s.

According to Lambo the following four factors are important to rate the score of a CSP:

- Quality of Certifications
- Scope of Certifications
- Security Maturity Level
- History of Breaches

CloudeAssurance is the company of Lambo which offers Cloud Assurance for organizations. The subscription options start at $2,000 per year. Further details about the framework that they use or the metrics for evaluating CSP’s are not available.

Other literature also describe methods for evaluating CSP’s:

An assessment of Security Requirements Compliance of Cloud Providers [14] is a paper in which the authors use different open frameworks to assess Cloud services.

In their assessment, they use CSA’s CloudAudit deliverables and with the Goal Question Metric approach they measure the quality of the goals and questions taken from CSA’s Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ).

More information about CSA’s Cloud Controls Matrix, Consensus Assessments Initiative Questionnaire and CloudAudit can be found under the section CSA in this thesis.

This is an example of a metric for their assessment of Amazon AWS:

First, they describe the metrics:

Goal	Question	Metric
G-01 Compliance	Control Area: Independent Audits	
	Q-01.3 What is the quality of evidence of network penetration tests of your Cloud service infrastructure that you conduct regularly as prescribed by industry best practices and guidance?	M-01.3.1 Evidence compliance score and completeness score of network penetration test policies

Then they check the metrics with the service provider. Information about penetration testing on Amazon AWS can be found via this link: http://aws.amazon.com/security/penetration-testing/

Metric	Evidence	Evidence Compliance	Evidence Completeness
M-01.3.1	Penetration Testing	Partial Compliance	Initial

1.16 Cloud Security Certifications

1.16.1 European union Agency for Network and Information Security (ENISA)

ENISA is a centre of expertise to address cyber security issues of the European Union. Their objective is to make ENISA the European hub for exchange of information, best practices and knowledge in the field of information security.

As a result of the European Cloud Strategy, ENISA has created a Cloud Certification Schemes List (CCSL) and a Cloud Certification Schemes Metaframework (CCSM).

1.16.2 Cloud Certification Schemes List (CCSL)

This list gives an overview of different existing certification schemes which could be relevant for **Cloud computing customers**. CCSL shows the main characteristics of each certification scheme.

For this thesis it is out of scope to cover all the specifics of the different certifications. The following table will give a short summary of each certification. The full list with all the details is available on the following link: https://resilience.enisa.europa.eu/Cloud-computing-certification

Logo	Certification name	Description
TÜVRheinland CERTIFIED Certified Cloud Service www.tuv.com ID 0000040060	Certified Cloud Service – TÜV Rheinland	TÜV Rheinland is an international certification body and offers auditing services to organizations. The certification is based on ISO 27000, NIST recommendations and data privacy regulations.

	CSA Certification – OCF Level 2	This certification is developed by the Cloud Security Alliance (CSA) and is based on the Cloud Controls Matrix. It is part of the CSA STAR program.
	EuroCloud Self Assessment	EuroCloud Europe is a non-profit organisation as is the ECSA programme. This program is not funded by any industry sponsor nor does it receive any financial means from other organisations or government bodies. The self-assessment is the personal assessment of a Cloud Service Provider without confirmation by any ECSA accredited Auditor Organization. [15]
	EuroCloud Star Audit Certification	ECSA delivers a Cloud Certification and Tools that have been approved by ENISA and have been developed under the European Cloud Strategy. [16]
	ISO/IEC 27001	The International Organization for Standardization is an independent, non-governmental membership organization and the world's largest developer of voluntary International Standards. ISO/IEC 270001 is a standard for information security management in general. It is not specifically focussed on Cloud services.
	PCI DSS v3	Payment Card Industry Data Security Standard v3. This is a standard developed by the PCI Security Standards Council. Companies who work with credit card info have to comply with this standard.
	Leet Security Rating Guide	Leet Security is an ICT Services Rating Agency. It rates the different aspects of security: Confidentiality, Integrity and Availability with a certain letter. From E as lowest rating: Implements basic security measures to A as highest rating: Implements maximum levels of security according to the state of art.

	Service Organization Control	Service Organization Controls (SOC) reports are designed to help service organizations, organizations that operate information systems and provide information system services to other entities, build trust and confidence in their service delivery processes and controls through a report by an independent Certified Public Accountant.
	Cloud Industry Forum Code of Practice	The purpose of the Code of Practice for Cloud Service Providers ("Code") is to bring greater transparency and trust to doing business in the Cloud. Code of Practice certified Cloud service providers have declared and committed to providing good quality services that adhere to the guidelines and best practices set out in the COP. The COP is a comprehensive framework that enables service providers to benchmark their operations against standards developed by their peers and in many ways is a checklist for best practice in the provision of Cloud services. The COP covers a broad range of areas and disciplines but focuses on TRANSPARENCY, CAPABILITY & ACCOUNTABILITY. [17]

1.17 Cloud Computing Standardization

Identical to other technologies, standards are needed to provide a uniform way to offer Cloud services. Cloud Computing standards are now being developed to support specific Cloud computing functions and requirements, such as virtualization, infrastructure management, service level agreements (SLAs), audits and Cloud-specific data handling.

NIST maintains a standards inventory on the following website: http://1.usa.gov/1SZnmQ4 [18]

In the following sections, some of the Cloud specific standards are summarized.

1.17.1 ISO/IEC JTC 1 SC 38 Cloud Computing and Distributed Platforms

This standard is still under development. It focusses on interoperable Distributed Application Platform and Services including:

- Web Services
- Service Oriented Architecture (SOA)
- Cloud Computing

On July 2015, these were the published reports from the Cloud Computing Study Group:

- Taxonomy, terminology and value proposition for Cloud Computing
- Assessment of the current state of standardization in Cloud Computing
- Standardization market/business/user requirements and challenges

Published initial Cloud Computing standards, on July 2015:

- ISO/IEC DIS 17788: Overview and Vocabulary
- ISO/ IEC DIS 17789: Reference Architecture

The standard is a work in progress and the next meetings for the working groups are in April 2016 and October 2016.

NIST claims SC38 is leading Cloud Computing Standardization.

1.17.2 NIST-FISMA Standard [19]

The FISMA Implementation project develops information security standards (Federal Information Processing Standards) and guidelines (Special Publications in the 800-series) for non-national security federal information systems, including the development of:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements (management, operational and technical security controls) for information and information systems in each such category.

The FISMA standard is not a Cloud specific standard, therefore the standard assumes that the assets owner has full control over the security management process of their assets. With Cloud computing, some of that control is lost to the Cloud service provider.

1.17.3 ISO 27000 Standard [20]

The ISO27000 standard provides a model to guide the definition and operation of information systems management. It targets all types of organizations, not only federal agencies like FISMA. The ISO 27000 standard has a series of security standards that address different areas in the information systems security management as follows:

- **ISO 27001** – Gives an overview of the specification of any Information Security Management System (ISMS) that is based on ISO27000 standard. It shows how the ISMS standard is aligned with the Plan-Do-Check-Act (PDCA) management model. It summarizes the key terminologies existing in the security management process and gives a summary of security controls objectives that should be operated.

- **ISO 27002** – Focuses on security controls' implementation guidance to help organizations during the ISMS implementation, reviewing and authorization phases. It shows how these phases could be done to address different security targets including Human Resources, physical security, communication security, access control, etc.

- **ISO 27003** – Gives guidance on implementation of different ISMS phases including planning processes, do processes, check processes and act processes phases.

- **ISO 27004** – Addresses the ISMS measurements and metrics that could be used, stakeholders and responsibilities, measurement operations, data analytics of the measurement results, and further improvement actions that could be taken.

- **ISO 27005** – Addresses the security risk management process. It details a methodology for information security risk management including risk analysis, treatment, and acceptance.

- **ISO 27006** – Provides guidelines to help organizations in the accreditation process of ISMS certification. It documents the key requirements that should be satisfied and how they can be addressed.

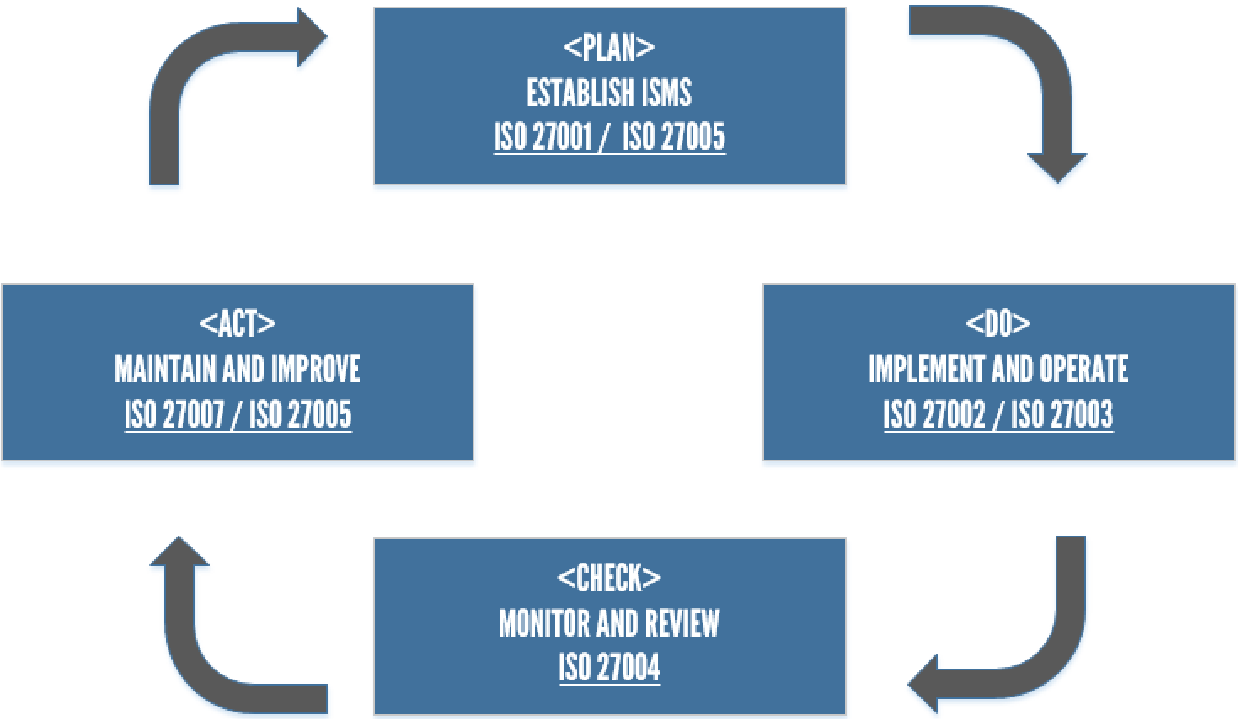


Figure 8 - ISO 27000 main phases, flow and standards

This standard is, just like the FISMA standard, not focused on the use of Cloud services. There are however standards under development that focus on the Cloud:

- **ISO 27017** – Will provide guidance on the information security elements of Cloud computing, recommending and assisting with the implementation of Cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO 27000 standards including ISO 27018 (privacy aspects of Cloud computing), ISO 27031 (business continuity) and ISO 27036-4 (relationship management). [21]
  The standard is expected to be published at the end of 2015.

- **ISO 27018** – Provides guidance aimed at ensuring that Cloud service providers (such as Amazon and Google) offer suitable information security controls to protect the privacy of their customers' clients by securing Personally Identifiable Information (PII) entrusted to them.
  Six of the key principles of ISO 27018 are [22]:

  - **Consent** – CSPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer. Moreover, a customer must be able to use the service without submitting to such use of its private information.

  - **Control** – Customers have explicit control of how their personal data is used.

- **Transparency** – CSPs must inform customers where theirs data resides and make clear commitments as to how that data is handled.
- **Accountability** – ISO 28018 asserts that any breach of information security should trigger a review by the service provider to determine if there was any loss, disclosure, or alteration of personal data.
- **Communication** – In case of a breach, CSPs should notify customers, and keep clear records of the incident and the response to it.
- **Independent and yearly audit** – A successful third-party audit of a CSPs compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, a CSP must subject itself to yearly third-party reviews.

Sometimes the standards do not fit all use cases so organizations may choose to develop their own standard, which the following cartoon illustrates.

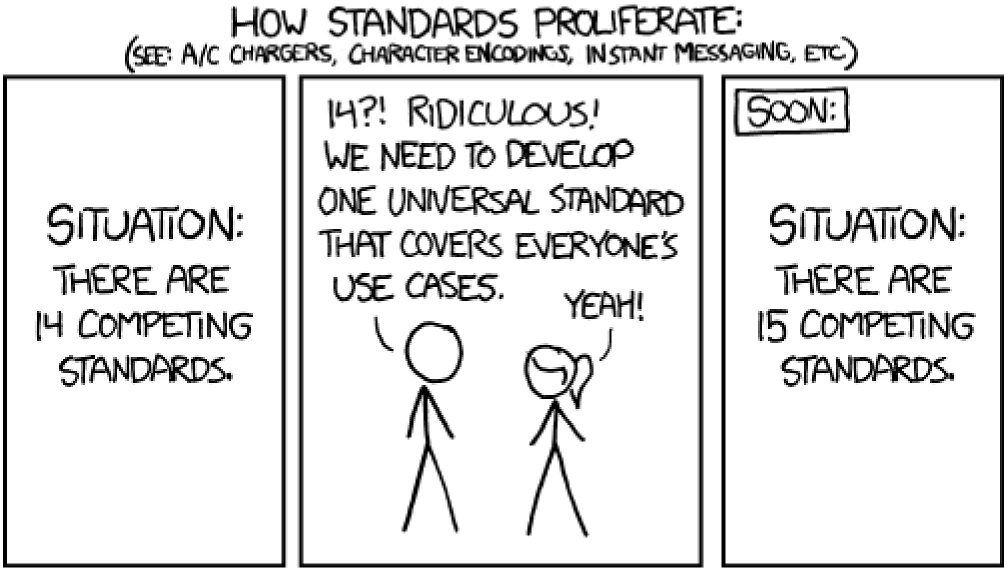

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Figure 9 How Standards Proliferate - xkcd

1.18 Cloud Security Alliance

The Cloud Security Alliance (CSA) is a member-driven organization that promotes the use of best practices for providing security assurance within Cloud Computing. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer Cloud security-specific research, education, certification, events and products. [23]

CSA has two certification programs, one for Cloud service providers: the CSA Security, Trust & Assurance Registry (STAR) and one for Cloud security users: Certificate of Cloud Security Knowledge (CCSK).

1.18.1 CSA Security, Trust & Assurance Registry (STAR)

CSA has a three-tiered STAR Cloud matrix system.

T1. **STAR-Self-Assessment** – based on the CCM framework and the CAIQ questionnaire.
To qualify for tier 1, the group must take a self-assessment on its security practices – which over 100 groups have successfully done today. Thirty percent of this group are enterprises, rather than Cloud vendors. Tier 1 qualifiers include Terremark, Rackspace, Orange, Datapipe, Adobe, AWS, TrendMicro, PayPal, and Swisscom.

T2. **STAR-Certification** – At this level of assessment, the Cloud provider's security is assessed using the control areas that are defined in the CCM framework. Therefore, a score will be assigned to the Cloud provider. STAR certification acts as a next level of assurance.
To achieve tier 2, vendors must undergo a third-party audit to meet ISO27001 and SOC2, scoped for Cloud. Today 15 companies have met this requirement.

T3. **STAR-Continuous** – is based on publishing the assessment results related to the security properties monitoring based on the CloudTrust protocol. The CSA is currently working on this program, and hopes to have this set by mid-year

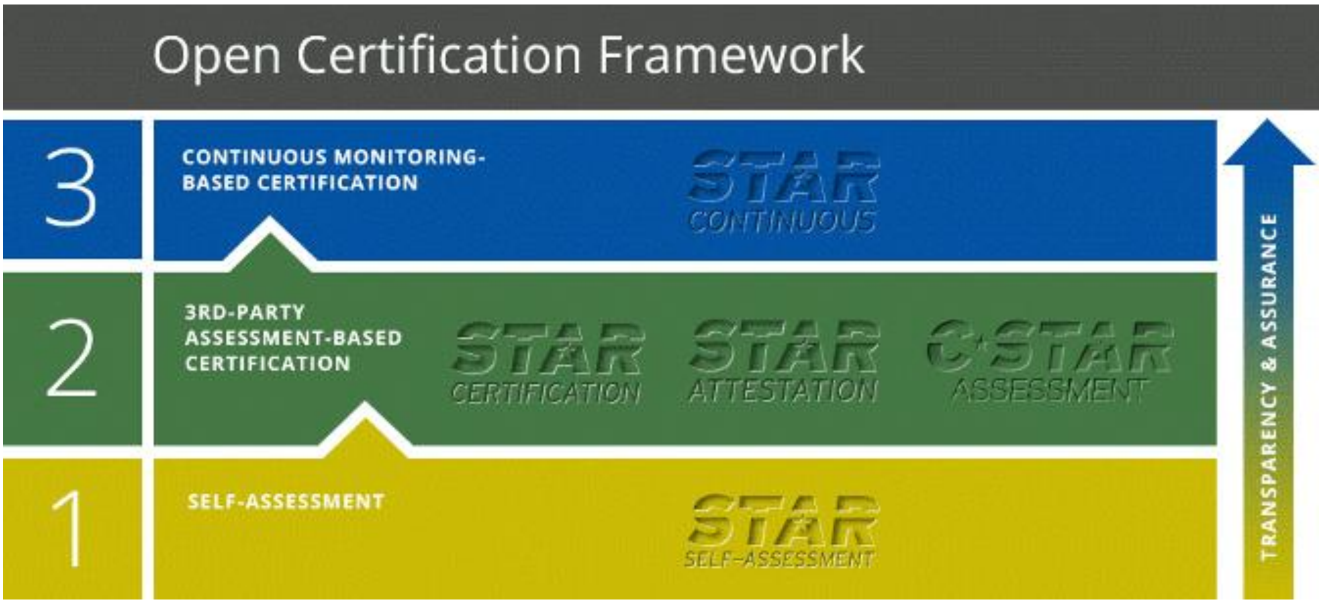


Figure 10 – CSA STAR [24]

1.18.2 Certificate of Cloud Security Knowledge (CCSK)

The CCSK is an examination testing for a broad foundation of knowledge about Cloud security, with topics ranging from architecture, governance, compliance, operations, encryption, virtualization and much more. The body of knowledge for the CCSK examination is the CSA Security Guidance for Critical Areas of Focus in Cloud Computing V3, and the ENISA report “Cloud Computing: Benefits, Risks and Recommendations for Information Security”. [25]

1.19 CSA Governance, Risk Management and Compliance (GRC) Stack

The GRC stack is a toolkit for enterprises, Cloud providers, security solution providers, IT auditors and other key stakeholders to instrument and assess both private and public Cloud against industry established best practices, standards and critical compliance requirements.

It contains four initiatives:

- Cloud Controls Matrix Framework
- Consensus Assessments Initiatives Questionnaire
- CloudAudit
- Cloud Trust Protocol (CTP)

1.19.1 Cloud Controls Matrix (CCM) Framework

The CCM framework is basically a list of different controls that give detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. It links the controls to industry-accepted security standards, regulations, and controls frameworks such as ISO 27001/27002, ISACA COBIT, PCI, NIST ...

An example of a control from the domain Mobile Security is given below:

Table 2 - MOS-01 Mobile Security Anti-Malware

<table>
<tr><td colspan="3"><b>Control Domain</b></td><td colspan="3">Mobile Security Anti-Malware</td></tr>
<tr><td colspan="3"><b>CCM V3.0 Control ID</b></td><td colspan="3">MOS-01</td></tr>
<tr><td colspan="3"><b>Updated Control Specification</b></td><td colspan="3">Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.</td></tr>
<tr><td colspan="6"><b>Architectural Relevance</b></td></tr>
<tr><td>Phys</td><td>Network</td><td>Compute</td><td>Storage</td><td>App</td><td>Data</td></tr>
<tr><td>X</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3"><b>Corp Gov Relevance</b></td><td colspan="3">X</td></tr>
<tr><td colspan="6"><b>Cloud Service Delivery Model Applicability</b></td></tr>
<tr><td colspan="2">SaaS</td><td colspan="2">PaaS</td><td colspan="2">IaaS</td></tr>
<tr><td colspan="2">X</td><td colspan="2">X</td><td colspan="2">X</td></tr>
<tr><td colspan="6"><b>Supplier Relationship</b></td></tr>
<tr><td colspan="3">Service Provider</td><td colspan="3">Tenant / Consumer</td></tr>
<tr><td colspan="3">x</td><td colspan="3"></td></tr>
<tr><td colspan="6"><b>Scope Applicability</b></td></tr>
<tr><td colspan="3"><b>AICPA 2009 TSC Map</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>AICPA Trust Service Criteria (SOC 2 SM Report)</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>AICPA 2014 TSC</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>BITS Shared Assessments AUP v5.0</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>BITS Shared Assessments SIG v6.0</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>BSI Germany</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>Canada PIPEDA</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>CCM V1.X</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>COBIT 4.1</b></td><td colspan="3"></td></tr>
<tr><td colspan="3"><b>COBIT 5.0</b></td><td colspan="3">APO01.03
APO13.01
APO07.03
APO07.06
APO09.03
APO10.04</td></tr>
</table>

<table>
<tr><td colspan="2"><b>COPPA</b></td><td colspan="2"></td></tr>
<tr><td colspan="4"><b>CSA Enterprise Architecture (formerly Trusted Cloud Initiative)</b></td></tr>
<tr><td>Domain > Container > capability</td><td colspan="2">Public</td><td>Private</td></tr>
<tr><td>SRM > Governance & Risk & Compliance > Technical Awareness and Training</td><td colspan="2">Provider</td><td>X</td></tr>
<tr><td colspan="2"><b>CSA Guidance V3.0</b></td><td colspan="2">None (Mobile Guidance)</td></tr>
<tr><td colspan="2"><b>ENISA IAF</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>95/46/EC – European Union Data Protection Directive</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>FedRAMP Security Controls (Final Release, Jan 2012) – LOW IMPACT LEVEL --</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>FedRAMP Security Controls (Final Release, Jan 2012) – MODERATE IMPACT LEVEL --</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>FERPA</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>GAPP (Aug 2009)</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>HIPAA / HITECH Act</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>ISO / IEC 27001-2005</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>ISO / IEC 27001-2013</b></td><td colspan="2">Clause
6.1.1,
6.1.1(e)(2)</td></tr>
<tr><td colspan="2"><b>ITAR</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Jericho Forum</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Mexico - Federal Law on Protection of Personal Data Held by Private Parties</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>NERC CIP</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>NIST SP800-53 R3</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>NIST SP800-53 R4 App J</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>NIZSM</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>ODCA UM: PA R2.0</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>PCI DSS v2.0</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>PCI DSS v3.0</b></td><td colspan="2"></td></tr>
</table>

1.19.2 Consensus Assessments Initiatives Questionnaire (CAIQ)

This questionnaire links the different controls from the Cloud Controls Matrix to yes or no questions. An example of this is displayed below:

Table 3 - MOS-01 Question

MOS-01	**Mobile Security Anti-Malware**	
Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?		
Yes	No	Not Applicable

1.19.3 CloudAudit

The goal of CloudAudit is to provide a common interface and namespace that allows enterprises who are interested in streamlining their audit processes (Cloud or otherwise) as well as Cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorized consumers of their services to do likewise via an open, extensible and secure interface and methodology. [26]

This program seems inactive. Last news or online forum activity dates from 2012.

1.19.4 Cloud Trust Protocol

The CTP API is designed to be a RESTful protocol that Cloud service customers can use to query a Cloud service provider (CSP) on current security attributes related to a Cloud service such as the current level of availability of the service or information on the last vulnerability assessment.

The following figures provides a general idea of the principles of CTP through 3 simple use cases where a Cloud service customer uses CTP to query a Cloud service provider about security attributes of its services.

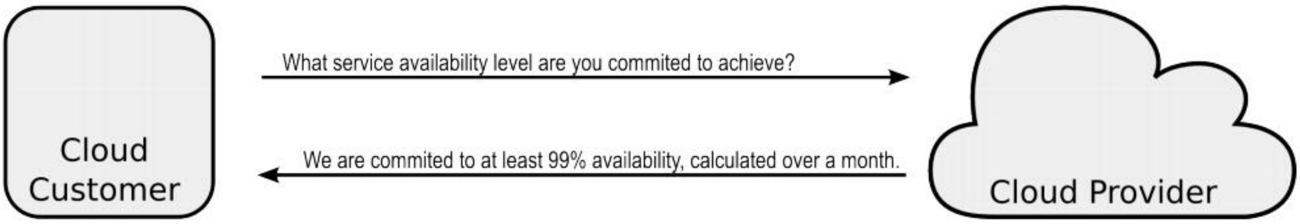

Cloud Customer
What service availability level are you commited to achieve?
We are commited to at least 99% availability, calculated over a month.
Cloud Provider

Figure 11 - Availability query [27]

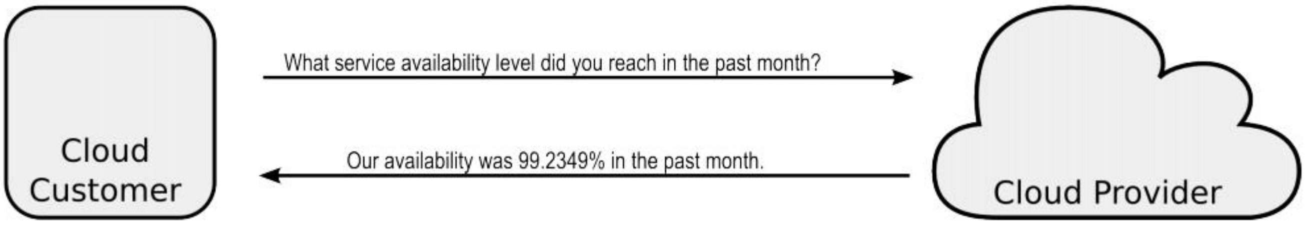

Cloud Customer
What service availability level did you reach in the past month?
Our availability was 99.2349% in the past month.
Cloud Provider

Figure 12 - History of availability [27]

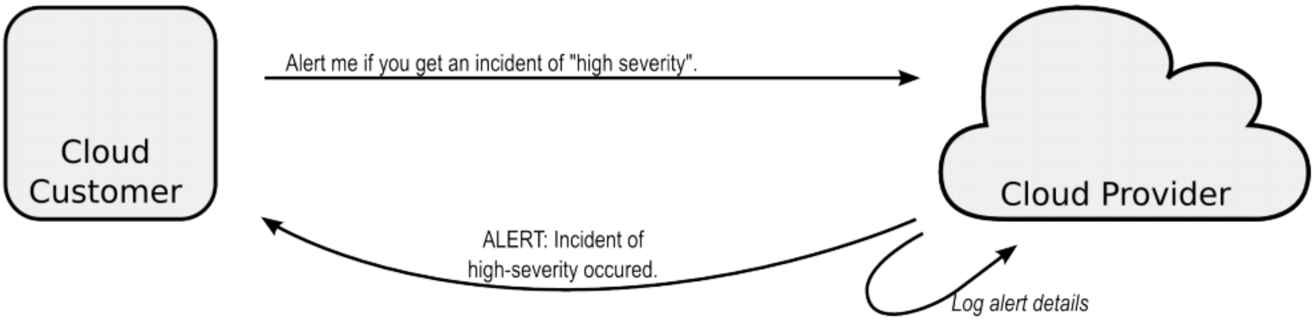

Cloud Customer
Alert me if you get an incident of "high severity".
Cloud Provider
ALERT: Incident of high-severity occured.
Log alert details

Figure 13 - Alert incident [27]

1.20 Risk Management

1.20.1 ISO 31000:2009 Risk management – Principles and guidelines

ISO 31000:2009, Risk management – Principles and guidelines, provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, effectively allocate and use resources for risk treatment.

However, ISO 31000 cannot be used for certification purposes, but it does provide guidance for internal or external audit programmes. Organizations using it can compare their risk management practices with an internationally recognised benchmark, providing sound principles for effective management and corporate governance. [28]

1.20.2 Federal Risk and Authorization Management Program (FedRAMP)

Federal Risk and Authorization Program is a risk management program that provides a standardized approach for assessing and monitoring the security of Cloud products and services. It is an initiative from the government of the United States to accelerate the adoption of secure Cloud solutions.

FedRAMP authorizes Cloud systems in a three-step process:

1. **Security Assessment** – The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.

2. **Leveraging and Authorization** – Federal agencies view security authorization packages in the FedRAMP repository and leverage the security authorization packages to grant a security authorization at their own agency.

3. **Ongoing Assessment & Authorization** – Once an authorization is granted, ongoing assessment and authorization activities must be completed to maintain the security authorization.

FedRAMP is the result of close collaboration with cybersecurity and Cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defence (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry. [29]

1.21 Assets in the Cloud [11]

The Cloud Security Alliance gives the following advice when an organization want to move to the Cloud with some of their assets:

1.21.1 Identify the Asset for Cloud Deployment

Assets supported by the Cloud fall into two general categories:

1. Data

2. Applications / Functions / Processes

With Cloud computing our data and applications do not necessarily need to reside in the same location. It is possible to host an application in a private datacentre and outsource a portion of its functionality to the Cloud through a Platform as a Service.

1.21.2 Evaluate the Asset

In this step the organization needs to determine how important the data or function is to the organization. For each asset, the following questions should be asked:

- How would the organization be harmed if the asset became widely public and widely distributed?

- How would the organization be harmed if an employee of the Cloud provider accessed the asset?

- How would the organization be harmed if the process or function were manipulated by an outsider?

- How would the organization be harmed if the process or function failed to provide the expected results?

- How would the organization be harmed if the information / data were unexpectedly changed?
- How would the organization be harmed if the asset were unavailable for a period of time?

With these questions the organization is assessing confidentiality, integrity and availability requirements for the asset.

1.21.3 Map the Asset to Potential Cloud Deployment Models

Now that the organization has an understanding of the importance of the asset. The next step is to determine which deployment model is best to minimize risk.

The organization needs to determine if it is willing to accept the following options: public, private internal / external, community or hybrid.

1.21.4 Evaluate Potential Cloud Service Models and Providers

In this step, the organization should focus on the degree of control they have to implement risk mitigations in the different SPI tiers. (SPI = SaaS, PaaS, IaaS). At this point, the organization might switch to a fuller risk assessment.

1.21.5 Map out the potential data flow

When the organization is evaluating a specific deployment option, they need to map out the data flow between the organization, the Cloud service and any customer/other nodes. Most of these steps have been high-level, but before making a final decision, it is essential to understand whether, and how, data can move in and out of the Cloud.

1.22 Top threats to Cloud computing

According to a study conducted by the Cloud Security Alliance (CSA) these are the top 9 Cloud Computing Top threats in 2013:

1. **Data breaches** – Sensitive data falls into the hands of competitors.
2. **Data Loss** – Losing important company data
3. **Account Hijacking** – An attacker gains access to your credentials and can eavesdrop of your activities and transactions, manipulate data, return falsified information and redirect clients to illegitimate sites.
4. **Insecure APIs** – Badly designed security for API's.
5. **Denial of Service (DoS)** – DoS attacks are meant to prevent users of a Cloud service from being able to access their data or their applications.
6. **Malicious Insiders** – A current of former employee with authorized access that misuses that access to negatively affect the confidentiality, integrity or availability of the organizations information systems.

7. **Abuse of Cloud Services** – Attackers can use the Cloud to help them attack an organization.

8. **Insufficient Due Diligence** – Adopting the Cloud without a complete understanding of the CSP environment, applications or services being pushed to the Cloud.

9. **Shared Technology Issues** – Vulnerabilities in infrastructure that make multi-tenancy possible.

1.23 Shadow-IT

Shadow-IT is a term used to define IT applications and hardware that are used by employees in a company without any formal IT department approval.

“We classify Shadow-IT as an insider threat which is caused by the human factor of an organization. We consider this human factor to be an insider (i.e. employee) who installs non-approved software without having any malicious intentions.”

[30]

The reason employees use non-approved IT applications is because of the fact that they are better and/or easier to use than the applications the organization offers. For example when an employee wants to share a large file with a client, they might use WeTransfer or Dropbox because the email attachment limit was too small.

The motivation for Shadow-IT is generally not malicious. Employees believe they are not doing anything illegal, especially when installing open-source software.

Making users aware of Shadow-IT is not always easy, one example is the following situation:
“When I warned the CEO of the company that I would need to uninstall all the non-approved software he had installed – he answered that he is the CEO and he needs all those apps”

Primary concerns about Shadow-IT [31]:

1. Security of corporate data in the Cloud (49%)

2. Potential compliance violations (25%)

3. The ability to enforce policies (19%)

4. Redundant services creating inefficiency (8%)

1.24 Compliance

Many industries need to comply with certain certifications. The health care sector in the United States for example needs to certify that their computing service complies with the Health Insurance Portability and Accountability Act (HIPAA). When a healthcare related business wants to move their computation operations to the Cloud, it will require that the Cloud Service Provider complies with the HIPAA certification for its service.

Some of the US certification:

- **HIPAA: Health Insurance Portability and Accountability Act** – This Act sets some rules for handling patient data in the healthcare sector.
- **SOX: Sarbanes Oxley** – An act for accounting firms.
- **GLBA: Gramm-Leach-Bliley Act** – Act for financial companies.
- **FISMA: Federal Information Security Management Act** – This act is for federal agencies regarding information security.
- **SAS 70: Statement on Auditing Standards** – An auditing standard for independent auditors.
- **PCI DSS: Payment Card Industry Data Security Standard** – Deals mostly with Point of Sale terminals having the adequate security safeguards.

2 *Focus, methodology and use cases*

During the technological research it became clear that private Cloud did not add many new risks caused by the adoption of Cloud, most of the risks were risks that a traditional IT infrastructure also has. Therefore, it was decided to focus on the risk of a data breach when using Public Cloud SaaS Cloud services in an enterprise. A public Cloud SaaS service brings most of the new risks that are associated with adoption of the Cloud.

In large enterprises, the Chief Information Officer (CIO) is often convinced that Cloud services are not used within the organization. However, this is in many cases not realistic, discovery assessments by Skyhigh networks show an average of 987 Cloud services in use per organization. [32]

When the use of Cloud services is not officially sanctioned, an organization is still subjected to the risks that come with Cloud adoption. This is called Shadow-IT.

In the book “Controls and Assurance in the Cloud: Using COBIT 5” the following figure is used to visualize the risk with the different deployment and service models.

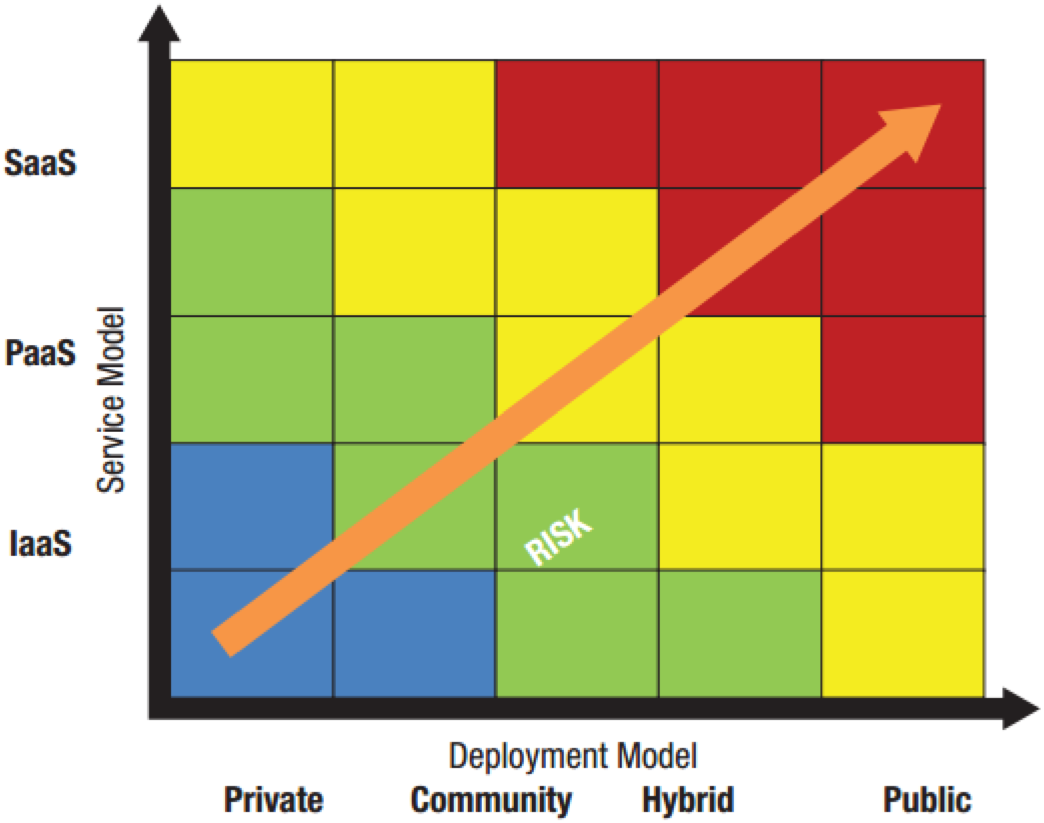


Figure 14 Cloud Computing Risk Map [33]

Two use cases will be introduced to give an example on how the new Cloud risks can be addressed properly. The use cases will be used to make a risk assessment about the adoption of a public Cloud SaaS application in the organization.

The following chapters will be partially based upon ISO standards. The figure below gives a high level overview on Risk Management according to ISO 31000:2009.

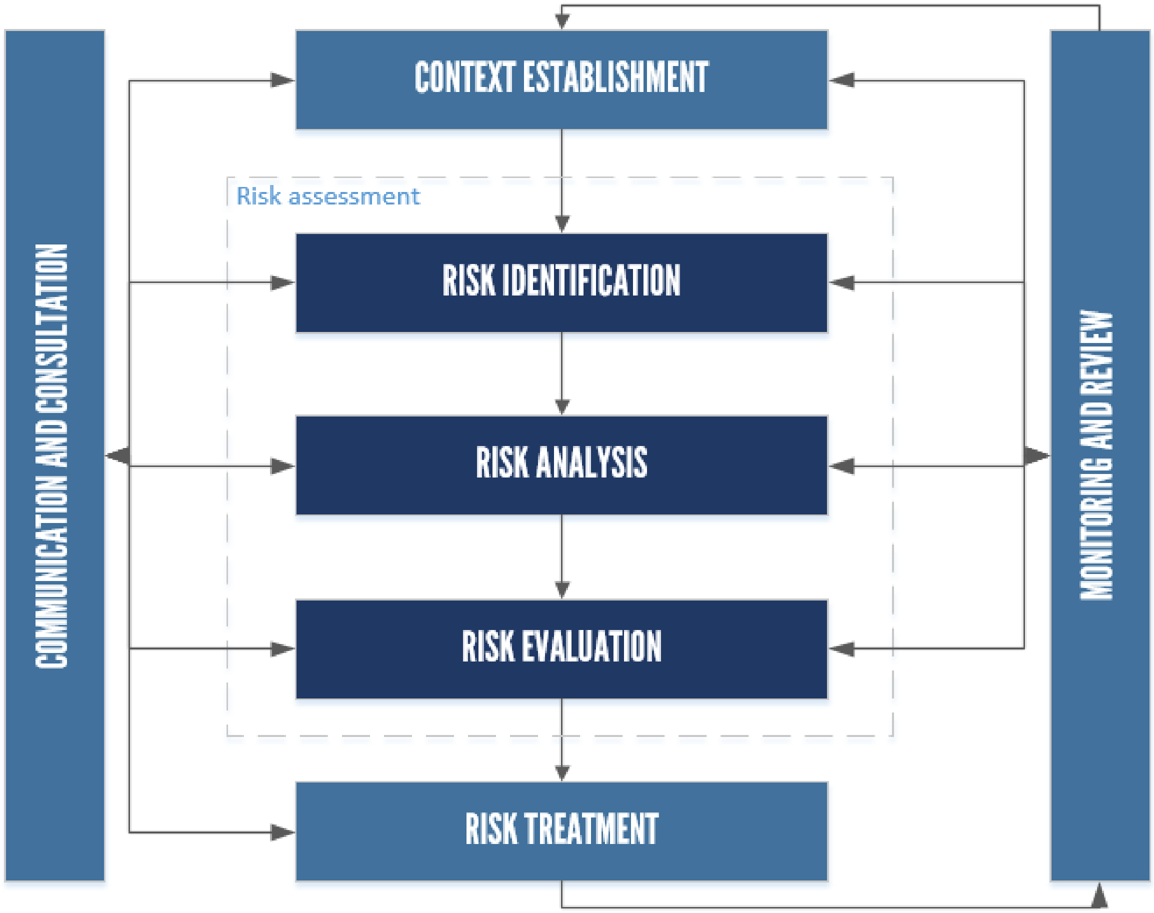


Figure 15 - The risk management process [28]

Risk management is a continuous procedure that should not be done only once. In this thesis an initial partial risk assessment will be done. It is out of scope to do a complete risk assessment, the focus of the risk assessment will be data breaches caused by the use of public Cloud SaaS.

First, the context establishment is describing the use case scenario.

After gaining an overview of the use case, a listing will be made with all the threats to the company. The analysis approach is threat-oriented. *A threat-oriented approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are* *identified based on adversary intent.* [34] This step can be linked to the Risk Identification of ISO 31000:2009.

For each threat event the likelihood and the impact is determined specific to the use case. Combining the likelihood and the impact results in the risk of that threat event. This is a combination of the Risk Analysis and Risk Evaluation steps of the ISO standard.

The last chapters of this thesis “How to protect Cloud services for an enterprise?” and “How to handle a data breach?” can be linked to the Risk treatment part of the risk management process. With protection techniques the risk of the threat is minimized. Not all risks can be brought down to zero, so the company needs to know how to respond to an attack. With a good incident response plan, the impact of a data breach can be minimized which also lowers the risk.

[redacted] Use case scenarios

The following text will provide a description of the different use cases to illustrate a risk assessment.

2.1.1 Harvard University Google Apps

Harvard University is a university located in Cambridge and Boston, Massachusetts, United States and has an enrolment of over 20,000 students. The University offers Google Apps to students to facilitate collaboration with each other. This use case was chosen because of the detailed information available about the use of Google Apps.

Besides Google Apps the University also has SharePoint which is used mostly by faculty and staff members for more confidential data.

Harvard University has a data classification table which illustrates the importance of different classified information.

The use case guidance and data classification table can be found in Appendix A.

Because a university is not exactly the same as an enterprise another use case is added to include the differences.

2.1.2 Foursquare Dropbox for Business

Foursquare is a company that develops the apps Foursquare and Swarm. The Foursquare app is a location based social network where users can share places and review them. Swarm is also a location based social network, but here users can share their own location.

As the business of Foursquare grew it quickly became apparent that they needed a more robust, reliable solution for sharing files across locations. They chose Dropbox as the best solution for digital collaboration. It became a centralized repository for critical assets. It enables easy access to client contracts, sales presentations and internal collateral. Eric Friedman, Director of Sales and Revenue Operations says: “Our rule of thumb has become: if it’s not in Dropbox, it doesn’t exist”.

The full use case can be found in Appendix B.

2.1.3 Shadow-IT: Confessions of a rogue marketer

This use case is different from the previous two because here a user started using public Cloud SaaS applications that were not approved by the IT department. This also creates other risks to the organization.

In the use case a marketer confesses why he used different Cloud services without approval. He used the Cloud for file sharing, storage, project management and collaboration services. At any given moment he had at least four active subscriptions to Cloud services that he used for business purposes.

The reason why he was using these Cloud services was to get his job done as efficiently as possible. Tight deadlines, high project volume and lofty campaign goals caused him to turn to the Cloud for agility.

The full article of this use case can be found in Appendix C.

3 What is the risk of a data breach in the Cloud?

Intro

Enterprises will only consider Cloud adoption when they have the assurance their date is safe. Data security and data loss protection is of utmost importance to these large companies.

Before protecting the enterprise data, it is necessary to have a clear overview of the different threats, attacks and vulnerabilities. Identifying possible threats and threat sources requires the use of different sources, along with the experience of the risk assessor.

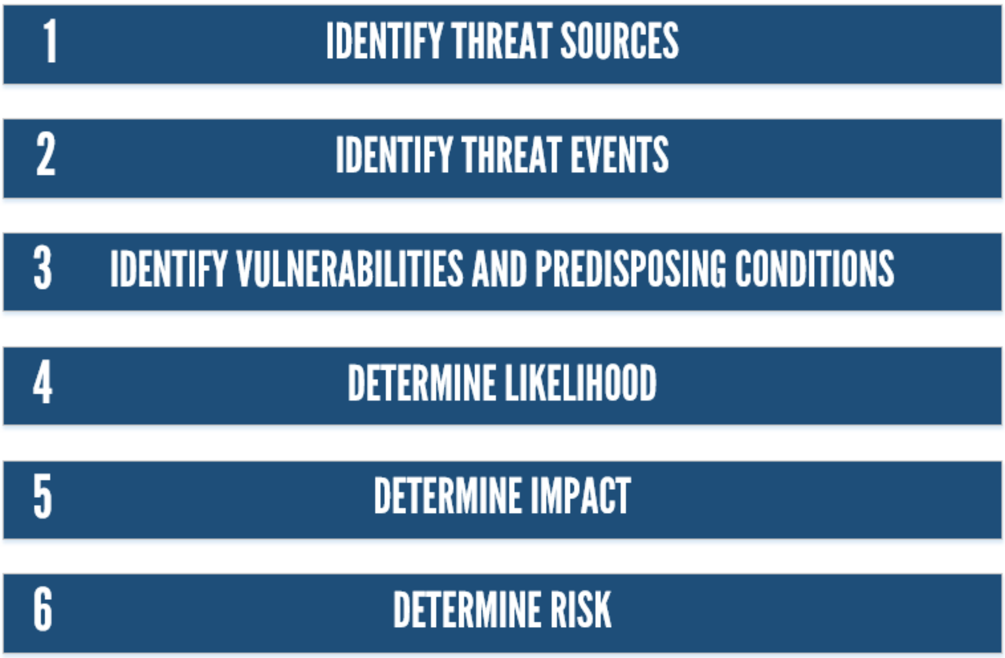
This chapter will cover the most important threats, attacks and vulnerabilities associated with the use of a public SaaS service within an enterprise. Even if an organization does not officially sanction such a service, employees may still use them (Shadow-IT).

The Cloud specific threats are examined on their likelihood and impact. Combining these factors creates the risk of this threat. To illustrate these risks in an enterprise context, use cases are linked to the threats that cause data breaches and data losses.

It is important to acknowledge that although the use of public Cloud SaaS in an enterprise creates new threats, it also mitigates or negates some of the current security threats.

Structure

Special publication 800-30 by NIST gives the following advice to produce a list of information security risks.



1 IDENTIFY THREAT SOURCES

2 IDENTIFY THREAT EVENTS

3 IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS

4 DETERMINE LIKELIHOOD

5 DETERMINE IMPACT

6 DETERMINE RISK

Figure 16 - NIST Steps to produce list of Information Security risks

In the risk assessment that follows on the use cases Harvard and Foursquare, step 2 & 3 will not be done exactly as NIST recommends in SP 800-30. The method that NIST provides has many factors to incorporate in the assessment that required information that was not available. Some of these factors will be incorporated in the decision of likelihood and/or impact but will not be assessed separately.

In addition, steps *2 Identify threat events* and *3 Identify vulnerabilities and predisposing conditions* will be done differently. The terms threat, risk, vulnerability are often used with different meanings. The following figure gives a good overview on the definition of a threat: "interaction of actor, motivation and vulnerability".

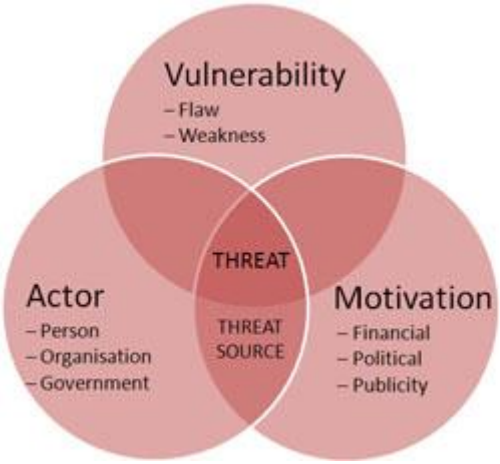


Figure 17 - Threat visualisation [35]

In the risk assessment, the vulnerabilities of public SaaS are listed first and then these vulnerabilities will be used to list the different threats.

3.3 Identify threat sources

For each threat, there is a threat source, knowing this threat source is essential to gain a complete understanding of the risk it poses. Some literature refers to threat source as threat agent or threat actor.

The following text is based on Table D-2: Taxonomy of Threat Sources that is part of the Special Publication 800-30 by NIST.

NIST SP 800-30 categorizes the different threats in four groups:

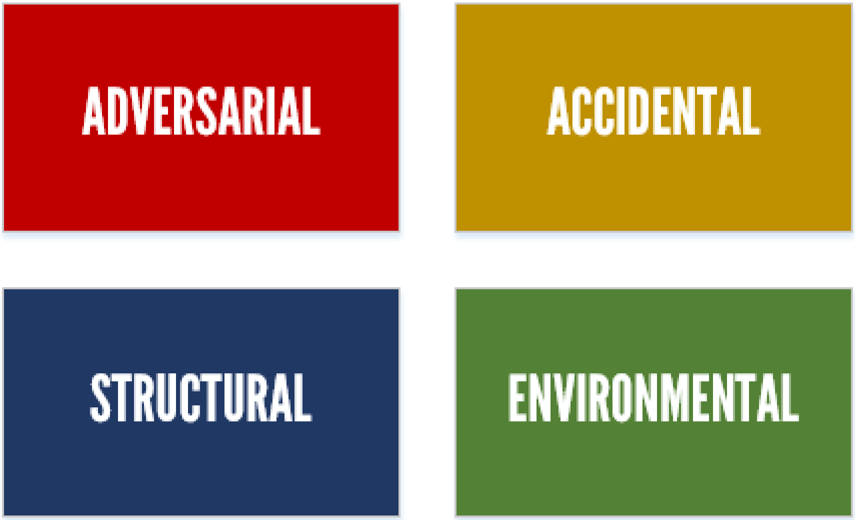


Figure 18 - Threat Sources

3.3.1 Internal vs External threats

There is a clear distinction between threats in an organization:

- **Internal threats** – these are threats that originate from inside the organization. For example an employee who just got fired wants to take revenge and tries to send all confidential data to a competitor.
- **External threats** – all threats that originate from outside the organization are classified as external threats. For example, someone who tries to brute-force the password of a legitimate user on the VPN web interface of the organization.

3.3.2 Adversarial threat source

Individuals, groups, organizations or states that seek to exploit the organization’s dependence on cyber resources.

Individual

In this category it is necessary to make a difference between internal and external individuals. Both can bring harm to the organization but they have to be treated as different threats.

An example of an internal individual threat is an employee who just got fired and wants to take revenge on the company. He copies all the confidential data he can access to an USB-stick and hands it over to the competitor.

An example of an external individual threat is a hacker defaces the company website via a vulnerability found in the Content Management System (CMS).

Group

A group threat is similar to the threat of an individual but they may have more resources to exploit a vulnerability. A real world example of an external group threat source is the Lizard Squad which was an active hacking group in 2014. They took the servers of the game League of Legends offline with a DDoS attack. This attack was of unseen scale with a bandwidth of 600Gbps.

Organization

Organization threat sources can be competitors that try to gain access to confidential data to gain information about the future decisions. It can also be a supplier, partner or customer that tries to gain advantage by misusing cyber resources.

Nation state

It is no big secret anymore that government intelligence agencies spy on all sorts of organizations. Edward Snowden has spread information about the American National Security Agency (NSA) that reveals extensive spying operations on governments, organizations and individuals.

The malware detected on computer systems of Belgacom is an example of nation state hacking. In leaked documents from the NSA it was confirmed that the British surveillance agency Government Communications Headquarters was behind the attack, codenamed Operation Socialist.

3.3.3 Accidental threat source

Erroneous actions taken by individuals in the course of executing their everyday responsibilities.

An employee can lose his smartphone by accident and when this smartphone is not properly protected the finder of this phone could possible access confidential company data.

Network and Infrastructure administrators can make a configuration mistake which for example could allow external access to confidential data.

3.3.4 Structural threat source

Failures of equipment, environmental controls, or software due to aging, resource depletion or other circumstances which exceed expected operating parameters.

Depending on the infrastructure the organization uses these threat sources can be caused by errors in storage, processing, communications, operating systems, networking …

3.3.5 Environmental threat source

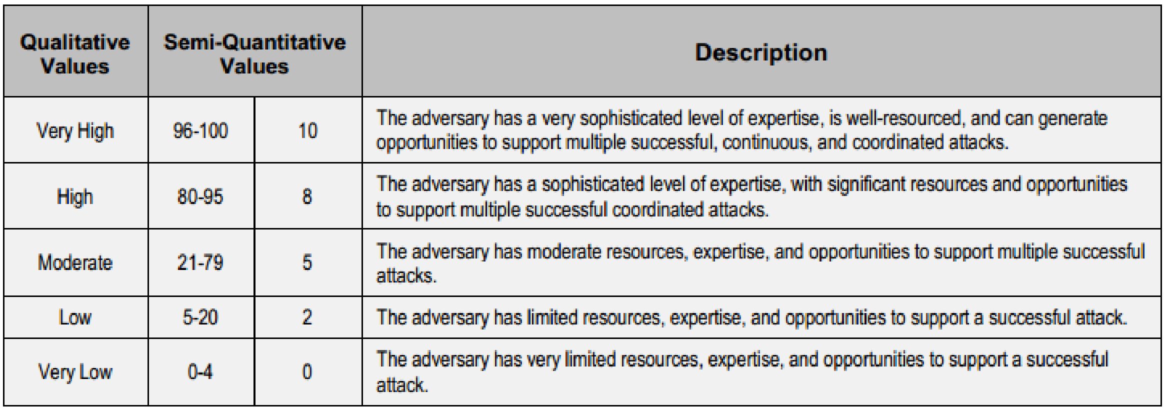
Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

Examples of these disasters include hurricanes, fires, tsunamis, earthquake …

3.3.6 Human threat source

When evaluating human threat sources SP800-30 gives the advice to make use of assessment scales on the capability, intent and targeting of the adversary. An example of such an assessment scale is given in the figure below.

- **Motivation** – Why would they target this organization; how motivated are they?
- **Capability** – What is their level of skill in exploiting the threat?
- **Resources** – How much time, money, and other resources could they deploy?
- **Probability of attack** – How likely and how often would your assets be targeted?
- **Deterrence** – What are the consequences to the attacker of being identified?



Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Figure 19 - Assessment scale - Characteristics of adversary capability

While it is worth considering using this technique to assess the human threat sources this way, it is not necessary. In the risk assessment for this thesis, these factors are incorporated in the likelihood of a threat event.

Public SaaS specific vulnerabilities

3.4.1 Risk increasing factors

The following are the risk increasing factors specific to SaaS Cloud computing from the book "Security Considerations for Cloud Computing"

- **S1.D Legal trans-border requirements** – Because data in the Cloud can be anywhere, it is necessary to think about the legal requirements, especially concerning personal private information. Data protection may not be possible in data centres located in high-risk countries.

- **S1.E Multitenancy and isolation failure** – In a multi-tenant environment the different resources should be isolated, when this is not the case, other tenants would be able to see confidential data.

- **S1.F Lack of visibility surrounding technical security measures in place** – A lot of the security responsibility is for the CSP, therefore the customer needs to know what security measures are in place to have some sort of assurance that their data is safe.

- **S1.G Absence of Disaster Recovery Plan (DRP) and backup** – When no proper back-ups are made and there is no DRP, the risk of unavailability or data loss will be very high for an enterprise.

- **S1.H Physical Security** – In all public Cloud models the data centre is not located on the enterprise's premises, therefore the responsibility of physical security is for the CSP.

- **S1.I & S3.D Data disposal (infrastructure and service level)** – When data is deleted in the Cloud, it should really be deleted in the datacentre too. If the contract with the CSP expires, the data should be completely be disposed in a safe manner. When a hard disk is recycled there is a risk that confidential data still remains when it was not properly deleted.

- **S1.J Offshoring infrastructure** – Information send to the Cloud needs to be transferred over the internet. This needs to be done in a secure manner to assure the confidentiality and integrity of the data.

- **S1.K Virtual Machine (VM) security maintenance** – For public Cloud SaaS the CSP is responsible for the security maintenance of the VM's. When important security patches are unapplied to an inactive VM, this VM can then be compromised when activated.

- **S1.L Cloud provider authenticity** –It is the enterprise's responsibility to check the identity of the Cloud provider to ensure that it is not an imposter.

- **S2.B Application mapping** – When the functionality of the Cloud service does not align with the existing business processes additional undesirable features could be introduced.

- **S2.C Software-oriented architecture (SOA) related vulnerabilities** – New challenges are with SOA so new vulnerabilities should be recognized. The vulnerabilities may not be visible to the enterprise since the CSP is responsible for the SOA libraries.

- **S3.C Data ownership** – It should be clearly defined who is the owner of the data between the enterprise and the CSP.

- **S3.E Lack of visibility into software systems development life cycle (SDLC)** – Because of the lack of visibility the customer does not know how secure the applications are developed.

- **S3.F Identity and access management (IAM)** – When there are no clear roles and responsibilities it may be possible for users to access data they are not supposed to access.

- **S3.G Exit strategy** – Vendor-lock-in is a commonly known problem, so an exit strategy has to be considered.

- **S3.H Broad exposure of applications** – Public Cloud SaaS applications have a broader exposure which increases the attack space.

- **S3.I Ease to contract SaaS** – SaaS applications are very easy to start using so business units may contract Cloud applications which are in conflict with internal enterprise policies.

- **S3.J Lack of control of the release management process** – CSPs are able to release patches quickly and that may cause unexpected side effects on the enterprise.

- **S3.K Browser vulnerabilities** – Most public Cloud SaaS are offered via the web browser, so when a web browser becomes infected, the access to the application can be compromised.

Here follow some other risk factors that are not specific to the Cloud, but that increase because of the use of public Cloud SaaS.

- **Dependency on Internet connection** – Even more than before the organization is dependent on an internet connection. When the internet is unavailable, all Cloud services are unavailable too.

- **Cloud services have a broad adoption** – Because a lot of enterprises are able to use these Cloud applications easily, adversaries are more likely to focus their attacks on these services.

[redacted] Identify threats

In a full risk assessment, a list of all threats would be created that are applicable for the organization. The thesis will focus on the **threats specific to the public Cloud SaaS.**

Threats that are not specific to the Cloud can obtain a higher risk because of the use of Cloud. An example of such threat is a natural disaster. When the datacentre of the Cloud provider is located in an area with a higher likelihood of hurricanes the risk of unavailability will increase.

The following threats are the focus of the risk assessment in this thesis. These threats will be split up in different threats linked to different vulnerabilities.

DATA LOSS
DATA BREACH
Data theft, disclosure

Figure 20 - Main threats

[redacted] Risk Assessment

3.6.1 Approach

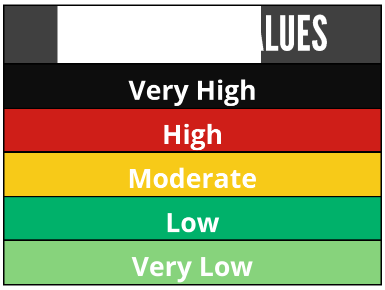
In the following risk assessment, the different threats are assessed with a **qualitative approach**. This means that the risk is expressed with a level like low, medium, high. In a quantitative approach the risk would be expressed in money.

Most risk assessments use a qualitative approach, rather than a quantitative approach. The goal is to order the resulting risks to help determine which need to be the most urgently treated, rather than to give them an absolute value. [36]

3.6.2 Determine likelihood and impact

For the **likelihood** and **impact** of a threat event, the following assessment scale will be used:

Table 4 -Assessment Scale Threat Events Likelihood & Impact



LUES
Very High
High
Moderate
Low
Very Low

Likelihood

The likelihood is the probability that a certain threat will result in the impact linked to that threat. For example, the probability that an earthquake will occur or the probability that a hacker succeeds in compromising the admin account.

- **Very High** – Very likely to occur
- **High** –Likely to occur
- **Moderate** – May occur at some time
- **Low** – Not very likely to occur but there is a chance
- **Very Low** – Virtually no chance of happening

Impact

The impact for each qualitative value can be described as follows:

- **Very High** – Serious business impact, breach of all data or complete data loss, losing control over management.
- **High** – Severe data breach, important data is leaked which could lead to serious business consequences. Compromised account can be used to gain more access to critical assets.
- **Moderate** – Compromise of user account, can be recovered by administrator. Data breach of less important data.
- **Low** – Low business impact. Data breach of unimportant data. Data loss can be recovered easily.
- **Very Low** – Virtually no impact on business.

3.6.3 Determine risk

The **risk** is obtained by combining the **likelihood** and the **impact**. The following table from the NIST SP 800-30 will be used for risk determination.

Table 5 - Assessment Scale - Level of Risk - NIST SP 800-30

	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

3.7 Risk assessment on use cases

3.7.1 Data Loss

T1. **CSP Hardware Confiscation**		
Description	When a criminal uses the Cloud infrastructure of a CSP for illegal purposes, hardware could be confiscated by law enforcement agencies. This can have serious consequences for the other customers of the CSP.	
Example	In 2012 the file sharing company MegaUpload was shut down. MegaUpload was accused of sharing unauthorized copies of films, songs and other digital entertainment. All servers were seized by the government agencies and consumer data was taken offline.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	No significant likelihood increasing factors	No significant likelihood increasing factors
Likelihood decreasing factors	↓ Google Apps is not known for illegal activities ↓ Legal procedures in place ↓ Hosting in low risk countries ↓ Big company, many customers ↓ Redundant infrastructure ↓ Not likely that all infrastructure will be confiscated	↓ Dropbox is not known for illegal activities ↓ Legal procedures in place ↓ Hosting in low risk countries ↓ Hosted on third party infrastructure (Amazon) ↓ Big company, many customers ↓ Redundant infrastructure ↓ Not likely that all infrastructure will be confiscated
Likelihood Total	**Very Low** Google hosts its platform on their own datacentres located all over the world. Government agencies can request data but need a legal process to force google to disclose user information. It is most unlikely that all their hardware will be confiscated. Google Apps has a redundant system. They aim to have a 0 recovery time objective (RTO). Even when a certain server is confiscated, the data will still be available on another server.	**Very Low** Dropbox works with third party service providers for the Dropbox Infrastructure and all datacentres are located in the United States. Legal procedures are in place for law enforcement agencies. Dropbox has several redundant systems to prevent data loss. Even when a certain server is confiscated, the data will still be available on another server.
Impact increasing factors	↑ Student data will be lost	↑ Critical assets will be lost
Impact decreasing factors	↓ No important data is stored on Google Apps	↓ Dropbox works with synchronisation to local computer so not all data will be lost
Impact	**Low** None of the high-risk confidential data is hosted on Google.	**High** **Dropbox synchronizes with files on the local computer, which prevents total loss of data** in case of CSP disruption.
Risk	**Very Low**	**Low**

T2. **CSP Bankruptcy**		
Description	If the Cloud Provider goes bankrupt, it is only a matter of time before the service goes offline.	
Example	In 2013 the Cloud service provider Nirvanix went down after a price war with big-name Cloud storage vendors like Microsoft, Google and Rackspace. Nirvanix gave their customers 2 weeks time to get their data out of the Nirvanix Cloud.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	No significant likelihood increasing factors	No significant likelihood increasing factors
Likelihood decreasing factors	↓ Google Apps has no financial problems ↓ Many customers ↓ Major player in SaaS solutions	↓ Dropbox has no financial problems ↓ Many customers ↓ Major player in file share service
Likelihood	**Very Low** Google Apps has many customers. As such it is very unlikely that the company goes bankrupt in the near future.	**Very Low** Dropbox is one of the major players in the file sharing business. They were founded in 2008 and have a user base of 400 million users. They just raised $1.1 billion [37] so it is unlikely that they go bankrupt in the near future.
Impact increasing factors	↑ Student data will be lost	↑ Critical assets will be lost
Impact decreasing factors	↓ No important data is stored on Google Apps	↓ Dropbox works with synchronisation to local computer so not all data will be lost
Impact	**Low** Students and faculty members will not be able to collaborate on Google Apps anymore. None of the high-risk confidential data is hosted on Google Apps but **everything on Google Apps may get lost.** There is no synchronisation to safe collaboration files offline.	**High** Since all critical assets are stored on Dropbox a CSP disruption may have serious impact on the business. The impact is set on High instead of Very High because the **Dropbox service stores files on the local computer which prevents total loss of data** in case of CSP disruption.
Risk	**Very Low**	**Low**

Poor / No Disaster Recovery

T3. **Natural Disaster**		
Description	Natural disaster could be a hurricane, tornado, fire, flooding … Planning on a natural disaster is called Disaster Recovery. Disaster Recovery is usually measured in two ways: Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The RPO is how much data you're willing to lose when things go wrong and RTO is how long you're willing to go without service after a disaster. [38]	
Example	A fire hits the datacentre of a Cloud provider. The CSP didn't have any kind of disaster recovery. There was no offsite datacentre provided or any kind of high availability or disaster recovery plan. The Cloud service is down and will take a very long time to get back online. All customer data is destroyed so it will be very unlikely that the Cloud provider will ever be in business again. This is a worst-case scenario since most of the large Cloud providers do have an offsite datacentre.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	No significant likelihood increasing factors	No significant likelihood increasing factors
Likelihood decreasing factors	↓ Redundant infrastructure	↓ Redundant infrastructure
Likelihood	**Very Low** Google has their own infrastructure and their datacentres are located all over the world. Their RPO design target is zero data loss and their RTO design target is instant failover.	**Very Low** There is no clear disaster recovery plan available online. Dropbox has datacentres on different locations and they claim in BCR-01 of the CSA Cloud matrix that they have established disaster recovery plans that are tested at regular intervals. In the business agreement article 12.i Force Majeure they state that neither the customer nor Dropbox is liable for a natural disaster.
Impact increasing factors	↑ Student data will be lost	↑ Critical assets will be lost
Impact decreasing factors	↓ No important data is stored on Google Apps	↓ Dropbox works with synchronisation to local computer so not all data will be lost
Impact	**Low** None of the high-risk confidential data is hosted on Google.	**High** Since critical assets are stored on Dropbox the loss or unavailability of certain documents may cause some business impact. With Dropbox the files are normally also stored locally so data loss is minimized.
Risk	**Very Low**	**Low**

3.7.2 Data Breach

Management Interface Compromise

■ **Brute force attack Admin credentials**		
Description	A brute force attack tries to guess the users password using a dictionary or random combinations of characters. The target here is the management interface of the Cloud Service.	
Example	In 2014 some accounts of iCloud, the Cloud service by Apple, were hacked. The accounts were from famous celebrities and the hackers published some private pictures online. The attack was a simple password guessing attack, which used a list of frequently used passwords.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Public access to login form ↑ No two-factor authentication ↑ Students that like to test things	↑ Public access to login form ↑ No two-factor authentication ↑ Reuse of passwords
Likelihood decreasing factors	↓ Security Awareness ↓ Security Policy that requires strong passwords ↓ Limited amount of login attempts	↓ Limited amount of login attempts
Likelihood	**Moderate**	**High**
	In the public Cloud everyone can see the login form. It is very likely that someone will try to guess the password of a user. This may or may not be automated. Two-factor authentication is optional in Harvard University. Worst case is assumed here. Students will probably try to guess / brute force the password.	In the use case article, it is not mentioned whether two-factor authentication is mandatory. The worst-case scenario will be assumed, two-factor authentication is not mandatory. In 2011, Dropbox suffered a bug which allowed any password to be accepted causing an enormous security issue for all users. Dropbox employees not be likely to brute force admin login.
Impact increasing factors	↑ Management interface compromised ↑ Student data breached	↑ Management interface compromised ↑ Critical assets breached
Impact decreasing factors	↓ No important data is stored on Google Apps	No significant impact decreasing factors
Impact	**Moderate**	**Very High**
	The Google Apps platform could be altered, data and accounts could be deleted. The high-confidential data is stored on SharePoint.	When the management Interface is compromised, the attack can change accounts, access critical assets, delete data, …
Risk	**Moderate**	**Very High**

■ Social Engineering Admin Account		
Description	Social Engineering is an attack that relies mostly on human interaction. It often involves tricking people into doing things they did not intent. Social Engineering can be used in many ways, sometimes adversaries call the victims on the phone while other techniques involve creating fake websites, emails, letters …	
Example	The Syrian Electronic Army (SEA), a hacker collective which supports the Assad regime in Syria uses social engineering to trick users into compromising their corporate Google Accounts. Via spear phishing they send a malicious email with a misleading link to a YouTube video, the link however directs the user to a rogue site controlled by the SEA. A fake google login page is displayed and the credentials of the user are stolen. If two factor authentication is present, their rogue site initiates the verification with google in real time in the background.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Public access to login form ↑ No two-factor authentication ↑ Students that like to test things	↑ Public access to login form ↑ Target of skilled adversaries ↑ No two-factor authentication
Likelihood decreasing factors	↓ Security awareness ↓ No target for skilled adversaries	No information available with significant likelihood decreasing factors, least secure context is presumed
Likelihood	**Moderate**	**Very High**
	Student in Harvard might like to try to get the admin credentials.	Because it is known that foursquare stores critical assets on Dropbox, more skilled adversaries might try to social engineer to get the admin credentials.
Impact increasing factors	↑ Management interface compromised ↑ Student data breached	↑ Management interface compromised ↑ Critical assets breached
Impact decreasing factors	↓ No important data is stored on Google Apps	No significant impact decreasing factors
Impact	**High**	**Very High**
	The Google Apps platform could be altered, data and accounts could be deleted. The high-confidential data is stored on SharePoint.	When the management Interface is compromised, the attack can change accounts, access critical assets, delete data, …
Risk	**Moderate**	**Very High**

Account and Credentials Hijacking

T6. **Brute force attack User Credentials**		
Description	A brute force attack tries to guess the users password using a dictionary or random combinations of characters. The target here is the user account of the targeted user.	
Example	In 2014 some accounts of iCloud, the Cloud service by Apple, were hacked. The accounts were from famous celebrities and the hackers published some private pictures online. The attack was a simple password guessing attack which used a list of frequently used passwords.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Public access to login form ↑ No two-factor authentication ↑ Students that like to test things ↑ Students do not care about security policy	↑ Public access to login form ↑ No two-factor authentication ↑ Reuse of passwords
Likelihood decreasing factors	↓ Security Awareness ↓ Security Policy that requires strong passwords ↓ Limited amount of login attempts	↓ Limited amount of login attempts
Likelihood	**Moderate**	**High**
	In the public Cloud everyone can see the login form. It is very likely that someone will try to guess the password of a user. Two-factor authentication is optional at Harvard University.	In the use case article, it is not mentioned whether two-factor authentication is mandatory. The least secure scenario will be assumed so two-factor authentication is not mandatory. In 2011, Dropbox suffered a bug which allowed any password to be accepted causing an enormous security issue for all users. Dropbox will be very wary not to let that happen again.
Impact increasing factors	↑ Student data breached	↑ Critical assets breached
Impact decreasing factors	↓ No important data is stored on Google Apps	↓ Data breached for one user
Impact	**Low**	**High**
	None of the high confidential data is stored on Google Apps so the impact is low.	The adversary will have access to the critical assets that are stored on that account.
Risk	**Low**	**High**

T7. **Social Engineering User Account**

Description	Social Engineering is an attack that relies mostly on human interaction. It often involves tricking people into doing things they did not intent. Social Engineering can be used in many ways, sometimes adversaries call the victims on the phone while other techniques involve creating fake websites, emails, letters …	
Example	The Syrian Electronic Army (SEA), a hacker collective that supports the Assad regime in Syria uses social engineering to trick users into compromising their corporate Google Accounts. Via spear phishing they send a malicious email with a misleading link to a YouTube video, the link however directs the user to a rogue site controlled by the SEA. A fake google login page is displayed and the credentials of the user are stolen. If two factor authentication is present their rogue site initiates the verification with google in real time in the background.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Public access to login form ↑ No two-factor authentication ↑ Students that like to test things ↑ Students do not care about security policy	↑ Public access to login form ↑ Target of skilled adversaries ↑ No two-factor authentication
Likelihood decreasing factors	↓ Security awareness ↓ No target for skilled adversaries	No information available with significant likelihood decreasing factors, least secure context is presumed
Likelihood	**High** Students might not care about security policy. The passwords could be very weak.	**Very High** Because it is known that foursquare stores critical assets on Dropbox, more skilled adversaries might try to social engineer to get user credentials.
Impact increasing factors	↑ Student data breached	↑ Critical assets breached
Impact decreasing factors	↓ No important data is stored on Google Apps	↓ Data breached for one user
Impact	**Low** None of the high confidential data is stored on Google Apps.	**High** The adversary will have access to the critical assets that are stored on that account.
Risk	**Low**	**High**

T8. **Man in the Cloud attacks**		
Description	A man in the Cloud attack exploits the vulnerability of synchronisation tokens. File storage Cloud services often make use of a local client that syncs data to the Cloud (Dropbox, Google Drive, OneDrive ...). With man in the Cloud attacks, adversaries steal the synchronization token and are able to download the victim’s files through the Cloud service. Stealing the synchronisation token consists of running a tool (Switcher) which can be achieved through a drive-by-download exploit or through a simpler Phishing attack. A full technical report about Man in the Cloud attacks is available via this link: https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf	
Example	A specific example of this attack in the wild is not available but researchers at Blue Coat Systems believe that a stealthy cyber-espionage framework dubbed Inception has made use of this kind of attack.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Google drive is vulnerable ↑ Drive-by download exploit ↑ Students are less careful in clicking links ↑ Not detected as malicious code	↑ Dropbox is vulnerable ↑ Drive-by download exploit ↑ Not detected as malicious code
Likelihood decreasing factors	↓ Security awareness ↓ Detection possible via file synchronisation service anomalies	↓ Detection possible via file synchronisation service anomalies
Likelihood	**High** Google Drive is vulnerable for this kind of attack. If anyone is vulnerable for the drive-by-download exploit, his or her account is compromised.	**High** Dropbox is vulnerable for this kind of attack.
Impact increasing factors	↑ Student data breached	↑ Critical assets breached ↑ Persistent
Impact decreasing factors	↓ No important data is stored on Google Apps	↓ Data breached for one user
Impact	**Low** None of the high confidential data is stored on Google Apps.	**High** The adversary will have access to the critical assets that are stored on that account. The synchronisation token does not change when the users changes his/her password.
Risk	**Low**	**High**

Side Channel Attacks

T9. **Cloud Side channel attacks**	
Description	Side Channel attacks are executed by requesting data with no actual information but the way the response is delivered is leaking the secret information you want. A non-technical example by cryptofails.com is given here: Suppose your birthday is coming up soon, and your best friend told you that they bought a gift for you. You’re anxious to know what they got you, so you ask them: "Is it a new watch?" “No.” (expression=neutral, eyes=looking at you) "Is it a hat?" “No.” (expression=neutral, eyes=looking at you) "Is it a computer?" “No.” (expression=neutral, eyes=looking at you) "Is it a book?" “No.” (expression=nervous, eyes=looking away from you) "Is it a video game?" “No.” (expression=relief, eyes=looking at you) Now can you guess what your gift is? From these results, you can be pretty sure that your gift is a book. If you want to be even more sure, you can ask the questions again. If your friend’s expression and eye movements are always changing after asking, “Is it a book?” you can be pretty sure that’s what it is. You’re getting no information from the actual data in the response (“No.”), but the way the response is delivered is leaking the secret information you want. [39] Cloud services are also vulnerable for these kinds of attacks. When file storage Cloud providers use **cross-user data deduplication** to store only a single copy of redundant data, an adversary can use this property to identify files, learn the content of files or create a covert channel. Another side channel attack is analysing the AJAX request from a search box like Google Search. With autocomplete the client sends search queries to the server for each character that the user types, the size of the result list will vary depending on what characters the user types. An eavesdropper could use the size of that result list to deduce which character the user typed. In a more detailed risk assessment the different kinds of side channel attacks would be split up into different threats and the risk would be calculated separately.
Example	The following example describes how a user (Alice) can learn the contents of a file that belongs to another user (Bob). Assume, for example, that Alice and Bob work in the same company, which uses a Cloud backup service to back up all of its employees’ machines. Once a year, all employees receive a new copy of a standard contract containing their updated salary. Alice wants to know Bob’s new salary, which is probably some multiple of $500 in the $50,000 to $200,000 range. All Alice has to do is generate a template of Bob’s contract, with Bob’s name and the date of the new contract, and then generate a copy of the contract for each possible salary (a total of 301 files). She then runs a backup to the company backup service that she and Bob use. The single file for which deduplication occurs is the one with Bob’s actual salary. [40]

	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Web application side channel attack	↑ Cross-user data deduplication
Likelihood decreasing factors	↓ No cross-user data deduplication ↓ No multi-tenant infrastructure	↓ Less useful attack for skilled adversaries
Likelihood	**Low** Cross-user data deduplication is not used for Google Drive so that is not a possible attack vector. Google has its own infrastructure so side channel attacks on the infrastructure are unlikely. There is however a chance of side channel attacks on the web applications of Google Apps.	**High** In 2010 cross-user data deduplication was an issue, the current situation however would require testing of the Dropbox Business system. Since Dropbox does not have its own infrastructure, side channel attacks on the shared infrastructure by other tenants are also possible. Dropbox was contacted via email and could not give an answer to the question whether the issue regarding cross-user data deduplication was resolved.
Impact increasing factors	↑ Student data breached	↑ Critical assets stored on Dropbox
Impact decreasing factors	↓ Limited amount of information through side channel attack	↓ For cross-user deduplication side channel attack a Dropbox account is required ↓ Limited amount of information through side channel attack
Impact	**Low** None of the high confidential data is stored on Google Apps.	**High** Since critical assets are stored on Dropbox, an incident like the example above with Alice and Bob could have serious consequences for the company since private information about employees could be accessed.
Risk	**Low**	**High**

No Clear data ownership

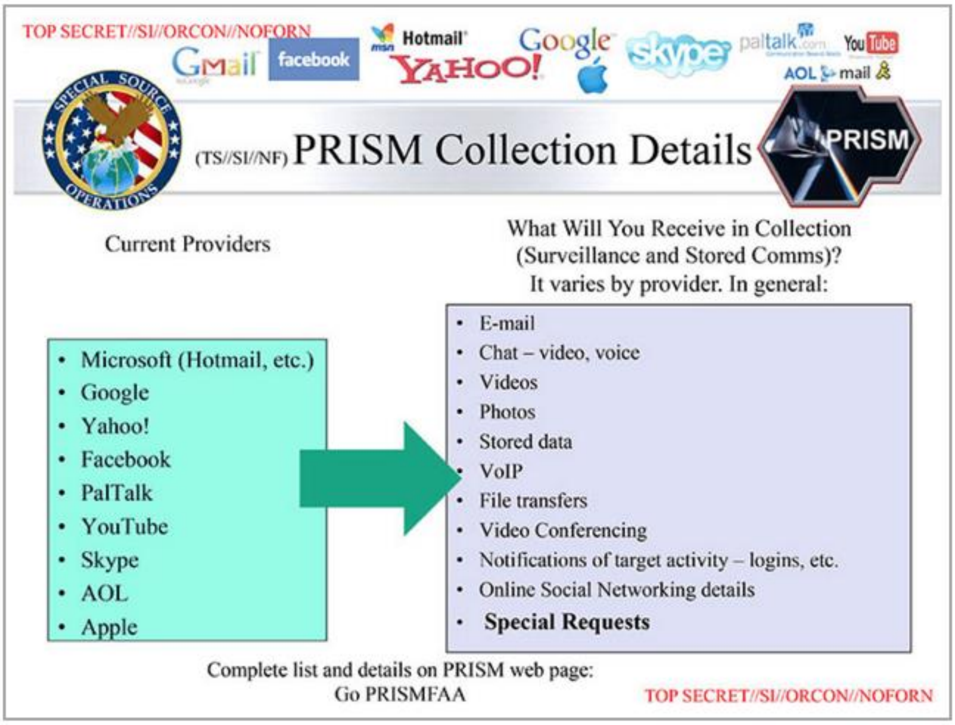
T10. Company data owned by CSP		
Description	When an organization makes use of a Cloud service the ownership of the data may be changed by using certain functions of this Cloud service. In some cases, contracts must be signed to assure the organization that it remains the owner of its data.	
Example	Company A uses a Cloud service for file storage. The contract was set for 5 years and has just expired. Company A would like to change to another CSP but access to their data is prohibited. The terms of agreement state that the data stored on the Cloud belongs to the Cloud provider. The CSP requires a certain amount of money from Company A to retrieve their data.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	No significant likelihood increasing factors	No significant likelihood increasing factors
Likelihood decreasing factors	↓ Google statement: "Google does not own your data"	↓ Dropbox statement: "Your stuff is yours"
Likelihood	**Very Low** Google Apps has a clear statement regarding data ownership: "Google does not own your data"	**Very Low** Dropbox also has a clear statement regarding data ownership: "Your Stuff is yours"
Impact increasing factors	↑ Students would lose ownership over data	↑ Critical assets would become property of CSP
Impact decreasing factors	↓ No important data is stored on Google Apps	No significant impact decreasing factors
Impact	**Low** None of the high confidential data is stored on Google Apps.	**Very high** Critical assets should remain sole property of foursquare.
Risk	**Very Low**	**Low**

Malicious Insiders

T11. **Malicious Insider**		
Description	A malicious insider is an employee that misuses his/her access to the organizations network, system or data to negatively affect the confidentiality, availability or integrity of the organizations information systems.	
Example	In 2008 Terry Childs, a network administrator for the San Francisco's network refused to give the passwords of the FiberWAN system to his supervisors. Childs was the only person with access to that system. When a new security manager was appointed, Childs felt threatened when he was required to share access to the system. He was arrested on the evening of July 12 but even then he refused to give up the passwords to the system. Childs offered to give the passwords only to Mayor Newson and on July 21 the Mayor paid Childs a visit in prison and received the passwords.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Disgruntled Google apps administrator	↑ Disgruntled employees
Likelihood decreasing factors	↓ Students and faculty members are not likely to pose a threat through Google Apps	↓ Segregation of duties
Likelihood	**Moderate** Students and faculty members are not very likely to pose a threat through the Google Apps service.	**High** A disgruntled employee may decide to delete critical assets through the Dropbox system or share confidential files with other parties.
Impact increasing factors	↑ Student data breach	↑ Critical assets stored on Dropbox ↑ Possible administrator
Impact decreasing factors	↓ No important data is stored on Google Apps	No significant impact decreasing factors
Impact	**Low** No high-confidential data is stored on Google Apps.	**Very High** Critical assets could be exposed. If the insider is the administrator for Dropbox the consequences could be disastrous.
Risk	**Low**	**Very High**

No legal data protection

<table>
<tr><th colspan="3">[redacted] Foreign government espionage</th></tr>
<tr><td><b>Description</b></td><td colspan="2">Government espionage is when a foreign government tries to steal intellectual property, confidential research, financial reports, …
Given the location independent nature of Cloud computing, the risk of foreign government espionage increases.</td></tr>
<tr><td><b>Example</b></td><td colspan="2">The surveillance program from the NSA code-named PRISM that was leaked by Edward Snowden in 2013 discloses how much data the NSA could acquire.
Most of the large Cloud service providers were included in the program as the following slide of a leaked presentation shows.



TOP SECRET//SI//ORCON//NOFORN
(TS//SI//NF) PRISM Collection Details
Current Providers
• Microsoft (Hotmail, etc.)
• Google
• Yahoo!
• Facebook
• PalTalk
• YouTube
• Skype
• AOL
• Apple
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
• E-mail
• Chat – video, voice
• Videos
• Photos
• Stored data
• VoIP
• File transfers
• Video Conferencing
• Notifications of target activity – logins, etc.
• Online Social Networking details
• <b>Special Requests</b>
Complete list and details on PRISM web page: Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN
Figure 21 - PRISM slide [41]

Most of the companies in that list deny involvement in the PRISM program. These were initial public statements by Google and Dropbox:
• <b>Google</b> – "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a backdoor for the government to access private user data."
• <b>Dropbox</b> – “We’ve seen reports that Dropbox might be asked to participate in a government program called PRISM. We are not part of any such program and remain committed to protecting our users’ privacy.”

There is some doubt however on these statements since companies who received an order under the FISA amendments act are forbidden by law from disclosing having received the order and disclosing any information about the order at all. (Mark Rumold, staff attorney at the Electronic Frontier Foundation) [42]</td></tr>
<tr><td></td><td><b>Google Apps for Harvard</b></td><td><b>Dropbox for Foursquare</b></td></tr>
</table>

Likelihood increasing factors	No significant likelihood increasing factors	No significant likelihood increasing factors
Likelihood decreasing factors	↓ Harvard and Google both U.S. organizations	↓ Harvard and Google both U.S. organizations
Likelihood	**Very Low** Harvard is an American University and Google is an American company. There is a chance that government agencies are looking at the data very likely not to cause harm or steal any research.	**Very Low** Dropbox and Foursquare are both American companies. Government espionage is unlikely aimed at them.
Impact increasing factors	↑ Student data breached	↑ Critical assets stored on Dropbox
Impact decreasing factors	• No important data is stored on Google Apps	No significant impact decreasing factors
Impact	**Low** No high-confidential data is stored on Google Apps.	**Very High** Exposure of critical assets.
Risk	**Very Low**	**Low**

Malware targeting Cloud

	[redacted] **Malware targeting Cloud**	
Description	Malware is not something new, but recent developments of malware include Cloud services as an attack vector.	
Example	In 2014 Adallom Labs discovered an unusual variant of the Zeus Trojan that targets Salesforce users. Zeus is malware that traditionally targeted online banking credentials and transactions. But now a variant of Zeus targets enterprise SaaS applications. It is not an exploit of a Salesforce.com vulnerability, this attack takes advantage of the trust relationship that is legitimately established between the end-user and Salesforce.com once the user has authenticated.	
	Google Apps for Harvard	**Dropbox for Foursquare**
Likelihood increasing factors	↑ Google Apps is popular Cloud service ↑ Students are less careful ↑ Personal laptops with no malware protection	↑ Dropbox is popular Cloud service ↑ Target of skilled adversaries ↑ No security awareness ↑ Access to Dropbox with personal devices
Likelihood decreasing factors	• Security Awareness	No information available to list significant likelihood decreasing factors, least secure context is presumed.
Likelihood	**High** Google Apps is a very popular Cloud service but due to the security awareness that Harvard provides the likelihood is set to High.	**Very High** Dropbox is one of the most popular file hosting Cloud service. It is likely that an unknowing user gets infected by malware.
Impact increasing factors	↑ Student data breach	↑ Critical assets breached ↑ Administrator infected personal device
Impact decreasing factors	• No important data is stored on Google Apps	No significant impact decreasing factors
Impact	**Low** A compromised account may be used for illegal purposes by the hacker entity.	**Very High** All critical assets could be exposed when the admin account is compromised. The administrator could have malware on his/her personal device.
Risk	**Low**	**Very High**

3.7.3 Risks overview

		[redacted]	[redacted]
T1	**CSP Hardware Confiscation**	VERY LOW	LOW
T2	**CSP Bankruptcy**	VERY LOW	LOW
T3	**Natural Disaster**	VERY LOW	LOW
T4	**Brute force attack Admin Credentials**	MODERATE	VERY HIGH
T5	**Social Engineering Admin Account**	MODERATE	VERY HIGH
T6	**Brute force attack User Credentials**	LOW	HIGH
T7	**Social Engineering User Account**	LOW	HIGH
T8	**Man in the cloud attacks**	LOW	HIGH
T9	**Cloud Side channel attacks**	LOW	HIGH
T10	**Company data owned by CSP**	VERY LOW	LOW
T11	**Malicious Insider**	LOW	VERY HIGH
T12	**Foreign government espionage**	VERY LOW	LOW
T13	**Malware targeting cloud**	LOW	VERY HIGH

The risk of data loss or data breach for Harvard University ranges from very low to moderate, mainly because the data they store on Google Apps is not valuable.

For Foursquare, the risk of data loss and data breaches ranges from low to very high. The data that is stored on Dropbox is critical which causes the impact to be much higher than the data for the Harvard use case.

It is important to know that the results do not represent a comparison between Google Apps and Dropbox.

[redacted] Shadow-IT

A description of Shadow-IT can be found in the Technology research chapter of this thesis. Shadow-IT is the term used for IT services that are used without approval of the organization's IT department. So public SaaS applications used without approval is also Shadow-IT.

The risk that Shadow-IT poses is substantial. According to discovery assessments by PwC and Skyhigh networks across Europe, the average number of Cloud services per organization is 987. [32]

Shadow-IT with Cloud services has arisen from the need for cheaper, faster and more agile solutions to achieve business goals, engage users & clients and exploit new opportunities to create competitive advantage. [32]

The key problem with Shadow-IT remains visibility. If the IT department is not aware of the problem, no security precautions can be implemented.

3.8.1 Use case Shadow-IT

The use case in Appendix C covers the story of a marketer that used unapproved Cloud services. Shannon Renz used the Cloud for file sharing, storage, project management and collaboration services. He had at least four active subscriptions to Cloud services that he used for business purposes.

The reason why he was using these services was not to intentionally compromise enterprise security, but rather **to get his job done as efficiently as possible**. With tight deadlines, high project volume and lofty campaign goals, **he needed the agility that the Cloud provides**.

3.8.2 Rise of Shadow-IT caused by Cloud

In a blogpost by Michael Higashi from CipherCloud he says: “Shadow-IT is by now in such rampant use that the very employees tasked with keeping enterprises safe from Shadow-IT are themselves adopting Shadow-IT.” [43]

The main reason why Shadow-IT has become such a problem is because it is so **easy**. Any employee from any department can use a Cloud service that suits their needs better than the solutions that are provided by the company they work for.

In many cases, the Cloud offers services that are **more user-friendly and accessible** than corporate-sanctioned enterprise solutions.

3.8.3 Cloud security issues for shadow-IT

- **Increased risk of data leaks** – The use of Cloud-based file sync and share services may cause data leakage due to inappropriate file or data access. [43]

- **Compliance issues** – Certain company data needs to comply to data privacy and security regulations. Some data needs to remain inside the borders of a country. The use of Shadow-IT can violate data privacy regulations simply by saving their data to the wrong Cloud service. [43]

4 *How to protect Cloud services for an enterprise?*

With public SaaS, security is a shared responsibility between the enterprise and the CSP. The security model for SaaS in the technology research tells us that the CSP is responsible for all aspects of the Cloud service.

It is important to make a good choice of CSP that offers the best security possible.

It is not because the vendor manages the security of the services that the company does not need to apply security practices. Security also means training employees to use Cloud services correctly and managing access control so only authorized users can access confidential data.

This chapter will cover what security controls can be used to provide better security for using Cloud services in an enterprise and how to deal with shadow-IT.

The security controls help to reduce risk. ISO 27001 includes this definition:

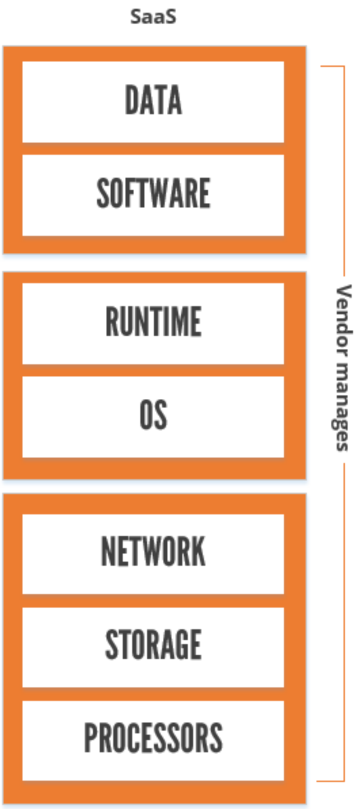


Figure 22 - SaaS Security Model

- **Control** – a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.

The focus in chapter 3 are the threats data loss and data breach for the use cases and the risk of Shadow-IT for any enterprise. This chapter will address these threats and suggest countermeasures to lower the risk that these threats pose for the organization.

In a whitepaper from CipherCloud [44] Cloud services are split up into three categories:

- **Non-sanctioned shadow-IT**

- **Sanctioned collaboration applications**

- **Core business process applications**

They use the following figure as further illustration.

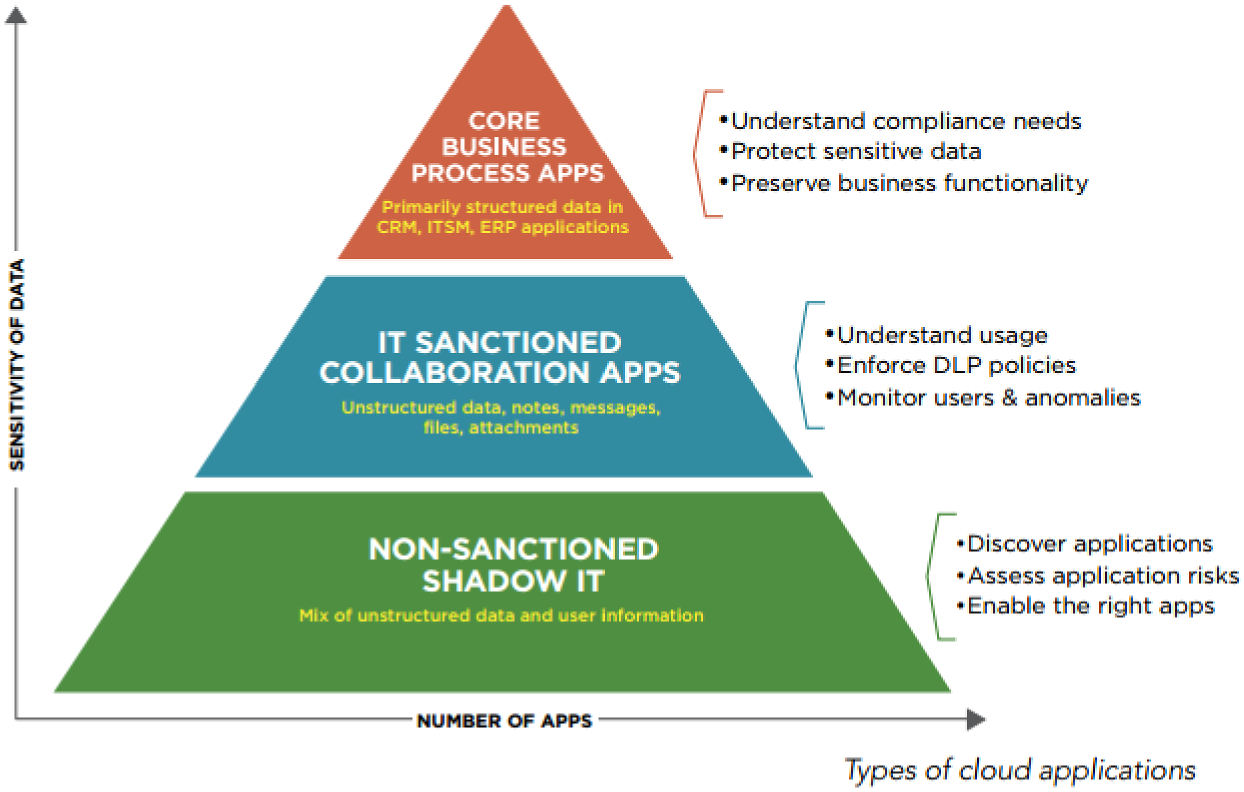

CORE
BUSINESS
PROCESS APPS
Primarily structured data in CRM, ITSM, ERP applications
•Understand compliance needs
•Protect sensitive data
•Preserve business functionality
IT SANCTIONED
COLLABORATION APPS
Unstructured data, notes, messages, files, attachments
•Understand usage
•Enforce DLP policies
•Monitor users & anomalies
NON-SANCTIONED
SHADOW IT
Mix of unstructured data and user information
•Discover applications
•Assess application risks
•Enable the right apps
SENSITIVITY OF DATA
NUMBER OF APPS
Types of cloud applications

Figure 23 - CipherCloud Types of Cloud applications [44]

The figure represents the ideal situation. If only non-sensitive data is stored on non-sanctioned Cloud services the risk of Shadow-IT would be low. The reason why the risk of Shadow-IT is high is that critical business data could be stored on these Cloud services without the enterprise knowing.

When there is no visibility into Shadow-IT, the figure would be more like the following:

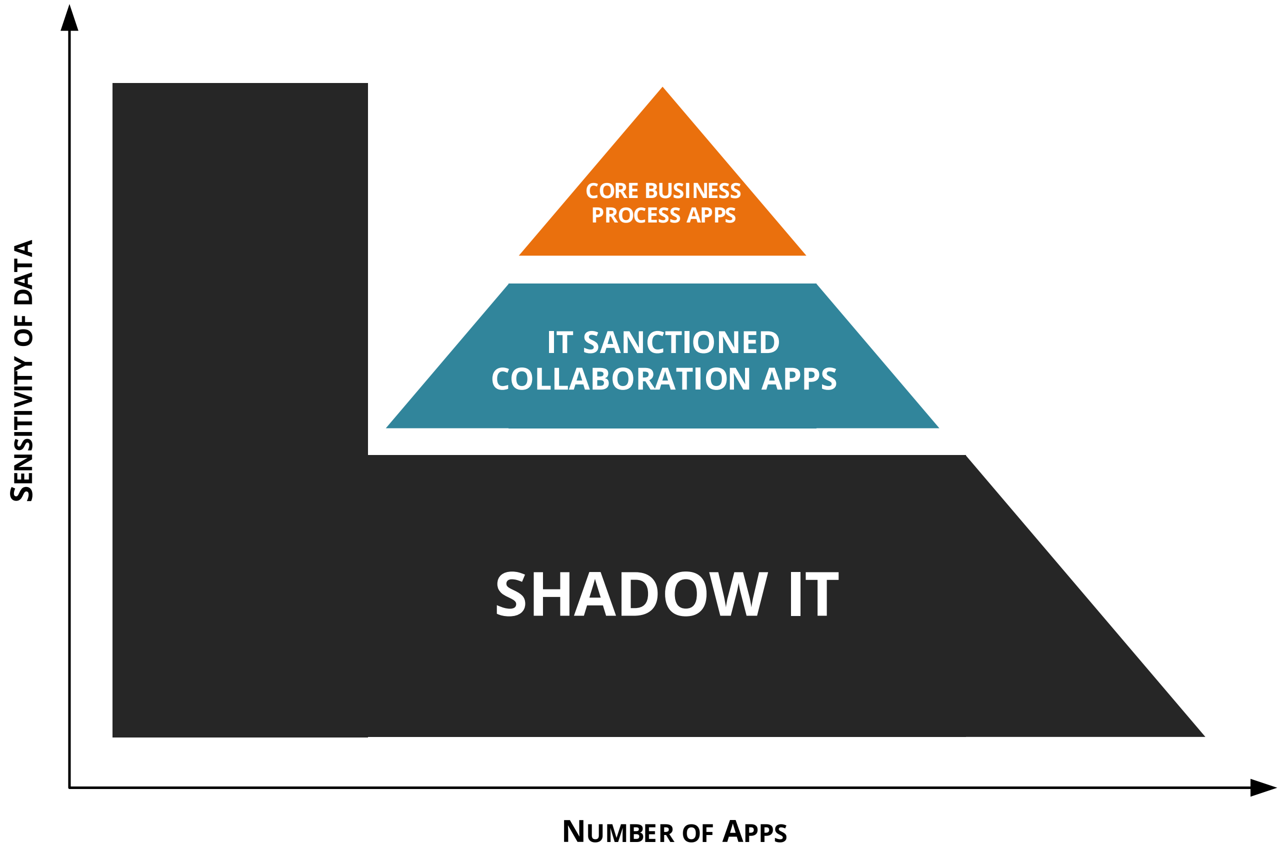


Figure 24 - Types of Cloud applications

The three different use cases link to these different categories:

- Dropbox for Foursquare links to core business process apps
- Google Apps for Harvard University links to IT sanctioned collaboration apps
- The Shadow-IT use case evidently links to Shadow-IT

To protect Cloud services there are numerous security controls that can be implemented. The controls can belong to different classes: management, operational, technical or a combination.

4.1 Structure

1. Risk treatment
2. List new security controls
3. Apply to use cases

4.2 Risk treatment

For treating risks, the method from the book Computer Security by Stallings and Brown will be used.

In most cases the threats with the highest risk rating are prioritized. In some cases management may choose to first threat the smaller risks because they can be resolved much more easy than the other risks. There is also an economic side to consider, to mitigate risks there is a cost involved. Low-level risks with a high treatment cost will be uneconomic to accept as the following figure illustrates.

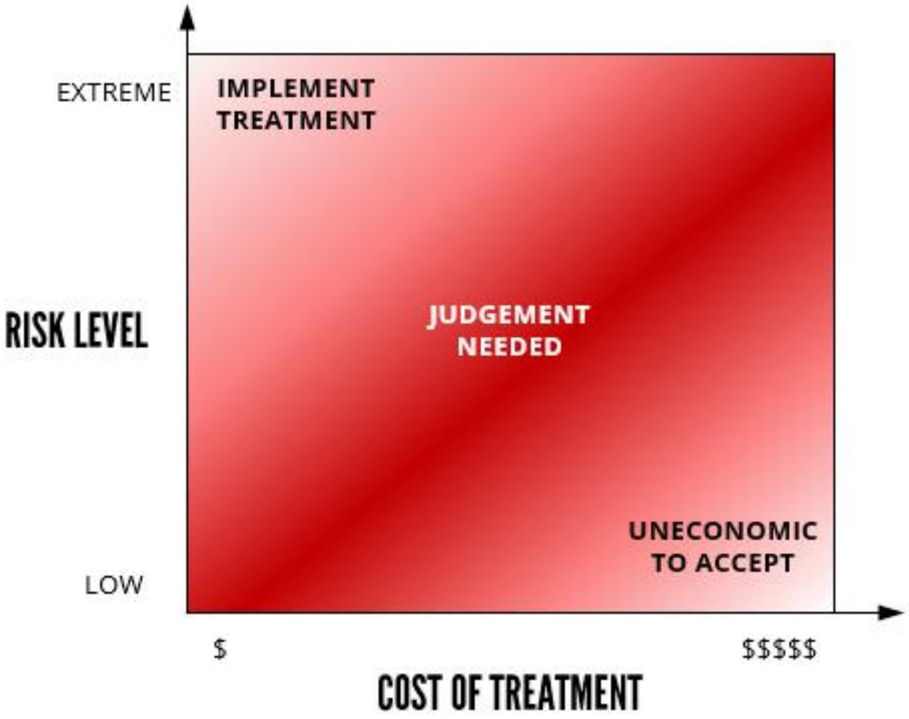


Figure 25 - Judgement about Risk Treatment [36]

The book Computer Security [36] lists five broad alternatives available to management for treating identified risks:

- **Risk acceptance** – Choosing to accept a risk level greater than normal for business reasons. This is typically due to excessive cost or time needed to treat the risk. Management must then accept responsibility for the consequences to the organization should the risk eventuate.

- **Risk avoidance** – Not proceeding with the activity or system that creates this risk. This usually results in loss of convenience or ability to perform some function that is useful to the organization. The loss of this capability is traded off against the reduced risk profile.

- **Risk transfer** – Sharing responsibility for the risk with a third party. This is typically achieved by taking out insurance against the risk occurring, by entering into a contract with another organization, or by using partnership or joint venture structures to share the risks and costs should the threat eventuate.

- **Reduce consequence** – By modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur. This could be achieved by implementing controls to enable the organization to quickly recover should the risk occur. Examples include implementing an off-site backup process, developing a disaster recovery plan, or arranging for data and processing to be replicated over multiple sites.
- **Reduce likelihood** – By implementing suitable controls to lower the chance of the vulnerability being exploited. These could include technical or administrative controls such as deploying firewalls and access tokens, or procedures such as password complexity and change policies. Such controls aim to improve the security of the asset, making it harder for an attack to succeed by reducing the vulnerability of the asset.

4.3 Choice of CSP

Not all of the risks can be met with countermeasures from the enterprise, some of the risks depend on the internal procedures and countermeasures specific for the CSP

The following risks from the use cases are the most related to the choice of CSP:

- CSP Hardware Confiscation
- CSP bankruptcy
- Natural Disaster
- Company data owned by CSP
- Foreign government espionage

These risks also present themselves in an outsourced data centre or with on premise hosting. The priority of these risks however will be different.

4.3.1 CSP hardware confiscation & bankruptcy

Risks like CSP hardware confiscation and bankruptcy are related to the reputation and financial situation of the CSP. Before starting to use Cloud services from a CSP it is necessary to do a background check on the CSP.

MegaUpload, the example of hardware confiscations was accused of hosting mainly pirated or illegal content. The file sharing service was commonly known as a source of illegal content, so from a business perspective it was not the best option to host business critical data. More respected Cloud providers with own data centres will have much less risk of hardware confiscations. They often have procedures to handle with government agencies, should illegal content appear on their services.

A big company like Google is not very likely to go bankrupt, a new start-up for Cloud services may have some trouble when they do not find enough customers. Just as with any third party the enterprise would like to work with, a financial background check is recommended.

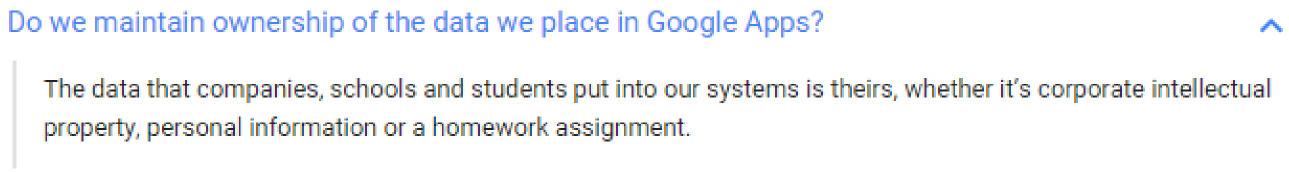
4.3.2 Natural disaster

The risk of a natural disaster can be mitigated by means of a redundant, high available setup comprising multiple, geographically dispersed data centres. A disaster recovery plan should be in place. This is the responsibility of the CSP. The enterprise needs to check what the disaster recovery plan is for the CSP.

Disaster recovery is usually defined by two parameters: Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The RPO is the maximum amount of data that gets lost during an incident. The RTO is the time it takes to recover from a data loss event.

4.3.3 Company data owned by CSP

It is important to check the user agreement with the CSP. The user agreement should have a clause that enables the customer to remain the owner of the data they store on the Cloud service. This is in particular important when tools provided by the CSP (e.g. google drive) can alter the data. In the figure below a clause from the google user agreement is displayed.



Do we maintain ownership of the data we place in Google Apps?

> The data that companies, schools and students put into our systems is theirs, whether it’s corporate intellectual property, personal information or a homework assignment.

Figure 26 - Data ownership for Google Apps [45]

4.3.4 Foreign Government espionage

When choosing a CSP it might be worth considering in what country the CSP operates. When a company is looking for a Cloud service to store their top-secret development designs of a new product, China might not be the best option. In regions such as China laws may allow local government unlimited access to the data regardless of its sensitivity. It might even be prohibited to encrypt data without ensuring local authorities can decrypt it as needed. [46] Different countries have different laws regarding the protection of privacy. Some data is bound by local law to remain within a country (e.g. Belgian law prohibits storing and manipulating medical information)

4.3.5 CSA Cloud Matrix and Consensus Assessments Initiative Questionnaire (CAIQ)

The CSA offers a tool that can help to check whether the CSP is a good match for your business requirements. The Cloud matrix is an excel file with controls that link to questions from the Consensus Assessments Initiative Questionnaire. Some CSPs have a publicly available CAIQ. The figure below illustrates an example from the Dropbox CAIQ.

Table 6 - Human Resources control [47]

Control group	Human Resources – Employment termination
CGID	HRS-04
CID	HRS-04.1
	HRS-04.2
Control Specification	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.
Consensus Assessments Questions	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?
	Do the above procedures and guidelines account for timely revocation of access and return of assets?
Comments and notes	Dropbox follows document procedures to govern changes in employment or termination. The procedures do account for timely revocation of access and return of assets.

4.4 Security policies

Security policies are a collection of several documents. The book “Security Policies and Implementation Issues” [13], defines the following types of documents:

- **Principles** – Establish the tone at the top and the authority by which policies are enforced
- **Policy** – A document that states ow the organization is to perform and conduct business functions and transactions with a desired outcome
- **Standard** – An established industry norm or method, which can be a procedural standard or a technical standard implemented organization-wide
- **Procedure** – A written statement describing the steps required to implement a process
- **Guideline** – A parameter within which a policy, standard, or procedure is suggested but optional
- **Definitions** – Statements that define the terms used in the policy documents and set the context in which the policies documents are interpreted

The combination of these documents describe how the organization handles security on all organizational levels.

Security policies rely on security controls to enforce their rules. The other way around, security controls are systematically put in place because of security policies. The following figure gives an overview on the relation between them.

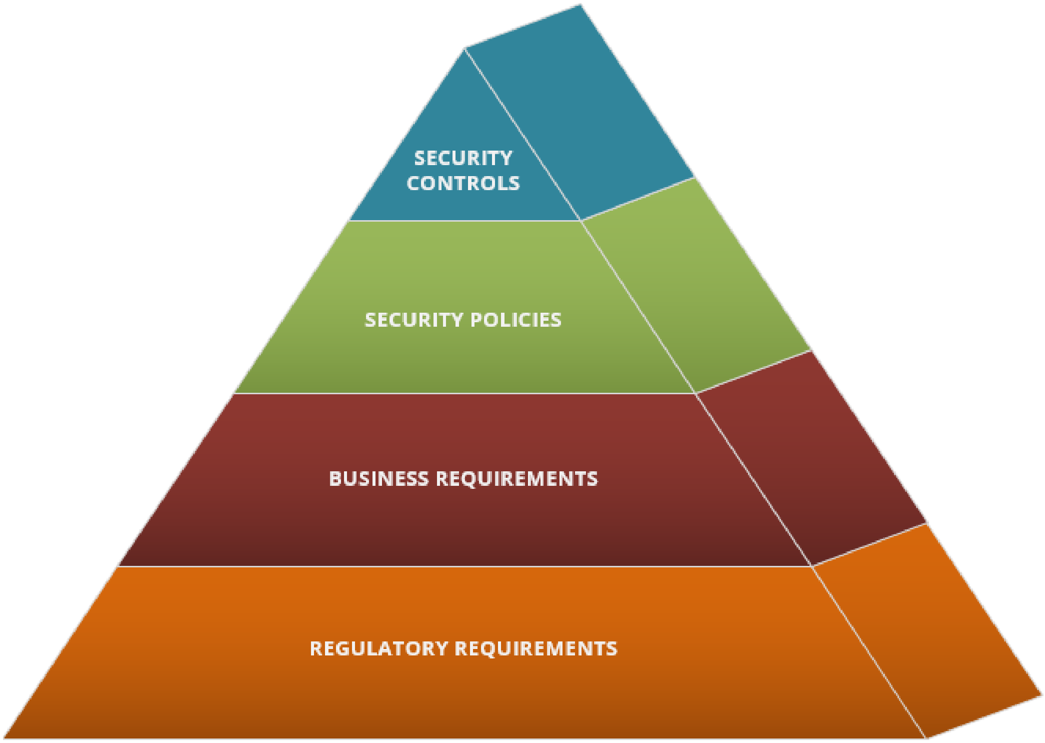


Figure 27 - Key relationships of security policies [13]

A policy can for example describe that all passwords used for company login credentials must be secure. This will result in a procedure that specifically describes how to achieve secure passwords. For example, minimum length of 10 character, expiration of passwords after 30 days and no reuse of old passwords. Security controls are the actual implementation of the procedure.

It is important that senior management supports the security policy and ensures that it is enforced.

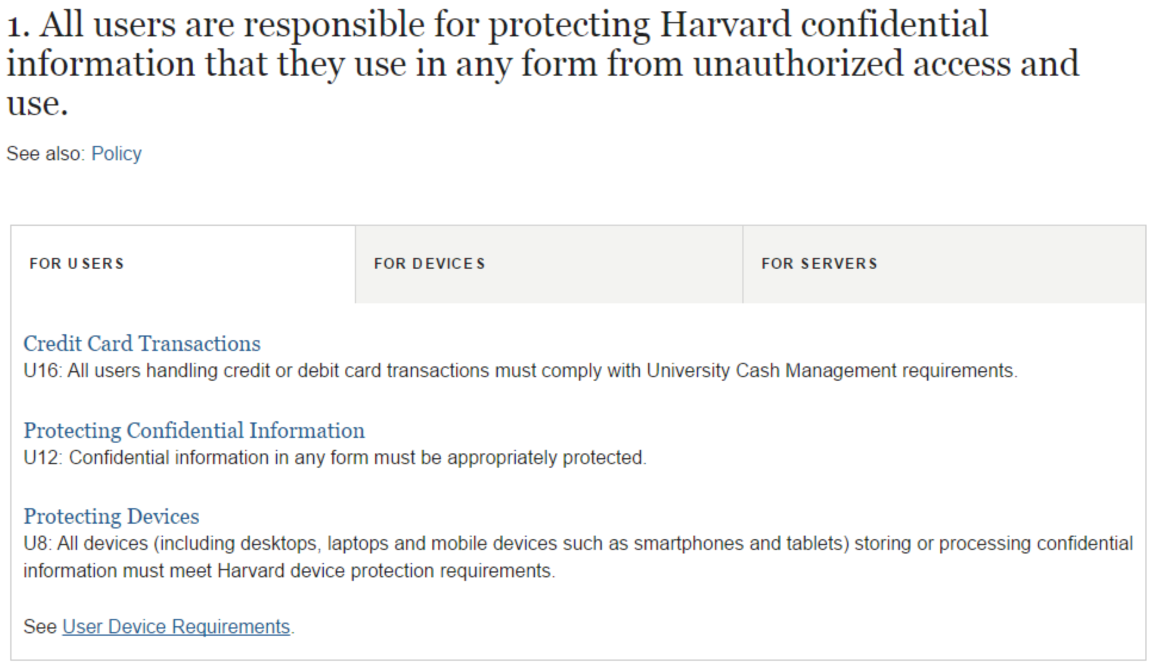
Large enterprises will have security policies but it is important to keep these policies up to date and adapt them with organisational changes. It is possible that because of the increasing use of SaaS application, some of the security policies will need an update.

Security policies addressing the risks that SaaS brings to an organization is necessary. The security team needs to develop a plan that defines secure use these services. It is important that new hires and employees are aware of the security policy and they should be encouraged to follow it.

4.4.1 Harvard University Information Security Policy example

Harvard University has a security policy available online available via the following link: http://policy.security.harvard.edu/

The following figure illustrates one policy statement for users.



1. All users are responsible for protecting Harvard confidential information that they use in any form from unauthorized access and use.

See also: Policy

Credit Card Transactions
U16: All users handling credit or debit card transactions must comply with University Cash Management requirements.

Protecting Confidential Information
U12: Confidential information in any form must be appropriately protected.

Protecting Devices
U8: All devices (including desktops, laptops and mobile devices such as smartphones and tablets) storing or processing confidential information must meet Harvard device protection requirements.

See User Device Requirements.

Figure 28 - Harvard Security Policy Statement

4.5 Data Classification

Data classification is a useful way to rank the value and importance of groups of data.
With the use of Cloud services, the importance of data classification is higher than before. It should be clear to employees which data can be shared with the Cloud. This is often not the case.

Data Loss Prevention (DLP) software often integrates data classification so that different policies can be applied to different levels of data classes.

Data classification can help with two problems regarding Cloud services: Access Control and sending confidential data to the Cloud.

Access Control

When company data is split up into classes it is easy to give the correct permissions to employees. For example: highly confidential data should only be accessible by C-level executives.

When access control does not work as it should, there is a risk that unauthorized people have access to confidential data. In a traditional IT network, only internal employees could access these files, but in the case of using a public Cloud service, this could mean that it is accessible by everyone on the internet.

Sending confidential data to the Cloud

Employees are not always aware that some data should not be shared with the Cloud. Data that needs to comply to certain laws or standards (HIPAA, FERPA, ...) cannot be shared with every

Cloud provider. Only if the Cloud provider complies with these laws or standards can data be stored on its services.

Data classification in combination with a control mechanism can make sure that confidential or sensitive data remains within the allowed environment.

Harvard Data Classification

Harvard University has a data classification table that describes five levels of Data classifications with examples.

Table 7 - Data Classification Harvard [48]

Level	Description	Example
5	Information that would cause severe harm to individuals or the University if disclosed.	Certain individually identifiable medical records and genetic information, categorized as extremely sensitive
4	Information that would likely cause serious harm to individuals or the University if disclosed	Passwords and Harvard PINs that can be used to access confidential information
3	Information that could cause risk of material harm to individuals or the University if disclosed.	Institutional financial records
2	Information the disclosure of which would not cause material harm, but which the University has chosen to keep confidential	Patent applications and work papers, drafts of research papers
1	Public Information	Course catalogs

4.6 Security Awareness Program

IT Security is only as strong as its weakest link.

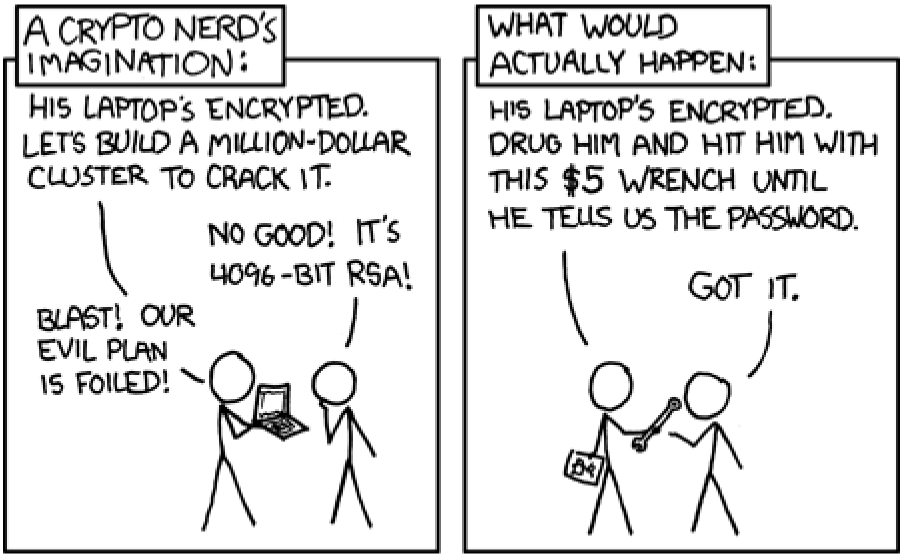

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Figure 29 - Security http://xkcd.com/538/

The figure above depicts in a humorous way that an adversary chooses the easiest path to gain access to a secured system. In reality, the adversaries do not need to torture the user with a wrench. A simple phishing attack against an unaware user does the trick.

Security experts consider people the weakest link in security. People can make mistakes or let their guard down. They may not have information security in mind when they do their jobs. Even with the most advanced technical countermeasures data breaches can still occur when an employee does something wrong.

Security Awareness, training, and education programs provide four major benefits to organizations [36]:

- Improving employee behaviour
- Increasing the ability to hold employees accountable for their actions
- Mitigating liability of the organization for an employee's behaviour
- Complying with regulations and contractual obligations

All employees in an enterprise need to have some level of security awareness, the learning objectives depend on the employee's role. NIST SP 800-16 [49] (Information Technology Security Training Requirements: A Role- and Performance-Based Model) gives guidance for security training. The NIST publication defines four layers of learning programs:

- **Security awareness** – For all employees

- **Security basics and literacy** – For all employees who are involved in any way with IT systems

- **Training** – For employees with roles and responsibilities relative to IT systems. This level of training recognizes beginner, intermediate and advanced skill requirements.

- **Education and experience** – For information technology security specialists and professionals. This level of learning program also recognizes beginner, intermediate and advanced skill requirements.

The following figure provides the model and overview of the information technology security learning continuum defined by NIST.

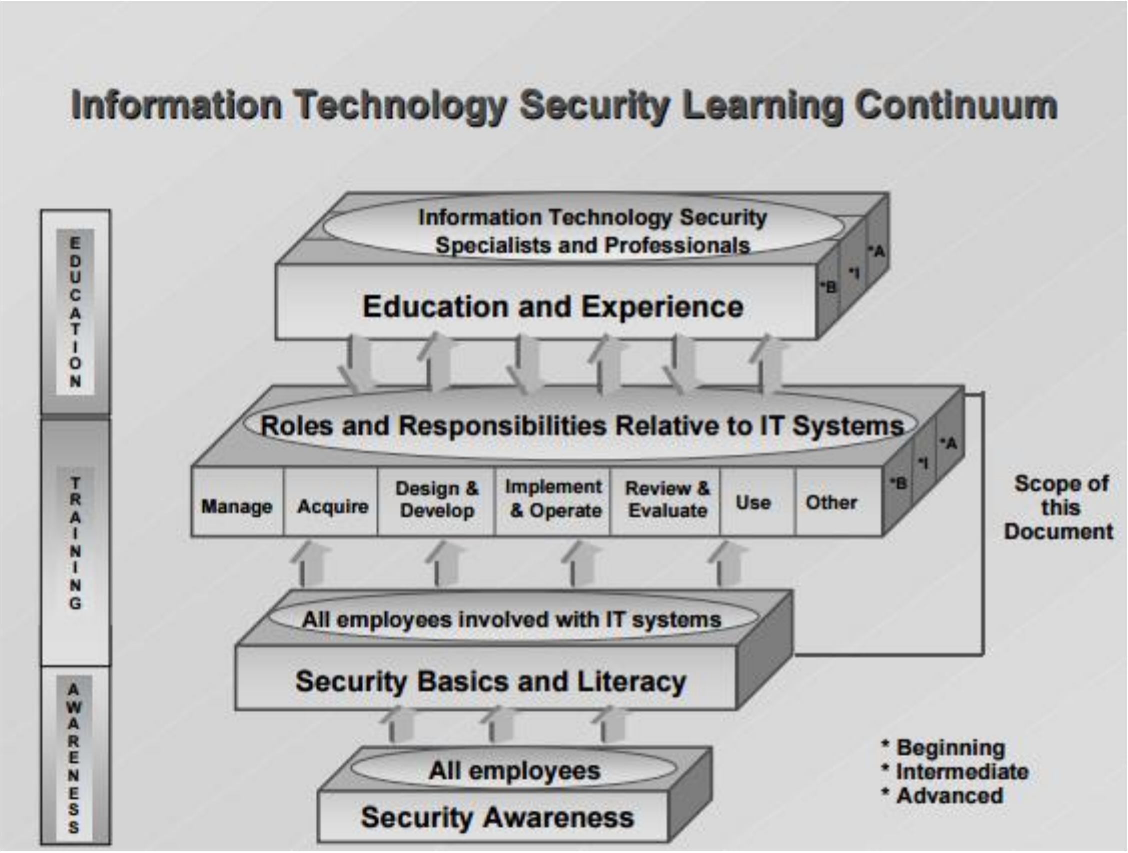

Information Technology Security Learning Continuum
EDUCATION
TRAINING
AWARENESS
Information Technology Security Specialists and Professionals
Education and Experience
*B
*I
*A
Roles and Responsibilities Relative to IT Systems
Manage
Acquire
Design & Develop
Implement & Operate
Review & Evaluate
Use
Other
*B
*I
*A
Scope of this Document
All employees involved with IT systems
Security Basics and Literacy
All employees
Security Awareness
* Beginning
* Intermediate
* Advanced

Figure 30 - IT Security Learning Continuum [49]

Security Awareness is something that has always been important and with the rise of Cloud services the importance is even higher. Employees are not aware of the risks that Cloud services pose, they just want to do their job as efficient as possible.

"IF SECURITY INTRODUCES BLOCKING TO THE ORG, IT WILL BE IGNORED, NOT EMBRACED. "
[50]

IT security is in many cases perceived as a blocking factor to do their job. When something is blocked, users will search for a workaround or a similar service.

Making users aware of IT security risks is not easy, and it is a continuous process.

4.6.1 Passwords

Many cloud services rely on passwords for authentication. It is important to have a good password to prevent adversaries from compromising your account. Most people do not like to remember hard passwords and tend to choose weak and frequently used passwords like “123456”, “password”, “Azerty123” …

Security awareness can encourage employees to choose passwords that are harder to guess / crack. In a case study conducted by Turkish students the number of weak passwords (cracked within 24 hours) was reduced from 98,8% to 63,6% in one-year time through security awareness. [51]

4.6.2 Security Culture at Facebook

The security culture at Facebook consists of five ingredients:

1. **Openness** – Everyone is responsible for security at Facebook. New hires have an orientation session with the security team. New engineers go through a six-week boot camp that includes several courses on security. Employees have direct access to security teams at any time.

2. **Company Mission** – Facebook’s mission is to make the world more open and connected. To do this effectively, they must do it securely.

3. **Community Collaboration** – Exchanging ideas, lessons, and best practices with other security teams helps to keep skills sharp and the company informed.

4. **Empathy** - Do not expect everyone to be a security expert, so look at your products from their perspective and plan for a variety of uses.

5. **Engagement** – Hacktober is a month-long program at Facebook with contests and workshops designed to engage employees on how to protect our company and all the people who use Facebook.

4.6.3 Security awareness at Riot Games

In the presentation “Levelling Up Security @ Riot Games” [52], Mark Hilllick explains how Riot Games handled the problem they had with Cloud services.

The situation at Riot was that the development team moved faster than the operational team. The development team had needs that the operational team could not provide fast enough. Because of this, the development team started using multiple virtual private Clouds from Amazon Web Services (AWS).

Another problem is that there were trust issues. Riot games develops a very popular game, League of Legends. Every now and then, a new game character is announced. The issue was that before the official announcement, employees with knowledge about the character would post it on Reddit to have their “moment of fame”.

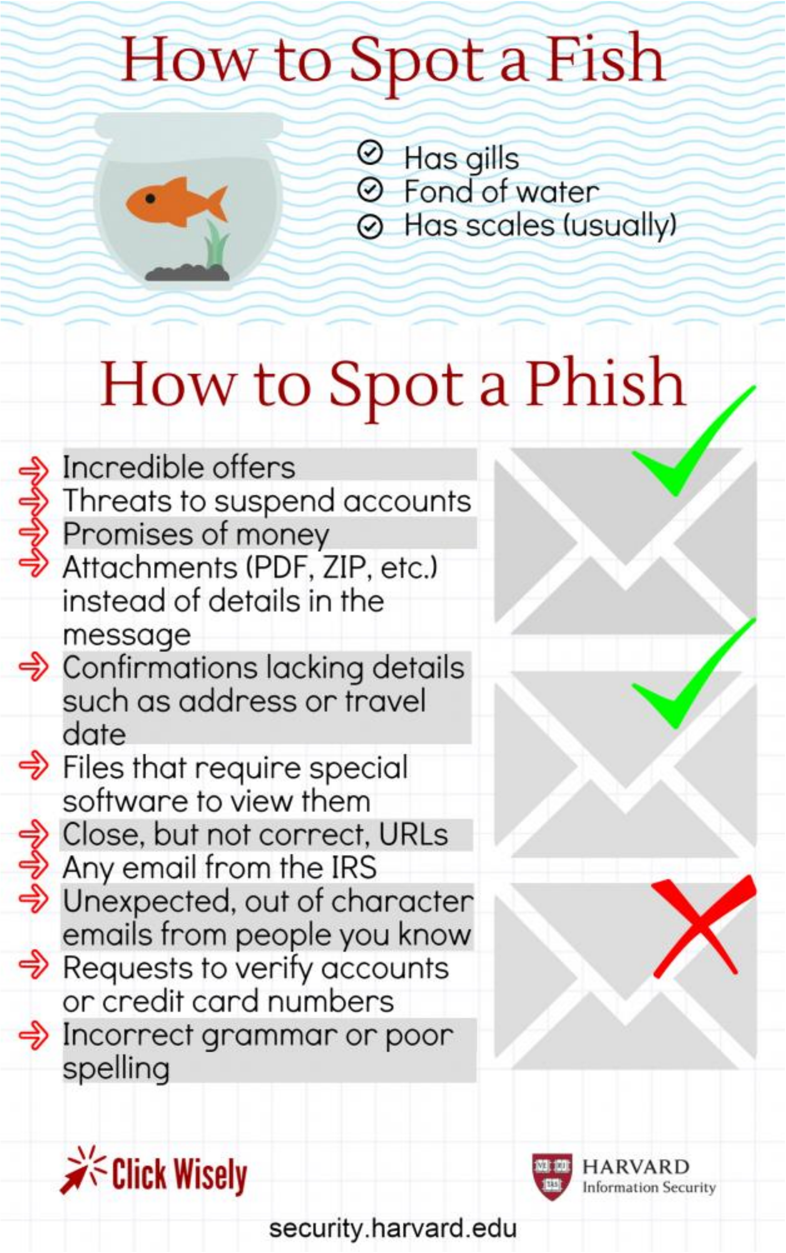
Mark Hillick and his team started several security awareness procedures to solve these problems.

For the developers they created small cards to place on their desk with “The definition of secure code”. It is a flashcard with very short rules on how to write secure code. This card reminds the developer to think about security.

Another initiative was the security week. Riot employees who helped with security were awarded with T-shirts. Because of these rewards, the motivation of the employees to actively help with security increased greatly.

4.6.4 Harvard University Security Awareness

The University of Harvard provides a website with information about IT security. Students and faculty members can consult this website for information about the security policies at Harvard and general security recommendations.



How to Spot a Fish

- Has gills
- Fond of water
- Has scales (usually)

How to Spot a Phish

- Incredible offers
- Threats to suspend accounts
- Promises of money
- Attachments (PDF, ZIP, etc.) instead of details in the message
- Confirmations lacking details such as address or travel date
- Files that require special software to view them
- Close, but not correct, URLs
- Any email from the IRS
- Unexpected, out of character emails from people you know
- Requests to verify accounts or credit card numbers
- Incorrect grammar or poor spelling

Click Wisely

HARVARD
Information Security

security.harvard.edu

Figure 31 - How to spot a Phish [53]

4.7 Security as a Service (SECaaS)

Security as a Service is a Cloud computing model that delivers managed security services over the internet. SecaaS is based on the Software as a Service (SaaS) model but limited to specialized information security services. [54]

SecaaS are provided for multiple areas: Identity and Access Management (IAM), Data Loss Prevention, Web Security, Security Assessment, Intrusion management …

In the following sections, several SecaaS solutions are described.

4.8 Cloud Access Security Broker (CASB)

Cloud Access Security Brokers are a new kind of security solution focused on Cloud services.

Gartner defines a CASB as follows:

- **Cloud access security brokers (CASBs)** are on-premises, or Cloud-based security policy enforcement points, placed between Cloud service consumers and Cloud service providers to combine and interject enterprise security policies as the Cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention and so on. [55]

CASBs provide a single point of control over multiple Cloud services concurrently, for any user or device. [56]

CASBs are delivered via a SaaS application or on premise via virtual or physical form factors.

They deliver a number of new features to the security landscape but also make use of existing methods adjusted to the Cloud. These existing methods come in the form of tokenization, encryption, data loss prevention (DLP) and analytics.

While the CASB market is still very young, Gartner predicts that this technology will become an essential component of SaaS deployments by 2017. [57]

A comparison for some of the different CASB vendors is included in Appendix D.

4.8.1 Deployment modes

- **Reverse proxy** – Users can reach the Cloud service via the proxy URL, for example: www.salesforce.com can be reached via the proxy as www-salesforce-com.proxy.net Bypassing the proxy for direct access should be disabled. This is the recommended way for proxying Cloud applications and is aimed at BYOD / unmanaged devices.

- **Forward proxy** – This method requires modifying the proxy settings on all devices and causes a substantial administrative burden. Native mobile applications with hard-coded hostnames may require a forward proxy. Managed devices are often configured this way.

- **API integration** – Some Cloud services offer API's which can be used for example to block external sharing.

4.8.2 Functionality CASB

Gartner [56] describes four pillars of functionality delivered by CASBs:

- **Visibility** – CASBs provide Shadow-IT discovery and sanctioned application control, as well as a consolidated view of an organization's Cloud service usage and the users who access data from any device or location.

- **Compliance** – CASBs assist with data residency and compliance with regulations and standards, as well as identify Cloud usage and the risks of specific Cloud services.

- **Data security** – CASBs provide the ability to enforce data-centric security policies to prevent unwanted activity based on data classification, discovery and user activity monitoring of access to sensitive data or privilege escalation. Policies are applied through controls, such as audit, alert, block, quarantine, delete and encrypt/tokenize, at the field and file level in Cloud services.

- **Threat protection** – CASBs prevent unwanted devices, users and versions of applications from accessing Cloud services. Other examples in this category are user and entity behaviour analytics (UEBA), the use of threat intelligence and malware identification.

4.8.3 Advantages CASB [58]

Skyhigh Networks defines the value of a CASB as follows:

- **Cost reduction**

    - Reduction in manual efforts required to analyse log data for Cloud visibility

    - Streamlined security assessments for Cloud services

    - Elimination of unapproved IaaS usage

    - Subscription consolidation

    - Elimination of orphaned subscriptions

  - Accelerated response to breaches and vulnerabilities

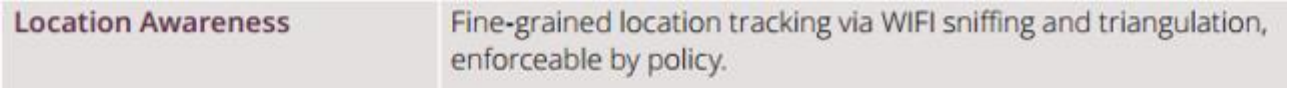
- **Risk mitigation**
  - Reduction in data lost due to the use of high-risk services
  - Reduction in data lost due to security breaches
  - Reduction in data lost due to insider threats
  - Reduction in risk of a compliance violation

4.8.4 Limitations of CASB

- Not all SaaS CSPs have API controls
- Limited offer of SaaS apps, focus on major ones: Salesforce, Dropbox, Box, Google Apps, Office 365
- Limited functionality after encryption. Specifically, encrypted data cannot be processed by the SaaS application servers. For example, if you encrypt a field with monetary values, the Cloud app is not able to report on sum totals of those dollar values appropriately
  - Encrypted data cannot be searched
    - Cyclic ciphers to make it searchable --> weak and easily cracked via chosen plaintext attacks
- Resiliency in the face of constantly changing Cloud applications - First-generation CASB products rely on hand-coded logic for such applications, and frequently break when the application is updated.
- As an emerging market, CASB capabilities vary from one vendor to the next

4.8.5 User privacy

An issue of using certain CASBs could be privacy. The following figure is a feature from the Bitglass for Dropbox solution.



Location Awareness	Fine-grained location tracking via WIFI sniffing and triangulation, enforceable by policy.

Figure 32 - Location awareness - Bitglass for Dropbox [59]

Tracking the location of employees may have legal consequences especially when the employee is unaware of it. Depending on the local laws, the employee should sign an employment contract that describes that the employer may keep track of the geolocation of the employee.

Considering that CASBs enable the employee to access business applications on their personal devices, the location tracking could have some legal implications.

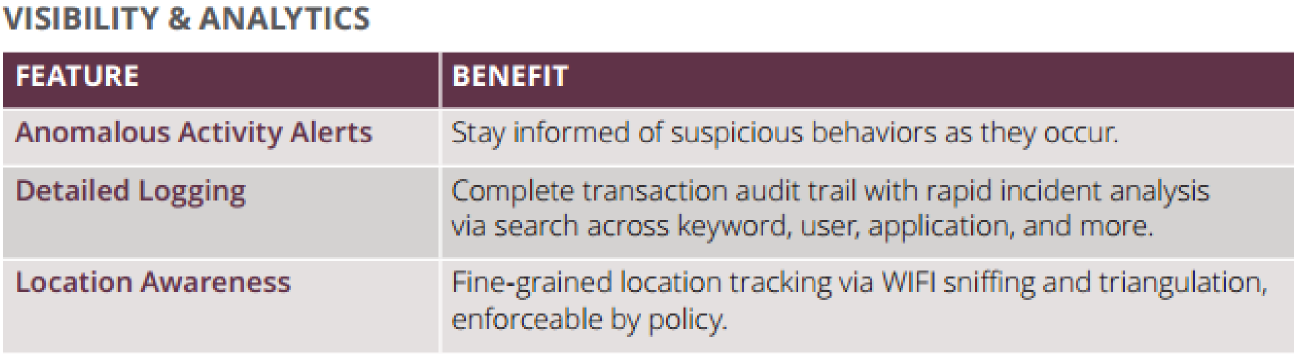
4.8.6 Example vendor: Skyhigh Networks [60]

Skyhigh networks claims to be the first company to offer a solution directly addressing the security, compliance, and governance challenges faced by enterprises moving to the Cloud. They have different features to cover the key functionality that Gartner describes.

- **Visibility**
  - **CloudTrust Ratings** assigns a risk rating for each service based on 50+ attributes.
  - **Cloud Usage analytics** visually summarizes the number of Cloud services in use and other statistics.
- **Compliance**
  - **Cloud Data Loss Prevention** enforces DLP policies on data sent to the Cloud.
  - **Pre-Built DLP Templates** to help identify content such as PII.
- **Data Security**
  - **Tokenization** substitutes sensitive data with randomly generated tokens to keep data on premises, satisfying data residency requirements.
  - **Rights management** enforces rights management policies for intellectual property through integration with DRM solutions.
- **Threat protection**
  - **User behaviour Analytics** automatically builds a self-learning model based on multiple heuristics and identifies anomalies indicative of insider threat data exfiltration.
  - **Darknet Intelligence** identifies stolen credentials leaked from breached Cloud services to reveal users and services at risk.

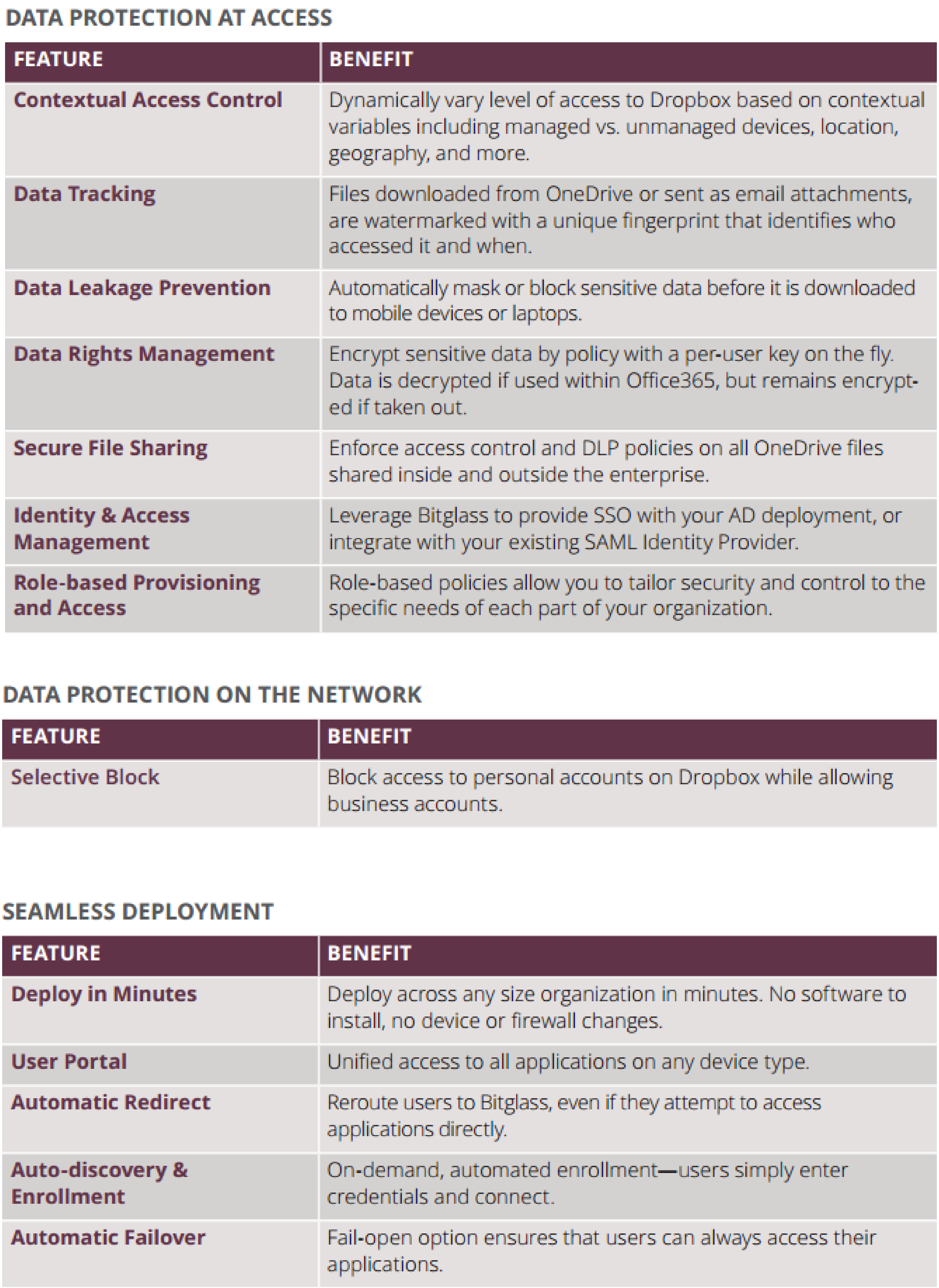
4.8.7 Example Solution: Bitglass for Dropbox

Bitglass offers these features for Dropbox:



VISIBILITY & ANALYTICS

FEATURE	BENEFIT
Anomalous Activity Alerts	Stay informed of suspicious behaviors as they occur.
Detailed Logging	Complete transaction audit trail with rapid incident analysis via search across keyword, user, application, and more.
Location Awareness	Fine-grained location tracking via WIFI sniffing and triangulation, enforceable by policy.



DATA PROTECTION AT ACCESS

FEATURE	BENEFIT
Contextual Access Control	Dynamically vary level of access to Dropbox based on contextual variables including managed vs. unmanaged devices, location, geography, and more.
Data Tracking	Files downloaded from OneDrive or sent as email attachments, are watermarked with a unique fingerprint that identifies who accessed it and when.
Data Leakage Prevention	Automatically mask or block sensitive data before it is downloaded to mobile devices or laptops.
Data Rights Management	Encrypt sensitive data by policy with a per-user key on the fly. Data is decrypted if used within Office365, but remains encrypted if taken out.
Secure File Sharing	Enforce access control and DLP policies on all OneDrive files shared inside and outside the enterprise.
Identity & Access Management	Leverage Bitglass to provide SSO with your AD deployment, or integrate with your existing SAML Identity Provider.
Role-based Provisioning and Access	Role-based policies allow you to tailor security and control to the specific needs of each part of your organization.

DATA PROTECTION ON THE NETWORK

FEATURE	BENEFIT
Selective Block	Block access to personal accounts on Dropbox while allowing business accounts.

SEAMLESS DEPLOYMENT

FEATURE	BENEFIT
Deploy in Minutes	Deploy across any size organization in minutes. No software to install, no device or firewall changes.
User Portal	Unified access to all applications on any device type.
Automatic Redirect	Reroute users to Bitglass, even if they attempt to access applications directly.
Auto-discovery & Enrollment	On-demand, automated enrollment—users simply enter credentials and connect.
Automatic Failover	Fail-open option ensures that users can always access their applications.

Figure 33 - Bitglass for Dropbox features [59]

4.8.8 List of CASB vendors

The following vendors provide similar CASB products. [56]

- Bitglass
- Blue Coat Systems (Perspecsys)
- CensorNet
- CipherCloud
- CloudLock
- Elastica
- FireLayers
- Imperva
- Microsoft (Adallom)
- Netskope
- Palerra
- Palo Alto Networks
- Skyhigh Networks
- Vaultive

4.9 Data Loss Prevention (DLP)

Data Loss Prevention is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. It gives the IT department control over what data end users can transfer.

Traditionally, data loss prevention was used to prevent accidental deletion of data, or users copying data to USB flash drives or hard drives. Nowadays DLP has evolved into a technique to prevent data loss or leakage through public Cloud services. Files that are uploaded to public Cloud services are analysed by DLP software to detect confidential information. Files with sensitive data are refused from uploading to the Cloud.

Two examples of Cloud features for DLP products are given in the next section but a full comparison of DLP software vendors is out of scope for this thesis.

McAfee Data Loss Prevention Endpoint [61]

- **Content-aware Cloud protection rule** blocks sensitive files from being synced to Cloud storages such as Box, Dropbox, Google Drive…
- **Application file access protection rule** blocks access to sensitive files such as Skype file transfer, Nero burning, and iTunes syncs

Symantec Data Loss Prevention for Cloud [62]

- **Cloud Storage DLP for Box** – content discovery to scan Box Business and Enterprise accounts.
- **Cloud Prevent for Office 365** – detect sensitive corporate information and take the right action at the right time by notifying users of policy violations. Use encryption gateway for secure delivery or block email to prevent loss of critical data.

4.10 Security Information & Event Management (SIEM)

Security Information & Event Management systems provide centralized logging capabilities for an enterprise and are used to analyse and correlate on the log entries it receives. SIEM products and services serve two purposes: providing centralized security logging and reporting for an organization, and aiding in the detection, analysis and mitigation of security incidents. [63]

CASBs provide capabilities similar to SIEM products. Spotting abnormal user behaviour through logs is a feature of SIEM products as well as CASB products.

4.11 User Behaviour Analytics (UBA)

User Behaviour Analytics is a feature that can be found in several security solutions. CASBs and SIEM systems provide detection of anomalous behaviour.

One of the most used methods to compromise and extend malicious control over an enterprise network is the use of compromised user credentials. With UBA, it is possible to detect behaviour that deviates from the normal user behaviour.

Examples of anomalous behaviour:

- **Downloading all corporate data** – if a user account starts downloading all corporate data, this may indicate that a hacker is trying to steal all confidential data through this user account.
- **Fast change of physical location** – if user account logs in at 8am in Belgium and at 9am in Australia, it may indicate that a hacker is login in to a compromised account.

UBA is a detecting mechanism and will in most cases only throw an alert when the breach has already occurred. Only when large amounts of data are being transferred to unknown devices can some software solutions take a preventive action.

4.12 Risk treatment for Use Cases

For both use cases **reduce consequence** can be achieved by not storing sensitive data on the Cloud service. If Foursquare would not store critical assets on Dropbox, several of the risks would be lower.

Another way to **reduce consequence** can be to **transfer risk** to an insurance company by taken an insurance against data breaches. An insurance however will not reduce the reputational damage.

When the cost of the countermeasure is too high, the organization can choose to **accept the risk.**

4.12.1 Risks Priority Harvard University

From the risks overview in Chapter 3, the risks for Harvard are moderate for the brute force and social engineering attacks on the admin credentials (T4, T5). Since the risk is only moderate, the University can choose to accept the risk.

4.12.2 Risks Priority Foursquare

Foursquare has several threats with a very high risk:

- T4 Brute force attack Admin Credentials
- T5 Social Engineering Admin account
- T11 Malicious Insider
- T13 Malware targeting Cloud

These should be treated most urgently.

The following threats have a high risk:

- T6 Brute force User credentials
- T7 Social Engineer User Account
- T8 Man in the Cloud attacks
- T9 Cloud side channel attacks

They have second priority for Foursquare.

4.12.3 Risk treatment

T1. **CSP Hardware Confiscation**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Very Low**	**Low**
Security Controls	• **Choice of CSP**	
Risk treatment	No action is required. This is something that should be considered when the enterprise is choosing a CSP.	This should be considered when the enterprise is choosing the CSP. **Risk Avoidance** could be achieved by a change of provider. The CSP Box for example focusses more on Cloud storage for businesses and might offer more assurance.

T2. **CSP Bankruptcy**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Very Low**	**Low**
Security Controls	• **Choice of CSP**	
Risk treatment	No action is required. This is something that should be considered when the enterprise is choosing a CSP.	

T3. **Natural Disaster**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Very Low**	**Low**
Security Controls	• **Choice of CSP** • **In house disaster recovery**	
Risk treatment	No risk treatment is needed.	No risk treatment is needed / possible except to lower the impact by storing less critical data on Dropbox.

■ **Brute force attack Admin Credentials**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Moderate**	**Very High**
Security Controls	• **Choice of CSP** • **Two factor authentication** • **Security policy: Password strength for admin accounts** • **Security Awareness: Passwords** • **CASB - User behaviour analytics (UBA)**	
Risk treatment	Since the CSP provides the security controls for logging in, the choice of the CSP has some effect on this risk. A CSP that allows infinite guesses on the login page may not be the best choice (see iCloud hack in the last chapter, section: data breach example) A way to **reduce the likelihood** is by enabling two-factor authentication for admin accounts. It disables the ability of the attacker guess the password. Another way to **reduce the likelihood** is by defining a security policy that enforces the use of strong passwords for admin accounts so that they becomes a lot harder to guess for the attacker. CASBs with UBA can detect excessive login attempts on the admin account, which can **reduce consequence** through early detection or **reduce likelihood** by taking preventive actions.	

⬛ **Social Engineer Admin Credentials**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Moderate**	**Very High**
Security Controls	• **Security policy: training and awareness for administrators** • **Security awareness: higher level education and experience**	
Risk treatment	Making users aware of phishing emails or bogus phone calls **reduces the likelihood** that the social engineering threat will succeed. Security awareness is especially important for employees with access to the management interface of the Cloud service. A security policy that enforces continual security training for administrators will keep the security awareness up to date.	

T6. **Brute force attack User credentials**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Low**	**High**
Security Controls	• **Choice of CSP** • **Two factor authentication** • **Security policy: Password strength for user accounts** • **Security Awareness: Passwords** • **CASB - User behaviour analytics (UBA)**	
Risk treatment	Since the CSP provides the security controls for logging in, the choice of the CSP has some effect on this risk. A CSP that allows infinite guesses on the login page may not be the best choice (see iCloud hack in the last chapter, section: data breach example) A way to **reduce the likelihood** is by enabling two-factor authentication for admin accounts. It disables the ability of the attacker guess the password. Another way to **reduce the likelihood** is by defining a security policy that enforces the use of strong passwords for user accounts so that they becomes a lot harder to guess for the attacker. Difficult passwords may be hard to remember for users so the security team should provide guidance on how to choose a good password. For example a user could choose a sentence to remember and then use the first letter of each word the make a easy to remember password, yet hard to guess for the attacker. CASBs with UBA can detect excessive login attempts on the admin account, which can **reduce consequence** through early detection or **reduce likelihood** by taking preventive actions.	

T7. **Social Engineer User Account**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Low**	**High**
Security Controls	• **Security awareness** • **CASB – DLP** • **DLP**	
Risk treatment	Making users aware of phishing emails or bogus phone calls **reduces the likelihood** that the social engineering threat will succeed. **Reducing likelihood** of a successful data breach can also be achieved by a DLP strategy.	

T8. **Man in the Cloud attack**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Low**	**High**
Security Controls	• **Security awareness** • **CASB - UBA**	
Risk treatment	One part of this attack depends on social engineering to execute the code to switch the synchronisation token. Raising security awareness **lowers the likelihood** that the social engineering attack succeeds. The code to switch the synchronisation token is stealthy and is not detected by anti-malware solutions. In some cases it is impossible to recover from an attack, and it may be required that the user account is deleted and a new one created. A CASB solution is able to detect anomalies in the way an account for file synchronization is used and accessed. Since the attack is detected, the **consequences can be reduced**.	

T9. **Cloud Side Channel attack**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Low**	**High**
Security Controls	• **Choice of CSP** • **Data encryption before uploading (CASB)**	
Risk treatment	Google is one of the most popular companies in SaaS with great security and a bug bounty program. All obvious and well-known security issues are fixed. There aren't a lot of CSP's that have the same level of security as Google so changing to another CSP is not really an option. The data that is stored on Google Apps is not high-confidential so encrypting before uploading will not be necessary.	The fact that data deduplication is used by Dropbox cannot be changed by the enterprise so the only way to avoid this is to encrypt the data before uploading or to change to another CSP. Example of **risk avoidance**: If the files are encrypted before uploading, the likelihood of a Cloud side channel attack through data deduplication is reduced to zero. But this has consequences for the usability of the service. Online collaboration with team members on Dropbox will not work anymore since the files are encrypted.

T10. **Company data owned by CSP**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Very Low**	**Low**
Security Controls	• **Choice of CSP**	
Risk treatment	No risk treatment is needed in both use cases. Google and Dropbox do not claim ownership over data uploaded to their services.	

T11. **Malicious insider**		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Low**	**Very High**
Security Controls	• **Security Policy** • **CASB - UBA** • **DLP** • **CASB - Access Control**	
Risk treatment	No high-confidential data is stored on the service. A student or faculty member could only disclose his or her own files. The administrator of the Google Apps service for the University could do malicious actions. This is a risk an organization always has and depends on trust.	An employee that is fired could take revenge by downloading all critical assets from Dropbox and send them to a competitor or publish them online. The security policy should define how to handle data access when an employee is fired. This policy is enforced with Access Control. A CASB could help with detecting anomalous behaviour. An employee that wants to download all critical assets is probably up to no good. DLP solutions prevent confidential data to be shared on the public Cloud. CASB with access control can limit the access of a certain user, this can be used to **reduce the consequence.**

[redacted] Foreign government espionage		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Very Low**	**Low**
Security Controls	- **Choice of CSP**	
Risk treatment	No risk treatment is necessary.	

[redacted] Malware targeting Cloud		
	Google Apps for Harvard	Dropbox for Foursquare
Risk	**Low**	**Very High**
Security Controls	- **Security awareness** - **CASB – malware detection**	
Risk treatment	A general sense of secure online behaviour can prevent users to get their computers infected by malware. A CASB can help by detecting anomalous behaviour from Cloud service accounts.	

4.12.4 Conclusion Harvard University

Harvard University does not have any serious risks related to the use of Google Apps in terms of data loss or data breach. Extra precautions do not seem necessary.

4.12.5 Conclusion Foursquare

Foursquare has some serious risks because it stores critical assets on Dropbox. A combination of security management and technical solutions will lower the risks. To lower the highest risk the following solutions should be considered:

- Two factor authentication
- Security policies
- Security Awareness
- Standalone or in Cloud Access Security Broker
  - DLP
  - UBA
  - Access Control
  - Malware detection

Cloud Access Security Brokers are an option to be considered, since they provide protection for the most urgent risks. Foursquare will have to make a study on what solution fits their needs best.

4.13 Shadow-IT

As a company you have the choice of blocking Shadow-IT that can be detected or allow it and try to make it work for the organization in a secure manner. In recent years, trying to block Shadow-IT has become a lot more difficult as more Cloud services are being used by employees, according to discovery assessments by PwC and Skyhigh networks across Europe, the average number of Cloud services per organization is 987. [32]

With traditional firewalls, blocking the countless amount of Cloud services is not feasible. This is where Unified Threat Management (UTM) can help. UTM is also referred to as the next generation firewall. UTM is capable of whitelisting specific applications or services for each user or group separately. Depending on the vendor, UTMs have different capabilities.

The decision of how an enterprise handles Shadow-IT will depend a lot on the nature and business of the enterprise. Financial institutes with highly confidential data might not be able to allow public Cloud services for their employees.

Options to handle with Shadow-IT without blocking it

- Make complying with enterprise solutions easier and simpler than not complying.
- Security Awareness: IT-policy training that guides employees to a detailed understanding of Cloud risks and policies.
- Security Policy: An acceptable use policy that describes in detail what the company is allowed to do if an employee who uses a personal device leaves the company. This policy should include language that not only allows the company to examine the device before the employee leaves the company, but it also should have language that requires the employee to check any other computing or storage device they own, or any Cloud service they use personally, to ensure that all corporate data is wiped from those systems. [64]
- Cloud access security brokers
    - Gain visibility over Cloud services
    - Assess the risk to each Cloud service
    - Enable the right applications
- DLP software (standalone or incorporated in CASB)
- Buy Enterprise licenses for Cloud services that offer more centralized controls, such as authentication, policy enforcement, and activity monitoring and reporting.

4.14 Conclusion and Future work

CASBs are still young, they promise to cover many of the new security issues with public SaaS. A comparative study between different providers could help in gaining more insight into the different capabilities they offer. The study should check if the promises the CASB providers make really are to be believed.

Also a lot of focus on management and awareness. Enterprises should have budget for a dedicated security team. Not different from security before the mainstream use of Cloud but the importance for it has risen.

Help from external partners with experience and expertise to make risk assessment specific for the enterprise's needs. The value of qualitative risk assessments depends on the experience and knowledge of the risk assessor. Subjective judgement will influence the results of the risk assessment.

5 *How to handle a breach of enterprise data?*

There is no such thing as 100% secure. Even with the most advanced security solutions, a company is still vulnerable to data breaches. Knowing how to handle a breach is essential for business continuity.

5.1 Incident Response (IR) Plan

The primary objective of an IR plan is to manage a cybersecurity event or incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs. [65]

SANS defines six steps to handle an incident:

1. **Preparation** – Prepare a team to handle incidents. Incident can range from power outage to disgruntled employees to state sponsored hackers. Security policies should define procedures for incident handling. A response plan/strategy should be in place to prioritize incidents based on organizational impact. Additionally a communication plan can help with contacting the necessary individuals during an incident.

2. **Identification** – The response team need to identify if the incident is actually a security incident and not a false-positive. The team may contact a local Cyber Emergency Readiness Team (CERT) to get information about the most recent viruses, worms, attacks …

3. **Containment** – Making sure the detected incident doesn't become worse. In case of a computer virus that spreads through the network, disconnecting the infected machines is an example of containment.

4. **Eradication** – Removing the root cause of the incident.

5. **Recovery** – Brining the affected systems back into the production environment.

6. **Lessons Learned** – Analysing the incident and making conclusions on how to make better future response and preventing recurrence.

5.2 Reporting requirement Belgium

Originally, there was no requirement for reporting data breaches for organizations outside of the telecom sector. For organizations in the telecom sector, the notification of the privacy commission should be within 24 hours after the detection of the breach. In addition, within 72 hours a more extensive report should be made available for the privacy commission.

From 1 January 2016, a new reporting requirement will become active for the EU. Organizations that suffer a data breach of personal data will need to notify the "Commissie van de Bescherming van de Persoonlijke Levenssfeer (CBPL)" and in most cases also owners of the involved data.

The reporting requirement act is still a work in progress in Belgium.

If the organizations in the Netherlands fail to comply to the reporting requirement there are fines up to €810.000 or 10% of their yearly revenue.

5.3 Computer Emergency Readiness Team (CERT)

CERTs are specialized teams of ICT professionals that handle security incidents. Many countries provide national CERT teams to respond to the evolving threat landscape on the internet.

CERT.be is the local CERT for Belgium and describes its roles as follows:

1. Gather and share information about security incidents
2. Give support during security incidents
3. Coordinate large scale security responses
4. Give support for CERT initiatives within companies
5. Share data and knowledge via publications and events

The advantages that CERT.be provides are neutrality, discretion, international network, expertise in cyber incidents and free of charge.

5.4 Federal Computer Crime Unit (FCCU)

In case of a data breach caused by criminals, the FCCU must be notified. The FCCU is the specialized unit in charge of fighting cybercrime in Belgium.

There are also Regional computer crime units (RCCU) that deal with local forensic research.

5.5 White hat hackers

Not all data breaches are a disaster for an enterprise. White hat hackers are IT professionals that hack with the intention to make the security of information systems better.

Several large service providers have a bug bounty program that allows hackers to report security issues to the company. In most bug bounty programs, the hacker is rewarded with money, gadgets or a message of appreciation. An example of a bug bounty program is hackerone.com, this platform is created by Facebook, Microsoft and Google.

In the Netherlands the National Cyber Security Centre offers a guide for responsible disclosure. This helps ICT professionals report vulnerabilities to companies.

In the presentation "Crowdsourced Security" [67], Inti De Ceukelaire describes the advantages for crowdsourced security as follows:

- Price
- Any time, any revision
- Lots of people
- Other perspectives

Disadvantages for crowdsourced security:

- Low quality reports
- Automated scanners
- Junk
- Takes time and effort

For large enterprises or governments, it might be worth considering how ethical hacking can be used as an advantage.

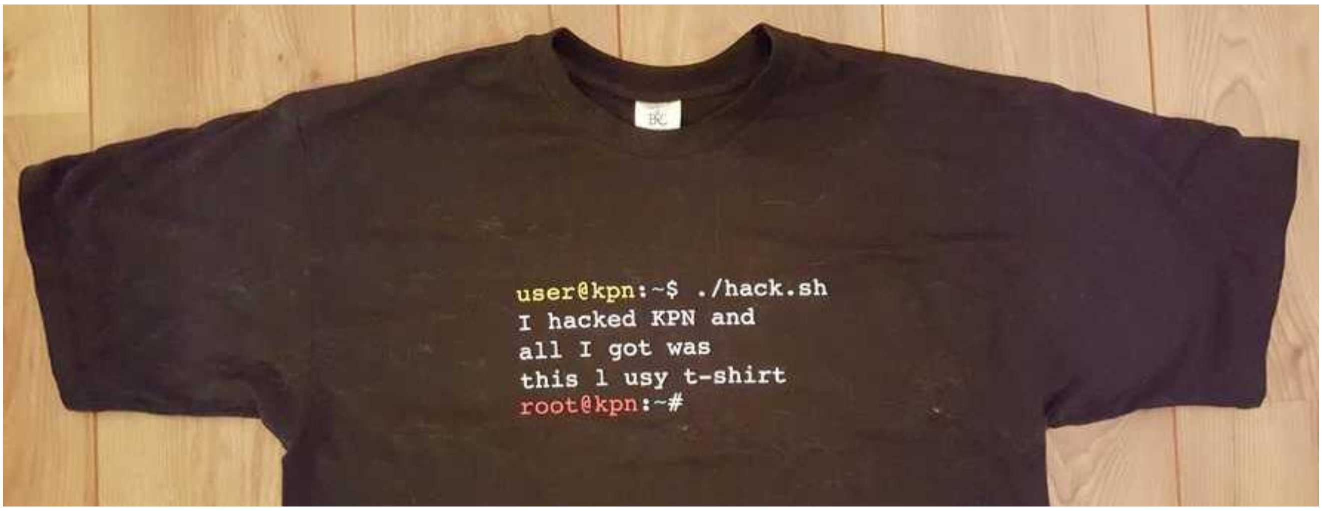
5.5.1 Phone house example ethical hacking

In October 2015, Sijmen Ruwhof discovered several security issues with a Phone House Store-in-Store concept. The Phone House booth was located in a Media Markt and customers could watch the computer screens. The main issue was that the Phone House used a Google Docs file to save all passwords in plaintext. Sijmen took pictures of this document and with these passwords, he could gain access to view and modify customer data of KPN, Vodafone, Telfort, T-Mobile, UPC, Tele2 and other companies.

Several other security issues can be read on Sijmen's blogpost.

Since this is a serious issue, Sijmen contacted the Phone House and Media Markt to make them aware of the issues. The first response from Media Markt was very hostile, the store manager threatened to sue Sijmen if he went public. Sijmen responded with an explanation about responsible disclosure and their attitude changed, they invited Sijmen for a cup of coffee.

Sijmen also notified the other stakeholders for Phone House. KPN's CERT team worked together with Sijmen and he received a T-shirt to thank him.



```
user@kpn:~$ ./hack.sh
I hacked KPN and
all I got was
this l usy t-shirt
root@kpn:~#
```

Figure 34 - KPN bounty

The full story can be found here: http://bit.ly/1ICJake [68]

5.6 Insurances

Insurance companies offer insurances to transfer some of the financial risk of a data breach to the insurer.

Cybersecurity insurances cover financial loss but do not prevent reputational damage. If the organization has repeated data breaches, its credibility will decrease. Reputational damage can lead to financial losses. Take TalkTalk for instance, following its data breach its stock price fell by 10 percent. [69]

The cybersecurity insurance market is more mature in the U.S. than in the E.U, primarily because of U.S. states' mandatory data-breach-notification laws. [70]

With the upcoming reporting requirement in the European Union, a rise in cybersecurity insurances might be possible. A recent PwC report forecasts that the global cyber insurance market will reach $7.5 billion in annual sales by 2020, up from $2.5 billion this year. [71]

In the Global State of information security study 2015, PwC states that more than half (51%) of respondents say they have purchased cybersecurity insurance. [72]

5.7 Data breach example: Apple – iCloud

In 2014, the result of a mass theft of nude celebrity photos was released on the internet. These pictures were retrieved from the iCloud accounts belonging to certain celebrities.

The hackers gained access to these accounts via a brute force attack on the login form and password recovery page. Although this attack did not compromise Apple's internal infrastructure, Apple could have prevented it by limiting the possible false login attempts on iCloud accounts.

It was not the first time this kind of flaw is discovered on Apple services. The Find my iPhone service also allowed attackers to try multiple password attempts without being locked out.

5.8 Additional information

- Chapter 16 of ISO 27017:2015: Information security incident management
  Released on 15 December 2015

6 References

[1] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” 2011.

[2] S. Srinivasan, Cloud Computing Basics, Houston: Springer, 2014.

[3] R. Heroux, “6 tips for satisfying security concerns on public cloud,” Scalar, 7 10 2014. [Online]. Available: https://www.scalar.ca/en/2014/10/6-tips-for-satisfying-security-concerns-on-public-cloud/. [Accessed 1 12 2015].

[4] N. Phaphoom, X. Wang, S. Samuel, S. Helmer and P. Abrahamsson, “A survey study on major technical barriers affecting the decision to adopt cloud services,” *The Journal of Systems and Software,* pp. 167-181, 2015.

[5] NIST, “NIST Cloud Computing Standards Roadmap,” NIST, 2013.

[6] D. Shackleford, “Orchestrating Security in the Cloud,” 22 September 2015. [Online]. Available: https://www.cloudpassage.com/assets/img/resources/sans-survey-orchestrating-security-in-the-cloud.pdf.

[7] RightScale, “State of the cloud report,” 2015.

[8] L. E. Nelson, “The State of Cloud Platform Standards: Q2 2015,” Forrester, Cambridge, 2015.

[9] Forrester, “Business Technographics Global Infrastructure Survey,” September 2014. [Online]. Available: https://www.forrester.com/Business+Technographics+Global+Infrastructure+Survey+2014/-/E-SUS2713.

[10] R. Fichera, G. O'Donnell and M. Caputo, “Vendor Landscape: Converged Infrastructure-Based Private Cloud Solutions,” Forrester, 2015.

[11] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” Cloud Security Alliance, 2009.

[12] European Commission, “Unleashing the potential of Cloud Computing in Europe,” European Union, Brussels, 2012.

[13] R. Johnson, Security Policies and Implementation Issues, Burlington: Jones & Bartlett Learning, 2015.

[14] N. Bhensook and T. Senivongse, “An Assessment of Security Requirements Compliance of Cloud Providers,” *IEEE 4th International Conference on Cloud Computing Technology and Science,* pp. 520-525, 2012.

[15] EuroCloud, “ECSA - Self Assessment,” [Online]. Available: https://eurocloud-staraudit.eu/quality.html. [Accessed 11 1 2016].

[16] Eurocloud, “ECSA,” [Online]. Available: https://eurocloud-staraudit.eu/. [Accessed 11 1 2016].

[17] Cloud Industry Forum, “Code of Practice for Cloud Service Providers,” 9 11 2015. [Online]. Available: http://cloudindustryforum.org/code-of-practice/cop.

[18] NIST, “Inventory of Standards Relevant to Cloud Computing,” NIST, [Online]. Available: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/StandardsInventory. [Accessed 15 12 2015].

[19] NIST, “Federal Information Security Management Act (FISMA) Implementation Project,” 5 November 2015. [Online]. Available: http://www.nist.gov/itl/csd/soi/fisma.cfm.

[20] S. Nepal and M. Pathan, Security, Privacy and Trust in Cloud Systems, Springer, 2014.

[21] IsecT, “ISO/IEC 27017,” 6 11 2015. [Online]. Available: http://www.iso27001security.com/html/27017.html.

[22] ISO, “Microsoft gives users confidence to move to the cloud,” 6 11 2015. [Online]. Available: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref1983.

[23] Cloud Security Alliance, “About,” 6 11 2015. [Online]. Available: https://cloudsecurityalliance.org/about/.

[24] Cloud Security Alliance, “CSA STAR,” 19 10 2015. [Online]. Available: https://cloudsecurityalliance.org/star/.

[25] Cloud Security Alliance, “Certificate of Cloud Security Knowledge,” 6 11 2015. [Online]. Available: https://cloudsecurityalliance.org/education/ccsk/#_about.

[26] Cloud Security Alliance, “CloudAudit Working Group,” 9 11 2015. [Online]. Available: https://cloudsecurityalliance.org/group/cloudaudit//#_overview.

[27] A. Pannetrat, “CTP Data Model and API, rev. 2.13,” Cloud Security Alliance, 2015.

[28] ISO, “ISO 31000 - Risk Management,” 12 11 2015. [Online]. Available: http://www.iso.org/iso/home/standards/iso31000.htm.

[29] FedRAMP, “fedramp.gov,” 9 11 2015. [Online]. Available: https://www.fedramp.gov/about-us/about/.

[30] M. Silic and A. Back, “Shadow-IT - A view from behind the curtain,” *Elsevier,* pp. 274 - 283, 2014.

[31] Cloud Security Alliance, “Cloud Adoption Practices & Priorities Survey Report,” Cloud Security Alliance, 2015.

[32] PriceWaterhouseCoopers, “Managing the Shadow Cloud,” PriceWaterhouseCoopers, 2015.

[33] ISACA, Controls and Assurance in the Cloud: Using COBIT5, Rolling Meadows, IL: ISACA, 2014.

[34] NIST, “Special Publication 800-30 Guide for Conducting Risk Assessments,” NIST, Gaithersburg, 2013.

[35] J. Maniscalchi, “Threat vs Vulnerability vs Risk,” 30 November 2015. [Online]. Available: http://www.digitalthreat.net/2009/06/threat-vs-vulnerability-vs-risk/#.

[36] W. Stallings and L. Brown, Computer Security, London: Pearson Educated Limited 2012, 2012.

[37] J. Lim, “Dropbox: Focus On Future Value, Not The Current Valuation,” 23 November 2015. [Online]. Available: http://www.forbes.com/sites/jlim/2015/11/12/dropbox-focus-on-future-value-not-the-current-valuation/.

[38] R. Seth, “Disaster Recovery by Google,” 24 November 2015. [Online]. Available: http://googleforwork.blogspot.be/2010/03/disaster-recovery-by-google.html.

[39] Crypto Fails, “Crypto Noobs #2: Side Channel Attacks,” 24 November 2015. [Online]. Available: http://www.cryptofails.com/post/70097430253/crypto-noobs-2-side-channel-attacks.

[40] D. Harnik, B. Pinkas and A. Shulman-Peleg, “Side Channels in Cloud Services: Deduplication in Cloud Storage,” *IEEE Security & Privacy,* pp. 40-47, 2010.

[41] IC off the Record, “PRISM SLIDES,” 26 November 2015. [Online]. Available: https://nsa.gov1.info/dni/prism.html.

[42] A. Philip, “Dissecting Big Tech's Denial of Involvement in NSA's PRISM Spying Program,” 26 November 2015. [Online]. Available: http://abcnews.go.com/Technology/nsa-prism-dissecting-technology-companies-adamant-denial-involvement/story?id=19350095.

[43] M. Higashi, “Turn 25,” CipherCloud, 25 6 2015. [Online]. Available: Shadow-IT is by now in such rampant use that the very employees tasked with keeping enterprises safe from Shadow-IT are themselves adopting Shadow-IT.. [Accessed 1 12 2015].

[44] CipherCloud, “CIO's guide to enterprise cloud adoption,” San Jose.

[45] Google, “Privacy,” [Online]. Available: https://support.google.com/work/answer/6056650?hl=en. [Accessed 4 12 2015].

[46] V. Winkler, “Cloud Computing: Data Privacy in the Cloud,” Microsoft, August 2012. [Online]. Available: https://technet.microsoft.com/en-us/magazine/jj554305.aspx. [Accessed 4 12 2015].

[47] CSA, “STAR Registrant Dropbox, Inc,” 16 March 2015. [Online]. Available: https://cloudsecurityalliance.org/star-registrant/dropbox-inc/. [Accessed 4 12 2015].

[48] Harvard University, “Data Classification Table,” [Online]. Available: http://security.harvard.edu/dct. [Accessed 07 12 2015].

[49] NIST, “Special Publication 800-16 Information technology security training requirements: A role- and performance-based model,” NIST, Gaithersburg, 1998.

[50] R. Smith, “Crafting An Effective Security Organization,” in *QCon NYC 2015*, NYC, 2015.

[51] M. Eminagaoglu, E. Uçar and S. Eren, “The positive outcomes of information security awareness training in companies - A case study,” *Elsevier - Information security technical report,* no. 14, pp. 223 - 229, 2009.

[52] M. Hillick, “Leveling Up Security @ Riot Games,” in *Brucon 0x07*, Ghent, 2015.

[53] Harvard University, “Click Wisely,” [Online]. Available: http://security.harvard.edu/click-wisely#widget-3. [Accessed 7 12 2015].

[54] Techopedia, “Security as a Service (Secaas or SaaS),” [Online]. Available: https://www.techopedia.com/definition/26746/security-as-a-service-secaas-saas. [Accessed 7 12 2015].

[55] Gartner, “Cloud Access Security Brokers (CASBs),” Gartner, [Online]. Available: http://www.gartner.com/it-glossary/cloud-access-security-brokers-casbs. [Accessed 1 12 2015].

[56] C. Lawson, N. MacDonald and B. Lowans, “Market Guide for Cloud Access Security Brokers,” Gartner, 2015.

[57] N. MacDonald and P. Firstbrook, “The Growing Importance of Cloud Access Security Brokers,” Gartner, 2013.

[58] Skyhigh Networks, “The definitive guide to cloud security”.

[59] Bitglass, “Bitlass for Dropbox: Solution Brief,” Bitglass, 2014.

[60] Skyhigh, “Cloud Access Security Broker,” [Online]. Available: https://www.skyhighnetworks.com/cloud-access-security-broker/. [Accessed 4 12 2015].

[61] McAfee, “McAfee Data Loss Prevention Endpoint,” McAfee.

[62] Symantec, “Data Sheet: Symantec Data Loss Prevention for Cloud,” Symantec Corporation, 2015.

[63] K. Scarfone, “Introduction to SIEM services and products,” July 2015. [Online]. Available: http://searchsecurity.techtarget.com/feature/Introduction-to-SIEM-services-and-products. [Accessed 10 12 2015].

[64] S. Lawton, “Shadow-IT: How to Detect and Mitigate Cloud Security Risks,” 7 7 2015. [Online]. Available: http://www.tomsitpro.com/articles/preventing-shadow-it,2-932.html. [Accessed 10 12 2015].

[65] T. Bailey, J. Brandley and J. Kaplan, “How good is your cyberincident-response plan?,” McKinsey&Company, December 2013. [Online]. Available: http://www.mckinsey.com/insights/business_technology/how_good_is_your_cyberincident_response_plan. [Accessed 11 12 2015].

[66] M. Justaert, “Regering zoekt wettelijk kader voor 'ethisch hacken',” Standaard, 8 1 2016. [Online]. Available: http://m.standaard.be/cnt/dmf20160107_02055359. [Accessed 11 1 2016].

[67] I. D. Ceukelaire, “Crowdsourced security: Get hacked before you get hacked,” in *Belgian Internet Security Conference*, Brussels, 2015.

[68] S. Ruwhof, “Epic failure of Phone House & Dutch telecom providers to protect personal data: How I could access 12+ million records #phonehousegate,” 8 12 2015. [Online]. Available: http://sijmen.ruwhof.net/weblog/608-personal-data-of-dutch-telecom-providers-extremely-poorly-protected-how-i-could-access-12-million-records. [Accessed 14 12 2015].

[69] N. Hawthorn, “Compared to data breach costs, an ICO fine is simply a dropb in the ocean,” ITProPortal, 10 12 2015. [Online]. Available: http://www.itproportal.com/2015/12/10/compared-to-data-breach-costs-an-ico-fine-is-simply-a-drop-in-the-ocean/. [Accessed 14 12 2015].

[70] L. Constantin, “5 Things you need to know about cybersecurity insurance,” 25 4 2014. [Online]. Available: http://www.cio.com/article/2376802/security0/5-things-you-need-to-know-about-cybersecurity-insurance.html. [Accessed 14 12 2015].

[71] D. Gollom, “Cyber insurance market set to reach $7.5 billion by 2020 - PwC report,” PwC, 15 9 2015. [Online]. Available: http://www.pwc.com/ca/en/media/release/2015-09-15-cyber-insurance-market-reach-7-5-billion-2020.html. [Accessed 15 12 2015].

[72] PwC, “Key findings from The Global State of Information Security Survey 2015,” 2014.

[73] Cloud Security Alliance, “The Notorious Nine: Cloud Computing Top Threats in 2013,” February 2013. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[74] Aerohive, “Public or Private Cloud,” 2013. [Online]. Available: http://www.aerohive.com/pdfs/Aerohive-Whitepaper-Public-or-Private-Cloud.pdf.

[75] CDWG, “Private Cloud and Software as a Service,” 2012. [Online]. Available: CDWG.com.

[76] L. Cheng, R. Ithal, K. Narayanaswamy and S. Malmskog, Cloud Security for dummies, New Jersey: John Wiley & Sons, 2015.

[77] M. Rouse, “data loss prevention (DLP),” October 2014. [Online]. Available: http://whatis.techtarget.com/definition/data-loss-prevention-DLP.

[78] “SAS 70 FAQ,” [Online]. Available: http://sas70.com/sas70_faqs.html.

[79] A. Cser and R. Holland, “The Emergence Of The Cloud Security Gateway,” Forrester, 2015.

[80] F. Liu, “Market Overview: Public Cloud Services In China In 2015,” Forrester, 2015.

[81] T. Vissers, T. V. Goethem, W. Joosen and N. Nikiforakis, “Maneuvering Around Clouds: Bypassing Cloud-based Security Providers,” ACM, Denver, 2015.

[82] J. Vijayan, “From 55 Cents to $1,200: The Value Chain For Stolen Data,” 16 10 2015. [Online]. Available: http://www.darkreading.com/risk/from-55-cents-to-$1200-the-value-chain-for-stolen-data/d/d-id/1322692?.

[83] C. McFarland, F. Paget and R. Samani, “The Hidden Data Economy,” Intel Security, Santa Clara, 2015.

[84] ISO, “About ISO,” [Online]. Available: http://www.iso.org/iso/home/about.htm.

[85] F. Sabahi, “Cloud Computing Security Threats and Responses,” IEEE, 2011.

[86] R. Choubey, R. Dubey and J. Bhattacharjee, “A survey on Cloud Computing Security, Challenges and Threats,” *International Journal on Computer Science and Engineering (IJCSE),* pp. 1227-1231, 2011.

[87] F. B. Shaikh and S. Haider, “Security Threats in Cloud Computing,” in *6th International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, 2011.

[88] W. A. Jansen, “Cloud Hooks: Security and Privacy Issues in Cloud Computing,” in *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011.

[89] J. Sen, “Security and Privacy Issues in Cloud Computing,” Tata Consultancy Services, Kolkata.

[90] The Blackstone Group , “Cyber Secure: A Look at Employee Cybersecurity Habits in the Workplace,” CompTIA, 2015.

[91] CPNI, “Information Security Briefing: Cloud Computing,” CPNI, 2010.

[92] T. Lambo, "Why you need a Cloud Rating Score," 2012.

[93] ISACA, Security Considerations for Cloud Computing, Rolling Meadows, IL: ISACA, 2012.

[94] LEET Security, "Rating Levels," 4 November 2015. [Online]. Available: http://www.leetsecurity.com/niveles-calificacion/.

[95] AICPA, "Service Organization Controls (SOC) Reports for Service Organizations," 4 November 2015. [Online]. Available: http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganization%27sManagement.aspx.

[96] D. Deutsch, "Cloud Computing Standardization in ISO/IEC JTC 1 SC 38," in *NIST Cloud Computing Forum and Workshop VIII*, 2015.

[97] IsecT, "ISO/IEC 27018," 6 11 2015. [Online]. Available: http://www.iso27001security.com/html/27017.html.

[98] ENISA, "Cloud Computing Certification - CCSL and CCSM," 9 11 2015. [Online]. Available: https://resilience.enisa.europa.eu/cloud-computing-certification.

[99] Cloud Security Alliance, "The Notorious Nine - Cloud Computin Top Threats in 2013," Cloud Security Alliance, 2013.

[100] M. Silic and A. Back, "Shadow-IT - A view from behind the curtain," *Elsevier Computer and Security 45,* pp. 274-283, 2014.

[101] Cloud Security Alliance, "GRC Stack," 9 11 2015. [Online]. Available: https://cloudsecurityalliance.org/research/grc-stack/.

[102] M. I. M. Almanea, "A Survey and Evaluation of the Existing Tools that Support Adoption of Cloud Computing and Selection of Trustworthy and Transparent Cloud Providers," in *International Conference on Intelligent Networking and Collaborative Systems*, 2014.

[103] M. Rouse, "Federal Risk and Authorization Program (FedRAMP)," May 2014. [Online]. Available: http://whatis.techtarget.com/definition/Federal-Risk-and-Authorization-Program-FedRAMP.

[104] M. Hillick, "Levelling Up Security @ Riot Games," in *Brucon 0x07*, Ghent, 2015.

[105] R. Gallagher, "Operation Socialist," 13 December 2014. [Online]. Available: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

[106] Shared Assessments, "Evaluating Cloud Risk for the Enterprise," 2010.

[107] A. A. Nada Ahmed, "Modeling Security Risk Factors in a Cloud Computing Environment," *Journal of Information Assurance and Security,* pp. 279-289, 2013.

[108] E. V. d. Sar, “MegaUpload shut down by the feds, founder arrested,” 23 November 2015. [Online]. Available: https://torrentfreak.com/megaupload-shut-down-120119/.

[109] G. Sandoval, “After nearly four years, is it time to just settle the MegaUpload case?,” 23 November 2015. [Online]. Available: http://www.theverge.com/2015/9/28/9409847/megaupload-extradition-hearing-kim-dotcom.

[110] wikipedia, “Megaupload,” 23 November 2015. [Online]. Available: https://nl.wikipedia.org/wiki/Megaupload.

[111] S. Anthony, “Megaupload's demise: What happens to your files when a cloud service dies?,” 23 November 2015. [Online]. Available: http://www.extremetech.com/computing/114803-megauploads-demise-what-happens-to-your-files-when-a-cloud-service-dies.

[112] Google, “Google Transparency Report,” 23 November 2015. [Online]. Available: https://www.google.com/transparencyreport/userdatarequests/legalprocess/#why_might_a_government.

[113] B. Butler, “Report: Nirvanix customers have two weeks to get data out of the cloud,” 23 November 2015. [Online]. Available: http://www.networkworld.com/article/2170916/cloud-computing/report--nirvanix-customers-have-two-weeks-to-get-data-out-of-cloud.html.

[114] K. Leswing, “Apple: "Certain celebrity accounts" were compromised by a targeted attack,” 23 November 2015. [Online]. Available: https://gigaom.com/2014/09/02/apple-denies-icloud-nude-celebrity-hack/.

[115] Imperva, “Man in the Cloud (MITC) Attacks,” Imperva, 2015.

[116] B. Prince, “Stealthy 'Inception' Attackers Hide Behind Layers of Obfuscation,” 23 November 2015. [Online]. Available: http://www.securityweek.com/stealthy-inception-attackers-hide-behind-layers-obfuscation.

[117] M. Rouse, “Social Engineering definition,” 23 November 2015. [Online]. Available: http://searchsecurity.techtarget.com/definition/social-engineering.

[118] Y. Zhang, A. Juels, A. Oprea and M. K. Reiter, “HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis,” *IEEE Symposium on Security and Privacy,* pp. 313 - 328, 2011.

[119] E. Felten, “Side-Channel Leaks in Web Applications,” 24 November 2015. [Online]. Available: https://freedom-to-tinker.com/blog/felten/side-channel-leaks-web-applications/.

[120] M. Einar and C.-H. Eriksson, “Deduplication as an attack vector,” Linköpings Universitet, Sweden.

[121] Dropbox, “Dropbox Business Agreement,” 24 November 2015. [Online]. Available: https://www.dropbox.com/privacy#business_agreement.

[122] Google, “Your security and privacy,” 24 November 2015. [Online]. Available: https://support.google.com/a/answer/60762?hl=en.

[123] P. Venezia, “Sorting Facts from Fiction in the Terry Childs Case,” 24 November 2015. [Online]. Available: http://www.pcworld.com/article/149159/terry_childs_case.html?page=2.

[124] P. Venezia, “Why San Francisco's network admin went rogue,” 2015 November 2015. [Online]. Available: http://www.infoworld.com/article/2653004/misadventures/why-san-francisco-s-network-admin-went-rogue.html.

[125] F. Lardinois, “Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL and Apple Deny Participation in NSA PRISM Surveillance Program,” 26 November 2015. [Online]. Available: http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/.

[126] A. Luttwak, “A new Zeus variant targeting Salesforce.com - Research and Analysis,” 26 November 2015. [Online]. Available: https://www.adallom.com/blog/a-new-zeus-variant-targeting-salesforce-com-accounts-research-and-analysis/.

[127] D. McCullagh, “Dropbox confirms security glitch - no password required,” 30 11 2015. [Online]. Available: http://www.cnet.com/news/dropbox-confirms-security-glitch-no-password-required/.

[128] Crunchbase, “Adallom,” [Online]. Available: https://www.crunchbase.com/organization/adallom#/entity. [Accessed 4 12 2015].

[129] M. Hillick, “Levelling Up Security @Riot Games,” [Online]. Available: https://www.youtube.com/watch?v=7Y8iLXkyD7w. [Accessed 7 12 2015].

[130] Bitglass, “The definitive guide to cloud access security brokers,” Bitglass, 2014.

[131] D. Sullivan, “How can enterprises prevent shadow data leakage,” November 2015. [Online]. Available: http://searchcloudsecurity.techtarget.com/answer/How-can-enterprises-prevent-shadow-data-leakage. [Accessed 10 12 2015].

[132] G. Crump, “How is cloud data loss prevention changed by Shadow-IT,” September 2015. [Online]. Available: http://searchcloudstorage.techtarget.com/answer/How-is-cloud-data-loss-prevention-changed-by-shadow-IT. [Accessed 10 12 2015].

[133] P. Witsenburg, “Help, mijn cloud is lek?,” 10 12 2015. [Online]. Available: http://www.smartbiz.be/achtergrond/165180/help-mijn-cloud-is-lek/. [Accessed 14 12 2015].

[134] S. Martens, “Europa komt met meldplicht datalekken,” Computable, 8 12 2015. [Online]. Available: https://www.computable.nl/artikel/nieuws/security/5659261/250449/europa-komt-met-meldplicht-datalekken.html. [Accessed 14 12 2015].

[135] J. Kastrenakes, “Apple denies iCloud breach in celebrity nude photo hack,” The Verge, 2 9 2014. [Online]. Available: http://www.theverge.com/2014/9/2/6098107/apple-denies-icloud-breach-celebrity-nude-photo-hack. [Accessed 15 12 2015].

[136] J. Ong, “Apple says iCloud wasn't breached in celebrity photo leak, individual accounts were targeted,” The Next Web, 2 9 2014. [Online]. Available: http://thenextweb.com/apple/2014/09/02/apple-claims-icloud-wasnt-breached-celebrity-photo-leak/. [Accessed 15 12 2015].

[137] OWASP, “Blocking Brute Force Attacks,” OWASP, 18 March 2015. [Online]. Available: https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks. [Accessed 15 12 2015].

[138] Forbes, “The World's Biggest Public Companies,” [Online]. Available: http://www.forbes.com/global2000/list/#search:Google_industry:Computer%20Services. [Accessed 16 12 2015].

[139] D. Vellante, “Defining RPO and RTO,” 6 5 2008. [Online]. Available: http://wikibon.org/wiki/v/Defining_RPO_and_RTO. [Accessed 11 1 2016].

Appendix A

Level	*Data Classification and Examples (abridged version)*
5	***Information that would cause severe harm to individuals or the University if disclosed.***
Examples	• Research information classified as Level 5 by an IRB or otherwise required to be stored or processed in a high security environment and on a computer not connected to the Harvard data networks • Certain individually identifiable medical records and genetic information, categorized as extremely sensitive
4	***Information that would likely cause serious harm to individuals or the University if disclosed.***
Examples	• High Risk Confidential Information (HRCI) and research information classified as Level 4 by an IRB • Personally identifiable financial or medical information • Information commonly used to establish identity that is protected by state, federal, or foreign privacy laws and regulations • Individually identifiable genetic information that is not Level 5 • National security information (subject to specific government requirements) • Passwords and Harvard PINs that can be used to access confidential information
3	***Information that could cause risk of material harm to individuals or the University if disclosed.***
Examples	• Research information classified as Level 3 by an IRB • Information protected by the Family Educational Rights and Privacy Act (FERPA) to the extent it is not covered under Level 4 including non-directory student information and directory information about students who have requested a FERPA block • HUIDs associated with names or any other information that could identify individuals • Harvard personnel records (employees may discuss terms and conditions of employment with each other and third parties) • Institutional financial records • Individual donor information • Personal information protected under most other state, federal and foreign privacy laws not classified as Level 4 or 5
2	***Information the disclosure of which would not cause material harm, but which the University has chosen to keep confidential.***
Examples	• Unpublished research work and intellectual property not in Level 3 or 4 • Research information classified as Level 2 by an IRB • Patent applications and work papers, drafts of research papers • Building plans and information about the University physical plant
1	***Public information.***
Examples	• Research data that has been de-identified in accordance with applicable rules • Published research • Published information about the University • Course catalogs • Directory information about students who have not requested a FERPA block • Faculty and staff directory information

Need more detailed information? See the expanded Data Classification Table.
Need to talk to an expert? Contact rdsap@harvard.edu for research data and data use agreement questions and ithelp@harvard.edu for all other security questions. Report any data breach to your Help Desk.

Eff. 7.16.13

HARVARD
UNIVERSITY
Information Technology

University Data Classification Table*

Level 5	Level 4
Information that would cause severe harm to individuals or the University if disclosed.	***Information that would likely cause serious harm to individuals or the University if disclosed.***
Level 5 information includes individually identifiable information which if disclosed would create risk of criminal liability, loss of insurability or employability, or severe social. psychological, reputational, financial or other harm to an individual or group. Level 5 includes research information classified as Level 5 by an IRB.	Level 4 information includes High Risk Confidential Information (HRCI), as defined below, and research information classified as Level 4 by an IRB. Level 4 also includes other individually identifiable information which if disclosed would likely cause risk of serious social, psychological, reputational. financial, legal or other harm to an individual or group. "High Risk Confidential Information" means an individual's name together with any of the following data about that individual: social security number, bank or other financial account numbers, credit or debit card numbers, driver's license number, passport number, other government-issued identification numbers, biometric data, health and medical information, or data about the individual obtained through a research project.
Examples: information covered by a regulation or agreement that requires that data be stored or processed in a high security environment and on a computer not connected to the Harvard data networks, or to be handled in the same manner as the University's most sensitive data; certain individually identifiable medical records and genetic information, categorized as extremely sensitive.	***Examples:*** individually identifiable financial or medical** information ; information commonly used to establish identity that is protected by state , federal or foreign privacy laws and regulations, such as Massachusetts law protecting personal information, and not classified in Level 5; individually identifiable genetic information that is not in Level 5; national security information (subject to specific government requirements); passwords and PINs that can be used to access confidential information.

* *"Confidential Information." refers to all types of data under Levels 2-5. The higher the data level, the greater the required protection.*

**See note on HIPAA.

updated 11.17.14

HARVARD UNIVERSITY
Information Technology

University Data Classification Table

Level 3	*Level 2*	*Level 1*
Information that could cause risk of material harm to individuals or the University if disclosed. Level 3 information includes individually identifiable information which if disclosed could reasonably be expected to be damaging to reputation or to cause legal liability[+]. Level 3 also includes research information classified as Level 3 by an IRB. ***Examples:*** information protected by the Family Educational Rights and Privacy Act (FERPA), to the extent such information is not covered under Level 4, including non-directory student information and directory information about students who have requested a FERPA block; HUIDs when associated with names or any other information that could identify individuals; Harvard personnel records[++]; Harvard institutional financial records; individual donor information; other personal information protected under state, federal and foreign privacy laws and not classified in Level 4 or 5 .	***Information the University has chosen to keep confidential but the disclosure of which would not cause material harm.*** Level 2 information includes unpublished research work and intellectual property not in Level 3 or 4. Level 2 also includes information classified as Level 2 by an IRB. ***Examples:*** patent applications and work papers; drafts of research papers; building plans and information about the University physical plant.	***Public information.*** ***Examples***: research data that has been de-identified in accordance with applicable rules; published research; published information about the University; course catalogs; directory information about students who have not requested a FERPA block; faculty and staff directory information.

[+] See note below on contractual obligations.

[++] Harvard ‘s Confidential Information policy does not restrict or limit the rights of employees to discuss terms and conditions of their employment, including salary and benefits, with each other or with third parties.

Need to talk to an expert? Contact rdsap@harvard.edu for research data and data use agreement questions and ithelp@harvard.edu for all other security questions.
To report a data breach, contact your Help Desk.

Note on Medical Records and HIPAA: Harvard units or programs that are so-called "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA) must comply with HIPAA’s data security rules. As of the effective date of this policy, the covered entities are University Health Services, Harvard Dental Services, and certain University benefits plans. Other units or programs may be required to comply with HIPAA data security rules for limited purposes under the terms of specific contracts, such as a business associate agreement.

Note on Contractual Obligations: Data use agreements, research consent forms and other contracts under which Harvard personnel receive confidential information from outside parties often state specific data use and protection requirements. Harvard personnel working with such information must comply with such requirements. Use of such information must also comply with the applicable Harvard data security requirements if the contract calls for lesser levels of protection.

Appendix B

URL: https://www.dropbox.com/business/customers/case-study-foursquare

Going Local: How Foursquare uses Dropbox Business to stay in sync

Foursquare is a location-based mobile application designed to connect people and places. The app allows people to share and save the places they visit and get personalized recommendations based on where they've been. The Foursquare community is more than 25 million users and one million merchants strong.

Addressing a growing organization

When Foursquare launched its first product in 2009, the small team occupied a single office. This upstart crew was in close quarters and had no trouble sharing documents and project information. Eric Friedman, Foursquare Director of Sales and Revenue Operations, remembers, "It was just a handful of us, so it was easy to stay on the same page." But as the business grew, the headcount did too, and it quickly became apparent that Foursquare needed a more robust, reliable solution for sharing files across locations- and oceans. Says Friedman, "With offices in San Francisco, New York, and London, we needed a viable central file system that would allow us to easily create, organize, and manage all of our digital documents." Friedman set out to evaluate different systems, with security, quality, and reliability at the top of his list of requirements. As an early Dropbox user himself, Friedman says he quickly recognized that "Dropbox was the best solution for digital collaboration." Unlike file systems or network drives, Friedman knew from experience that Dropbox not only made files accessible from any device, but also synced them to the computer. This meant that even when Foursquare employees were traveling and didn't have an Internet connection, they could still access important documents.

"Having all of our files local on everyone's machine and backed up regularly is invaluable. Our rule of thumb has become: if it's not in Dropbox, it doesn't exist."

Operating on common ground

Because Foursquare was such an early adopter of Dropbox, many people from the organization had individual accounts before Dropbox Business was introduced. By the time the company switched to Dropbox Business, it had the system down pat. "Every one of our clients and partners has a home in Dropbox," Friedman says. "Everything that happens with them lives within the application, and it's also where our sales reps, account managers, legal, and design teams store all of their important documents." Having a centralized repository for critical assets makes it fast and easy for employees across the company's three locations to access client contracts, sales presentations, and internal collateral. And when employees need to edit large files in Adobe Photoshop or Microsoft Office, they can access documents and photos quickly because a copy is stored locally on their computers. Dropbox Business has helped Foursquare streamline previously time-consuming administrative tasks as well. As Friedman explains, "It's been incredibly helpful to use Dropbox during new employee onboarding. I can just add people to the team, share one folder, and they'll have everything I reference throughout my welcome process." Foursquare's interactions with external clients, such as merchants and agencies, has also been enhanced by Dropbox Business. Rather than emailing documents as attachments-and causing inbox overload-Foursquare staff can just send links to files in Dropbox. "It's a big time saver, especially when you're talking to twenty or thirty people in an email thread," Friedman says. "It definitely lets us work much faster."

A system that's become indispensable

When it comes to choosing favorite Dropbox Business features, having the ability to share with a link, undelete, and restore previous versions of files rank high for Friedman. He explains, "One instance that really helped me understand the power of Dropbox Business was when someone accidentally deleted a bunch of files we needed. Right away, I was able to go online and restore everything. It's nice to know that you can unwind from an accident very quickly if it happens." Above all else, having local, centralized access to files is what makes Dropbox Business most valuable to Foursquare. "With people on the road and in different offices, it's critical for us to make sure all our important information and documents live in one place and can be easily accessed at any time. Having all of our files local on everyone's machine and backed up regularly is invaluable." Friedman adds, "Our rule of thumb has become: if it's not in Dropbox, it doesn't exist."

Appendix C

URL: http://www.internap.com/2013/06/25/shadow-it-confessions-of-a-rogue-marketer/

Shadow IT: Confessions of a rogue marketer

An Open Letter to IT Departments:

I have a confession to make: in the past*, I've procured cloud services without your approval. I've used the cloud for file sharing, storage, project management and collaboration services and, at any given moment, I had at least four active subscriptions to cloud services that I used for business purposes. More often than not, you didn't even know about any of them.

Was I purposely circumventing you as a peculiar act of defiance or intentionally compromising enterprise security? Of course not. I was just trying to get my job done as efficiently as possible. With tight deadlines, high project volume and lofty campaign goals, I needed the agility that the cloud provides. To be honest, I didn't have the time to create a business case for these services and wait for your approval – especially when you're so busy running day-to-day infrastructure operations and handling high-priority requests from other areas of the business.

I was unknowingly a part of the phenomenon known as Shadow IT – using hardware or software not supported by an organization's IT department. And I'm not alone; Gartner predicts that 35% of enterprise IT expenditures will happen outside of the corporate IT budget by 2015 and the CMO will spend more on IT than the CIO by 2017.

At this point, you may be wondering what prompted me to confess these transgressions (on my current employer's website, no less). On our recent webinar Hybridization: Shattering Silos Between Cloud and Colocation, my colleague Adam Weissmuller spoke about Shadow IT and how cloud's accessibility and immediacy to the end user can often come at the expense of IT security and control. So, beyond letting you know that (a) the concept of Shadow IT is real, (b) it's likely happening in your organization more than you realize and (c) I'm sorry for putting your control measures and security at risk, I wanted to share with you Adam's suggestion for bringing Shadow IT back into the fold.

After identifying Marketing as one of the most notorious Shadow IT offenders, Adam illustrated how a cloud and colocation hybridized environment could enable quick, on-demand provisioning of additional server capacity for an upcoming marketing campaign. This type of infrastructure would enable IT to provide assets on demand, without capital outlay, and under its controls, while marketing can run their campaign on time without compromising enterprise security. You can listen to the full webinar recording here for more details, as well as other hybridization use cases: Hybridization: Shattering Silos Between Cloud and Colocation.

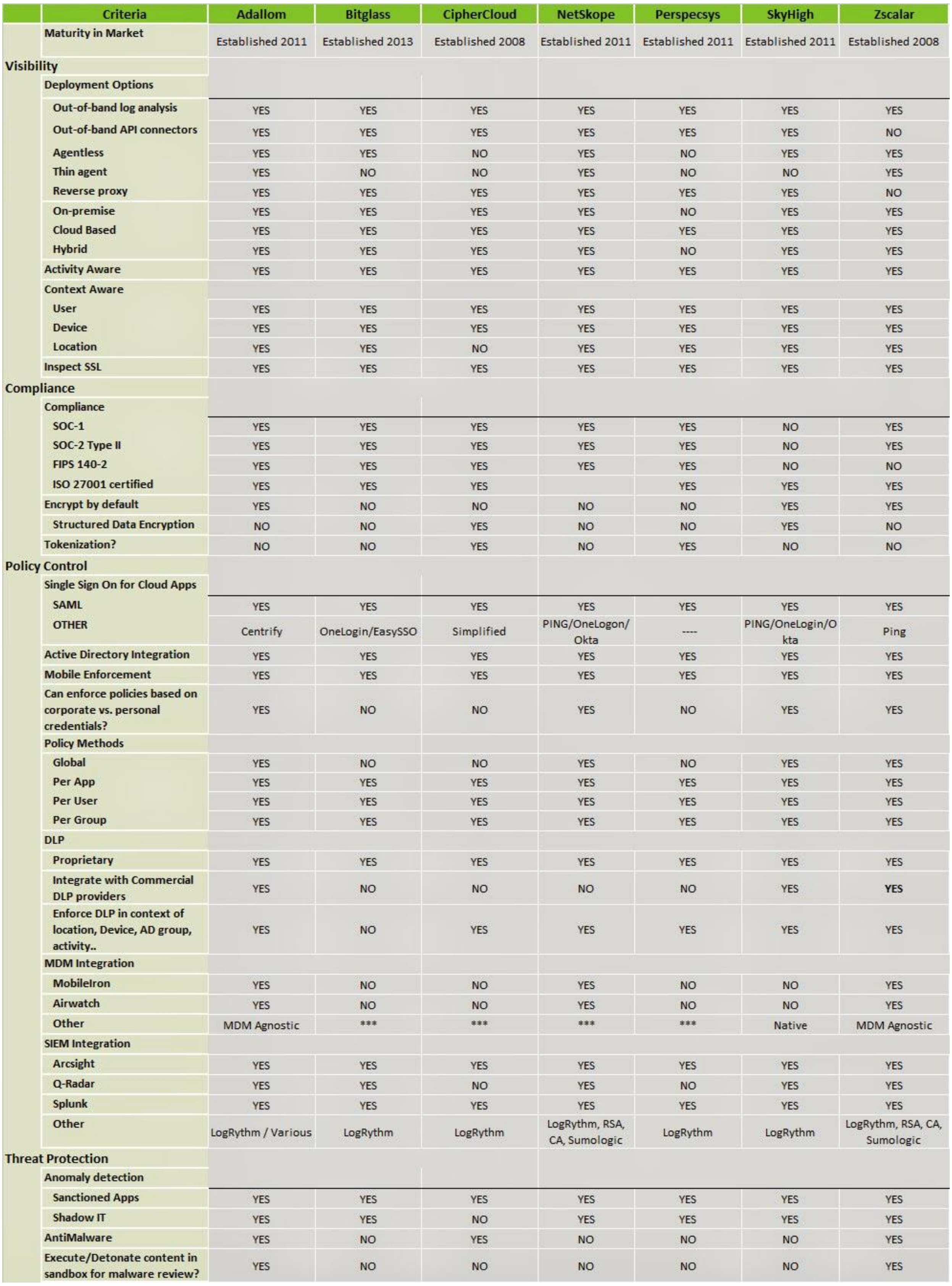
Thanks for reading and letting me shine the light on Shadow IT.

*Note that I have never and will never engage in such reckless behavior at Internap.

Posted on June 25, 2013 by Shannon Renz & filed under All Posts, Cloud Computing, Colocation

Appendix D - CASB comparison

URL: http://security-musings.blogspot.be/2015/04/comparing-cloud-access-security-broker.html



	Criteria	Adallom	Bitglass	CipherCloud	NetSkope	Perspecsys	SkyHigh	Zscalar
	Maturity in Market	Established 2011	Established 2013	Established 2008	Established 2011	Established 2011	Established 2011	Established 2008
Visibility								
	Deployment Options							
	Out-of-band log analysis	YES	YES	YES	YES	YES	YES	YES
	Out-of-band API connectors	YES	YES	YES	YES	YES	YES	NO
	Agentless	YES	YES	NO	YES	NO	YES	YES
	Thin agent	YES	NO	NO	YES	NO	NO	YES
	Reverse proxy	YES	YES	YES	YES	YES	YES	NO
	On-premise	YES	YES	YES	YES	NO	YES	YES
	Cloud Based	YES	YES	YES	YES	YES	YES	YES
	Hybrid	YES	YES	YES	YES	NO	YES	YES
	Activity Aware	YES	YES	YES	YES	YES	YES	YES
	Context Aware							
	User	YES	YES	YES	YES	YES	YES	YES
	Device	YES	YES	YES	YES	YES	YES	YES
	Location	YES	YES	NO	YES	YES	YES	YES
	Inspect SSL	YES	YES	YES	YES	YES	YES	YES
Compliance								
	Compliance							
	SOC-1	YES	YES	YES	YES	YES	NO	YES
	SOC-2 Type II	YES	YES	YES	YES	YES	NO	YES
	FIPS 140-2	YES	YES	YES	YES	YES	NO	NO
	ISO 27001 certified	YES	YES	YES		YES	YES	YES
	Encrypt by default	YES	NO	NO	NO	NO	YES	YES
	Structured Data Encryption	NO	NO	YES	NO	NO	YES	NO
	Tokenization?	NO	NO	YES	NO	YES	NO	NO
Policy Control								
	Single Sign On for Cloud Apps							
	SAML	YES	YES	YES	YES	YES	YES	YES
	OTHER	Centrify	OneLogin/EasySSO	Simplified	PING/OneLogon/Okta	----	PING/OneLogin/Okta	Ping
	Active Directory Integration	YES	YES	YES	YES	YES	YES	YES
	Mobile Enforcement	YES	YES	YES	YES	YES	YES	YES
	Can enforce policies based on corporate vs. personal credentials?	YES	NO	NO	YES	NO	YES	YES
	Policy Methods							
	Global	YES	NO	NO	YES	NO	YES	YES
	Per App	YES	YES	YES	YES	YES	YES	YES
	Per User	YES	YES	YES	YES	YES	YES	YES
	Per Group	YES	YES	YES	YES	YES	YES	YES
	DLP							
	Proprietary	YES	YES	YES	YES	YES	YES	YES
	Integrate with Commercial DLP providers	YES	NO	NO	NO	NO	YES	**YES**
	Enforce DLP in context of location, Device, AD group, activity..	YES	NO	YES	YES	YES	YES	YES
	MDM Integration							
	MobileIron	YES	NO	NO	YES	NO	NO	YES
	Airwatch	YES	NO	NO	YES	NO	NO	YES
	Other	MDM Agnostic	***	***	***	***	Native	MDM Agnostic
	SIEM Integration							
	Arcsight	YES	YES	YES	YES	YES	YES	YES
	Q-Radar	YES	YES	NO	YES	NO	YES	YES
	Splunk	YES	YES	YES	YES	YES	YES	YES
	Other	LogRythm / Various	LogRythm	LogRythm	LogRythm, RSA, CA, Sumologic	LogRythm	LogRythm	LogRythm, RSA, CA, Sumologic
Threat Protection								
	Anomaly detection							
	Sanctioned Apps	YES	YES	YES	YES	YES	YES	YES
	Shadow IT	YES	YES	NO	YES	YES	YES	YES
	AntiMalware	YES	NO	YES	NO	NO	NO	YES
	Execute/Detonate content in sandbox for malware review?	YES	NO	NO	NO	NO	NO	YES