Student Number: 100783840
Robert Sperrey

A Risk Analysis of Enterprise Cloud Services

Supervisor: Dr. Geraint Price

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date: August 25th 2015
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>List of Abbreviations and Acronyms</td>
<td>4</td>
</tr>
<tr>
<td>List of Figures and Tables</td>
<td>6</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>7</td>
</tr>
<tr>
<td><strong>Chapter 1 Introduction</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Chapter 2 The Taxonomy of Cloud</strong></td>
<td>10</td>
</tr>
<tr>
<td>2.1 NIST definition of Cloud Computing</td>
<td>10</td>
</tr>
<tr>
<td>2.1.1 Software as a Service (SaaS)</td>
<td>10</td>
</tr>
<tr>
<td>2.1.2 Platform as a Service (PaaS)</td>
<td>10</td>
</tr>
<tr>
<td>2.1.3 Infrastructure as a Service (IaaS)</td>
<td>11</td>
</tr>
<tr>
<td>2.2 NIST Cloud Computing Deployment models</td>
<td>14</td>
</tr>
<tr>
<td>2.3 Why is the NIST Cloud Computing Definition Inadequate?</td>
<td>14</td>
</tr>
<tr>
<td>2.4 NIST Cloud Computing Reference Model</td>
<td>16</td>
</tr>
<tr>
<td>2.5 Why is the NIST Cloud Computing Reference Architecture inadequate?</td>
<td>17</td>
</tr>
<tr>
<td>2.6 The Jericho Cloud Cube Model</td>
<td>18</td>
</tr>
<tr>
<td>2.7 The Cloud Security Alliance Cloud Computing Architectural Framework</td>
<td>20</td>
</tr>
<tr>
<td>2.8 Cloud vs Mainframe Computing</td>
<td>21</td>
</tr>
<tr>
<td>2.9 Detailed Identification of Cloud Components</td>
<td>22</td>
</tr>
<tr>
<td><strong>Chapter 3 Virtualisation and its role in the Cloud</strong></td>
<td>24</td>
</tr>
<tr>
<td>3.1 Introduction to Virtualisation</td>
<td>24</td>
</tr>
<tr>
<td>3.1.1 Density of Computing Power and cost effective security</td>
<td>24</td>
</tr>
<tr>
<td>3.2 The Hypervisor</td>
<td>25</td>
</tr>
<tr>
<td>3.3 Virtual Machine Management</td>
<td>25</td>
</tr>
<tr>
<td>3.4 Evolution of Virtualisation Security Mechanisms</td>
<td>26</td>
</tr>
<tr>
<td>3.5 Virtual Networking</td>
<td>27</td>
</tr>
<tr>
<td>3.6 Important Security Research in the area of Virtualisation</td>
<td>28</td>
</tr>
<tr>
<td>3.6.1: Blue Pill</td>
<td>28</td>
</tr>
<tr>
<td>3.6.2 Cloudburst</td>
<td>29</td>
</tr>
<tr>
<td><strong>Chapter 4 An analysis of Cloud based risks</strong></td>
<td>31</td>
</tr>
<tr>
<td>4.1 Objectives and Methodology</td>
<td>31</td>
</tr>
<tr>
<td>4.2 Summary results:</td>
<td>31</td>
</tr>
<tr>
<td>4.3 Source Literature</td>
<td>32</td>
</tr>
<tr>
<td><strong>4.3 Policy &amp; Organisational Risks</strong></td>
<td>33</td>
</tr>
<tr>
<td>Risk 1: Provider Lock In</td>
<td>33</td>
</tr>
<tr>
<td>Risk 2: Loss of Governance/Compliance Challenges</td>
<td>35</td>
</tr>
<tr>
<td>Risk 3: Loss of Business Reputation Due to co-tenant activities</td>
<td>38</td>
</tr>
<tr>
<td>Risk 4: Cloud Service Termination or Failure</td>
<td>40</td>
</tr>
<tr>
<td>Risk 5: Cloud Provider Acquisition</td>
<td>42</td>
</tr>
<tr>
<td>Risk 6: Cloud Supply Chain Failure</td>
<td>43</td>
</tr>
<tr>
<td><strong>4.4 Technical Risks</strong></td>
<td>45</td>
</tr>
<tr>
<td>Risk 7: Resource Exhaustion</td>
<td>45</td>
</tr>
<tr>
<td>Risk 8: Isolation Failure</td>
<td>47</td>
</tr>
<tr>
<td>Risk 9: Cloud Provider Malicious Insider</td>
<td>49</td>
</tr>
<tr>
<td>Risk 10: Management Interface Compromise</td>
<td>51</td>
</tr>
<tr>
<td>Risk 11: Intercepting Data In Transit</td>
<td>53</td>
</tr>
<tr>
<td>Risk 12: Insecure or Ineffective Deletion of Data</td>
<td>55</td>
</tr>
<tr>
<td>Risk 13: Distributed Denial of Service</td>
<td>58</td>
</tr>
</tbody>
</table>
Risk 14: Loss of Encrypton Keys ................................................................. 60
Risk 15: Subject of malicious probes or scans ........................................... 62
Risk 16: Compromise of Service Engine .................................................... 64
Risk 17: Conflicts between Customer Hardening procedures and Cloud environment .......................................................... 65
Risk 18: Subpeona and E-discovery ............................................................. 66
Risk 19: Risk from Changes of Jurisdiction ................................................ 67
Risk 20: Data Protection Risks .................................................................. 68
Risk 21: Licensing Risks ........................................................................... 69
Chapter 5 Conclusions ............................................................................. 71
Bibliography .............................................................................................. 73
List of Abbreviations and Acronyms

AMD – Advanced Micro Devices - CPU vendor
AMD-V – AMD Secure Virtual Machine Architecture
AV – Anti-Virus
AWS – Amazon Web Services (PaaS vendor)
CA – Certificate Authority – entity issuing digital certificates that certify ownership of a signature key used for data origin authentication in the SSL protocol.
CCTV – Closed Circuit Television
CIDDos – Cloud Internal Denial of Service
CPU (computer) Central Processing Unit
CRM – Customer Relationship Management (Line of Business Application)
CSA – Cloud Security Alliance – Cloud Industry Organisation promoting Cloud Security
CSP – Cloud Service Provider
DoS – Denial of Service
DDoS – Distributed Denial of Service
DMA – Direct Memory Access (by Server add on devices)
DPA – (UK) Data Protection Act
ENISA – European Network and Information Security Agency
EAL4 – Evaluation Assurance Level 4 – certification level used in Common Criteria independent security evaluation standard
Foursquare – geolocation services vendor
Gartner – Market research organisation
HIPAA – Health Insurance Portability Accountability Act – U.S legislation applicable to organisations handling personally identifiable data
IaaS – Infrastructure as a Service
IEEE – Institute of Electronic and Electrical Engineering (standards body)
Intel – CPU vendor
IP – Internet Protocol
IPSec – Secure Internet transmission protocol offering confidentiality, Integrity and Data Origin Authentication.
ISO 27001 – International Standard concerning Information Security
ISP – Internet Service Provider
ITU-T X.1500 (also known as CYBEX) Cloud audit standard addressing Cloud Supply Chain.
LEA – Law Enforcement Agency
Linux – Open Source, community developed operating system
Microsoft Office 365 – hosted office automation suite
Netflix – Video on Demand provider
NIST – (American) National Institute of Standards and Technology
NTFS – New Technology File System - Microsoft originated storage file system
OEM – Original Equipment Manufacturer
OS – Operating System
OVF – Open Virtualisation Format (facilitates virtual machine portability)
PaaS – Platform as a Service
PCI-DSS – Payment Card Industry Data Security Standard (information security standard for organisations processing Credit Card data)
PII – Personally Identifiable Information
RAID – Redundant Array of Inexpensive Disks – a method of using multiple disks to assure data integrity
RAM – Random Access Memory – computer working memory space.
Reddit – Social Networking service
SaaS – Software as a Service
SANS Institute – U.S Cyber Security training Organisation
SecaaS – Security as a Service – CSA definition of Cloud based Security services
SED – Self Encrypting Disk
SLA – Service Level Agreement
SSAE16 SOC1 - (formerly SAS type 70) audit standard based on Committee of Sponsoring Organisations of the Treadway Commision(COSO) relating to Organisational Governance
SSD – Solid State Disk (offering secondary storage with no moving parts)
SSL – Secure Socket Layer – data transmission standard offering confidentiality and data origin authentication
ToE – Target of Evaluation – used in CC EAL4
TPM – Trusted Platform Module (for encryption key storage & generation)
UEFI – Unified Extensible Framework Interface – security hardened computer basic input output system
VLAN – Virtual Local Area Network
VM – Virtual Machine
VMM – Virtual Machine Manager
VMWARE – Vendor of Virtualisation software
VT-x – Intel Virtualisation Technology (CPU) Extensions
XEN – Open Source community developed virtualisation environment
XML – eXtensible Markup Language – internet based application programming interface
List of Figures and Tables

Figure 1: Risk vs. level of functionality in Cloud Services ................................. 15
Figure 2: Jericho Cloud Cube model ................................................................. 19
Figure 3: Key Cloud Components ....................................................................... 22
Figure 4: VMWARE virtualisation overview ....................................................... 26
Figure 5: Amazon Web Services Management Console ..................................... 51
Figure 6: Mitigated Cloud Risk overview ............................................................ 70
Executive Summary

The results of this study give grounds for optimism about the security of applications and data hosted in the Cloud.

The technology and mechanisms that make the efficiencies of Cloud Computing possible are mature and well scrutinised, with their origins in academic studies going back to 1970s Grid computing. Steady practical application and development since that time has resulted in a tight coupling of low cost, standard hardware and software based security mechanisms that minimise attack surfaces and have little in the way of proven real-world vulnerabilities. Network technologies and security tools are well understood and have evolved to a point where if properly implemented, give a high level of confidence in keeping intruders at bay. Data encryption and other data anonymisation tools remove many risks around data deletion, data protection and jurisdiction.

Indeed, there is a case to say that economies of scale in the Cloud allow best of breed tools and security management to be more cost effectively applied to a large number of Cloud tenants. The practical outcome of this could actually be better treatment of risk in the Cloud environment than in the traditional model where organisations look after their own IT infrastructure and apply their own security mechanisms.

However, it’s not all sunshine as the risk analysis later in this document shows. The key remaining risks revolve around governance, and trust in the Cloud Service Provider. If they doing everything they say they will do to maintain Security, then most of the risks are removed, the trouble is, how can one be sure they will do what they say they will? A trend that makes this worse is multi-tiering of providers, who build their service on the basis of an underlying Cloud platform from another provider. You may have an agreement with your direct provider, but what certainty or control does one have concerning what goes on at the lower layers, where failure could prove catastrophic to your service and thus your business? A further aspect of Cloud governance that reduces confidence is that the main industry bodies are based around voluntary membership who mainly only require self-certification to claim conformance to the standards they mandate for accreditation or membership.

Contractual safeguards are another key concern for prospective Cloud service Customers. Very large businesses with considerable buying power may find it possible to be able to negotiate a supply agreement with a Cloud Provider. Many, however, are ‘click to accept’ agreements with terms overwhelmingly favourable to the Cloud Service Provider (CSP). Either way, it is the case that the majority of Cloud Service contracts limit liability of the provider to a level that gives them little incentive to take security seriously.

To Sum up, most technical risks are well covered. Significant issues that remain are around governance and compliance. Put in one sentence: it is possible to outsource most things, but it is difficult to outsource responsibility.
Chapter 1 Introduction

A basic definition of ‘Cloud Computing’ is “the storage, processing and use of data on remotely located computers accessed over the Internet”. (EU Commission, Unleashing the Power of Cloud Computing in Europe) [1]

This study is motivated by the wholesale transference in recent years, of proprietary data and business processes to the Cloud, by business organisations of all sizes.

The aim is to try and understand what Security risks such an organisation is opening themselves up to, and to try and understand what level of control over security they may have. In short, what can they influence in terms of Cloud security, and what remaining issues may they have to accept. In doing this it is hoped to enable informed procurement and operational decisions concerning Cloud outsourcing.

Most organisations can realise a huge bottom line cost saving by transitioning their information systems to a Cloud environment. However, the question is, how can that organisation avoid the potentially business-fatal costs associated with an information security breach?

In order to provide focus, the primary audience that this document is intended for is medium size business, in the region of up to 1000 users. This kind or organisation is large enough to realise significant extra value from Cloud Computing. An organisation of such size also requires great commitment in moving to cloud and is large enough to attach great value to the risks involved. However, it is probably not large enough to have sufficient buying power to dictate terms to a potential provider or to commission a private Cloud. Furthermore, we have chosen to consider organisations that utilise applications (such as Customer Relationship Management, Human Resources or Accounts) that are cloud based, as there is a higher level of risk and lower level of control for such organisations. In short, it can be said that such a group has the most risk involved in outsourcing to the Cloud.

In Chapter Two we define the Cloud and its components so we can better identify the vulnerabilities. Various models exist to describe the main contexts, deliverables and actors in typical Cloud scenarios. We analyse these models to determine if they really measure up to against what we see in the real world. We also propose comparative risk profiles for the different classifications of Cloud service in Figure 1 on page 15. Finally, a comparison of a modern Cloud services versus mainframe technology from 30 years ago is made in order to illustrate some key differentiating characteristics of Cloud that can also be a specific source of vulnerabilities.

In Chapter Three we examine the underlying virtualisation technology that enables Cloud to offer such effective resource sharing and thereby cost efficiency. The history of this technology and how it has evolved with respect to security is examined. We also analyse the scrutiny that this technology has undergone over the years. Through this discussion and analysis, we arrive at
an overall assessment of the level of security associated with this technology and the risk that it may pose to potential users of Cloud services.

Chapter Four is the main analysis of this study. Literature sources drawn from studies by Cloud industry associations, independent market research, press sources and governmental agencies were reviewed to determine a representative list of the risks that are most pertinent to Cloud computing. Each of these risks was then analysed in detail by the author, with appropriate mitigations proposed for each one. Based on this, it is identified if a given risk really could be eliminated or reduced via appropriate treatment, or if it would likely remain a key concern that our target audience should consider very carefully, before making a commitment to engage Cloud services. The reasoned analysis used in this process is based on the author’s period of study on the Royal Holloway Information Security MSc, twenty years of practical experience working in the information technology sector, and the information sources identified in Chapter Three and the Bibliography section. An graphical summary of the result of this analysis is shown in Figure 6 on page 70.

The Conclusion section gives some high level recommendations for those considering Cloud, and also some suggestions for further areas of study.

Finally in this introductory chapter, during the research for this document I came across a press article that perhaps illustrates why I was motivated to study this particular area. In it, a senior executive of a large and well known British company that provides Cloud based accountancy software to thousands of small and medium businesses, gives opinion on the relevance of Security in the Cloud. (Online Security – Dark Spectre or Damp Squib? Accountingweb, 3/11/14, accessed 8/8/15 [2]). The essence of the article is that the data of small/midsize companies is uninteresting and thus not worth worrying about. A direct quote:

“For the smaller business with less of a national profile, the risks are fewer. There’s less cachet in such a business being targeted, and the smaller amount of customer data and financial records means the prize is less tempting for hackers”

Such an attitude seems shocking from a firm that is the guardian of the data of so many small and medium size organisations. Do they take any safeguards at all and at what point in their view does the data become worth worrying about? Who makes that judgement? Hopefully, in the course of this document the detail on how to choose a trustworthy Cloud Service Provider (CSP) will become apparent.
Chapter 2 The Taxonomy of Cloud.

In order to perform a valid assessment of the risks attributable to Cloud Computing, it is necessary to define the different types of Cloud Service, and the most important components of it.

Fortunately, there are a number of widely accepted definitions to choose from, although as we will discuss it is arguable if they fully describe the current Cloud Computing landscape.

2.1 NIST definition of Cloud Computing
One Cloud framework, first drafted in 2009 and finalised in 2011, and which has since gained widespread acceptance, is the American National Standards Institute (NIST) Definition of Cloud Computing SP 800-145 [3]. This has become widely referenced by other literature in this field and so makes a good orientation point. This NIST definition identifies three Service Models and then overlays them with four Deployment models. The three Service Models are:

- 2.1.1 Software as a Service (SaaS).
  This refers to a situation where the end user of the Cloud Service accesses an application hosted and managed by the CSP. The application is usually developed and/or owned by the CSP. The data manipulated by the application resides on the infrastructure belonging to the CSP, and the end user gains access through a web browser or some other kind of thin client running on their device (which could be a PC, Smartphone, Tablet, embedded device and so forth).

  From an information security perspective this can have a positive aspect because it means data can be locked down inside the cloud, removing data risks related to the endpoint (such as loss or theft of the device). However, it also means control is relinquished to the CSP, and there is an implicit degree of lock-in and required trust, especially if there is a high degree of business process integration between the application and operations of the cloud service customer.

  Examples of SaaS applications with such a high degree of integration are customer relationship management (CRM) services, human resources Management platforms or online accounts packages. Large companies may take months or even years to fully integrate their businesses with such packages – meaning they are then very tightly bound to the provider and have few options to quickly or cost effectively switch if they should identify the need.

- 2.1.2 Platform as a Service (PaaS) refers to a situation where the CSP hosts a computing platform that is accessible to the end user, and upon which the end user places and manages their own application. Such application could be an off the shelf application, or one developed and
maintained by the end user. In such cases, as well as the hardware platform, the connectivity, physical and environmental necessities, the CSP will likely provide an operating system environment on behalf of the end user. Most often, this will be a virtualised environment, allowing efficient use of resources (discussed in Chapter 2). In this PaaS Service model, it can be argued that responsibility for the data management has the potential to be ambiguous. For example which party has the responsibility to back up the Operating System environment and which to back up the application data? The application data, its regularity of backup, change control, journaling and data version generations may be under control of the service user, or it may be under control of the PaaS provider. There is a risk here that needs to be reduced by a clear agreement and establishment of service levels by creating a clear demarcation between responsibilities of the Service Provider compared responsibilities of the customer.

A widely deployed example of a PaaS service would be Amazon Web Services (AWS). This has been extremely successful and is deployed at huge scale – enabling the pricing of such a service to be very low. The scale at which it is deployed, and the vast number of tenants served by AWS makes it arguably the closest to the deployment of Utility Computing. The idea that computing resources can be ubiquitously available at large scale, cheap due to economies of scale, and with predictable availability and minimum downtime – just like energy, water and waste utilities.

However, it can be argued that PaaS is not yet a Utility in the same sense mainly due to the fact that it is controlled and owned by multiple private enterprises, even if a few of those private enterprise organisations are becoming dominant in the marketplace and arguably close to monopolistic. Contrast this with the traditional Utility model the suppliers of which have usually originated in State ownership, and even if they are not still in such public ownership are tightly regulated by Government. This is not the case with such Cloud Computing suppliers.

There is a case to say that the consequences of a player of the stature of AWS going out of business, gaining a market stranglehold, falling into ownership of malign ownership or just badly managed, or any number of other threats, could cause severe disruption to services used by large numbers of people which may have knock on consequences for even larger numbers of people. This is a significant security risk (see Risk 4: Cloud Service Termination or Failure, Page 35).

- **2.1.3 Infrastructure as a Service (IaaS)** is the last of the three NIST service models. In this model, the service user has a highest degree of input into the final solution in that they will usually provide the application, the operating system environment and will be responsible for the management and control of these components.

The environment will not necessarily be virtualised (in contrast with PaaS) and the end customer will usually have full tenancy of a given server. The
IaaS provider will usually be responsible for everything below the operating system.

This model is closest to what used to be referred to as ‘hosting’ before the concept of Cloud Computing was in general use. This means the provider literally provides a server, in a rack, in a managed data centre.

All the means to reliably enable the functionality of that server are also provided by the IaaS vendor:

- power (should be redundant, conditioned and with standby facilities such as uninterruptible power supplies, generators or both)
- air conditioning,
- fire control (early smoke detection, oxygen elimination systems to halt combustion)
- physical security measures (security personnel monitoring access and asset movement, access control, CCTV)
- telecoms connectivity.

The last area, telecommunications, is obviously crucial; if there is no telecoms connectivity the customer will not be able to access the service. Thus such providers should usually provide high speed backbone internet connectivity with redundant sources of connectivity from different suppliers. As well as assuring availability from the ability to use different communications paths and thus avoid external network disruption, this reduces dependence on a given supplier and can be a way to reduce telecoms costs through least cost routing. For these reasons, such facilities are often located near or in major telecoms interconnect facilities. Such providers may offer multiple geographic locations with mirroring or failover such that if there is a disaster at one facility the service can be resumed at the backup site.

In general, the IaaS provider is more concerned with provision of facilities rather than applications or computing platforms, for which the service user is responsible and therefore assumes more control. An example of such an IaaS provider is Rackspace.com. Although also active in PaaS, Rackspace is one of the largest worldwide providers of IaaS facilities and started their operations in this sector. Their charging model is based around a per-gigabyte of storage per-hour of use model. This a major motivator for their (and most cloud service) customers; instead of having to make major capital expenditures, they can pay as they go, take such capital expenditure off their balance sheets and pay for their IT expenses from operating expense (Opex) budgets which is a more efficient use of their funds, and results in a balance sheet that is more attractive to shareholders and investors. Though the transference of risk, complication and non-core activity to third parties is attractive, it is probably this transference of financial burden from Capex to Opex budgets that is the major driver of cloud adoption in companies.

It should be noted that the roles and responsibilities of the CSPs in the different models are not exclusive, but rather, additive. That is, a PaaS provider also needs to fulfil the roles, responsibilities and functionality of an
IaaS provider, and a SaaS provider needs to fulfil the roles, responsibilities and functionalities of a PaaS and IaaS. However, as we shall discuss in section 2.2, there is an increasing trend for providers to outsource certain roles which introduces additional security concerns.
2.2 NIST Cloud Computing Deployment models

The NIST definition further identifies four deployment models:

- **Private Cloud** where the Cloud service are used by only one organisation (even though that may be extended across many different departments, such as government for example).
- **Community Cloud** where the cloud is provided for a number of peer organisations and is possibly hosted by one of those organisations.
- **Public Cloud** where the cloud is operated by a non-peer organisation and is open to any type of organisation.
- **Hybrid Cloud** where one or more of the above deployment models are mixed, but the clouds are linked on a technological level to provide some kind of extra functionality such as load balancing.

For the mid-sized organisations that are the focus of this study, it can be argued that the biggest financial savings are likely to be from **Public cloud**, where the cost of the assets is spread over a greater number of users and all operations are outsourced to a third party. Such companies are therefore less likely to participate in Clouds based on the other deployment models.

One could also say that the risks applicable to Public Cloud are a superset of those applicable to the other, more closed models: some of the policy and organisational risks in the more closed models may not apply, by virtue of the fact that there should be more control possible in a more closed environment. In this study we will concentrate on risks applicable to the Public Cloud as this is more relevant to our target audience, but it is likely to be the case that some of these risks could be eliminated through use of the other more closed deployment models, albeit with a likely higher cost.

2.3 Why is the NIST Cloud Computing Definition Inadequate?

Although it is a useful reference point, this study takes the view that the NIST definition is only partially adequate for the purposes of anyone looking to perform a risk evaluation around a given Cloud Service Provider (CSP). This is because increasingly, the service offered to an end user is layered and comprises components sourced from different providers.

A SaaS provider may only actually be in control of the application layer of the service, and they may outsource the platform element of the service to another service provider. In theory, that platform provider could outsource the Infrastructure element of the service to a third provider. Each provider in the chain gives up a degree of control and influence over the risks involved in the part of the service they are outsourcing to the provider below.

The end customer may feel they are managing the risk adequately via contractual safeguards and other due diligence that we shall discuss in Chapter 3, but in reality they may not even know that the lower layer elements of the service are outsourced to fourth and fifth parties, and thus have no knowledge and even less control over the risks involved. A counter argument
could be that the top level contract with the SaaS provider provides the necessary safeguards, but this assumes that all controls and contractual provisions down the chain are adequate and properly drafted and enforced.

This concept of Cloud Supply Chain is also discussed in *Cloud Computing Law*, Millard P17 [4].

The major significance is that an outage at the IaaS or PaaS levels necessarily leads to an outage at the SaaS level.

This is illustrated in some historical outages of well known services such as Netflix, Reddit and Foursquare that one might have expected were standalone services, but in fact are underpinned by AWS. When AWS went down, so too did these services. This is illustrated in an online article from Infoworld (*The 10 Worst Cloud Outages and What We Can Learn From Them* – JR Raphael 27-6-2011)[5]. The article also illustrates what little control the SaaS provider has when this occurs; effectively there is nothing they can do until the PaaS recovers and in the meantime they will lose revenue because they cannot fulfil service to their end customer.

The NIST Cloud Computing Definition does not take any account of such nested services, and how this modifies the risk of any user at the top level of the chain. Figure 1 below, created as part of this study, is intended to illustrate this loss of control and hence increased risk (y axis) incurred by the end service user, mapped against the level of functionality from the different types of service (x axis):

![Risk vs. level of functionality in Cloud Services](image)

Figure 1: Risk vs. level of functionality in Cloud Services

Saas = Software as a Service   Paas = Platform as a Service   Iaas = Infrastructure as a Service
2.4 NIST Cloud Computing Reference Model

There is a further NIST *Cloud Computing Reference Architecture* (SP 500-2920) [6] that expands upon their Cloud Computing definition. In this, NIST add more depth to their definition, through definition of a set of Cloud ‘actors’. It also identifies the need for a management layer and introduces the concepts of security including whom should assume various security responsibilities. It also introduces the concept of portability of Cloud applications.

The five actors defined in the NIST reference architecture are:
- Provider
- Consumer
- Auditor
- Broker
- Carrier.

Provider and Consumer are the same roles we have already discussed when examining the NIST Cloud Computing definition.

The Cloud Auditor is a proposed independent body that can evaluate a provider’s Cloud service and security controls, and measure them against standards.

The Cloud Broker is a third party between the Cloud User and one or more Cloud Providers, and whom provides added value through ‘intermediation, aggregation and arbitrage’ Consideration of the way in which enterprises source and commission IT services bears out the validity of this notion; however, in actuality it can be argued that these tasks are fulfilled in real life by Systems Integrators and Resellers. It is these two organisations that often act as trusted advisors to the Enterprise customer and whom may propose ‘best of breed’ solutions to their customer. For instance, a cloud based CRM service from one cloud provider, a hosted voice service from another and so forth.

For instance, any number of resellers now propose the cloud based Microsoft Office 365 hosted desktop application suite to their customers – probably more enterprises will soon choose this presentation of Office than the on premise version, if not already. Such ‘brokers’ will earn their keep via a sales commission from the Cloud providers in question, or some other commercial (perhaps consultancy) arrangement with their customer. However, it is arguable if these parties in reality provide any form of value add in terms of intermediation, aggregation or arbitrage, or if the end user would expect such support direct from the Cloud Provider. Therefore is questionable if they really provide a solution in terms of security, or if the Cloud user is still directly reliant on the CSP.

The Cloud Carrier defined by NIST is the telecommunications intermediary between the Cloud Provider and the End Customer. However, in reality it can be argued that there are probably two providers; an Internet Service Provider
(ISP) contracted to the Customer and quite possibly a different one to the CSP. Each of these may have different deliverables (called Service Level Agreements or SLAs) in terms of things like speeds, time to fix outages, traffic management and so forth. To be of any use, terms of such SLAs should match between CSP and customer, or one party will be restricted by what is available from the SLA of the other. In any case the management and selection of ISPs is an important factor in the availability and therefore security of the Cloud service as the availability of the chosen service or application now depends on this - the end to end security being only as strong as the weakest link.

2.5 Why is the NIST Cloud Computing Reference Architecture inadequate?

Again for our purposes of examining the typical enterprise situation with respect to Security of Cloud Services, the NIST reference architecture does add some level of depth and colour, and defines some valid roles of players participating in the Cloud ecosystem. However, there it can be argued there are still some notable deficiencies for our purposes.

There is still no consideration given to CSPs who stack the services, and resell an IaaS and/or PaaS as part of a SaaS, with each layer abstracting control from the end user and potentially adding risk.

Furthermore, the NIST Reference Architecture makes mention of portability; the idea that in the event of security breaches or other dispute an end cloud customer could remove the SaaS application and data from one provider and move it transparently to another. In reality such applications are usually proprietary to the SaaS provider and not only would there likely be licensing and intellectual property issues, but the SaaS vendor would likely have a vested interest in making it as difficult as possible to move the service to another supplier. An organisation that has chosen a SaaS supplier, and possibly modified their business practices and procedures to fit in with this could easily become locked in to that supplier (see Risk 1, Provider lock-in on Page 31).

The NIST reference architecture also makes much of independent audit. However, in reality, unless they have exceptional levels of buying power and therefore leverage with the CSP, there is an argument to say an average Cloud customer of the size we have defined relevant to this study is unlikely to be able send its chosen auditors into a cloud provider to audit them. This alternative view is backed up by a 2012 study by the Stanford Technology Law Negotiating cloud Contracts: Looking at Clouds from Both side Now [7]. This review of 20 Cloud service customers found that the majority of CSPs refused them the possibility to perform pre or post contract audits on basis of cost and supposed security risk.
However, audit can be a relevant tool for the prospective customer if the Cloud provider should themselves choose to do an internal audit against a recognised standard or retains their own external auditor to do this. This is not as unbiased as a third party audit, as there is still a link between provider and auditor, but it is perhaps a relevant yardstick with which to compare providers. It is also potentially in the interests of the provider to do this, as a differentiator from their competitors. There are a number of standards that are frequently applied to Cloud implementations including SSAE16 SOC1, PCI-DSS, HIPAA and ISO 27001. However, they are not exclusively aimed at Cloud, and were developed in part before the mainstream advent of Cloud. The applicability of these standards to all aspects of Cloud would be a subject worthy of further study.

2.6 The Jericho Cloud Cube Model.
The Jericho Forum Cloud Cube Model (2009) from the Open Group [8] gives some further granularity to the NIST models and uses four dimensions to represent the security sensitivities of a cloud deployment:

- **Internal or External** – where is the data located relative to the organization in question – is it physically located inside the organization or outside?

- **Proprietary or Open** – Is the underlying technology standards based? For example the Open VirtualisationFormat (OVF) is a standard intended to offer consistency in virtual machine data, thus offering a degree of portability to the cloud service in question. Closed or proprietary technology limits interoperability and has security implications because it is less easy to apply appropriate scrutiny to such platforms.

- **Perimeterisation** – is the data and application within the bounds of an organisation’s logical IT infrastructure or outside it? Effectively, is it operating in a public or private cloud environment?

- **Insourced/Outsourced** - Who is operating the Cloud service in question? The organisation the model is being applied to or a third party?

**Jericho Cloud Cube Model [8]:**
Figure 2: Jericho Cloud Cube model

The Jericho model still only considers one tier of outsourcing thus could still to be considered to be removed from the real world deployment scenarios.

The Cloud Security Alliance (CSA) is an organisation dedicated to the security of Cloud services and comprises a membership drawn from Cloud practitioners, vendors, users and other interested parties. It is a source of Cloud security education, and produces one of the most comprehensive bodies of knowledge and best practice in the form of its Security Guidance for Critical Areas of Focus in Cloud Computing [9]. As such, this document will partially inform the risk analysis carried out in Chapter 4.

However, since, like many other references on the subject it is based upon the architectural references discussed above from NIST and Jericho. This means that the CSA document also fails to adequately deal with the concept of the cloud supply chain and the potential security risks posed by it.
2.8 Cloud vs Mainframe Computing

Finally, in this section concerning the definition of Cloud, it is perhaps interesting to consider if Cloud computing really is a new concept, or if in fact it has been around since the 1960s in the form of the Mainframe computer, as is claimed by some observers.

Such people would say that the concept of Mainframe computing is in many ways very similar to that which we have discussed for Cloud. Mainframes are centralised devices supplying computing power to large numbers of usually remotely connected users. Mainframes control and have access to large quantities of data storage. They are housed in data centres, just like Cloud servers. They are (or were) often owned and operated by data processing bureaus, akin to CSPs. Finally Mainframe clustering technology (providing multiple processing platforms and failover capabilities) has been available for years. Even virtualisation (a key Cloud technology) was first developed on Mainframe computers.

So in some ways, Cloud Computing does not look like anything new at all. However, the NIST Definition of Cloud Computing and the Essential Characteristics defined within it help us to identify a number of differences that make Cloud a different concept to Mainframe Computing. These are:

- **On Demand Self Service and the ability to self-provision.** This demands a team of systems programmers in a Mainframe environment.
- **Broad Network Access** over standard media (i.e. Internet). In the Mainframe environment access has traditionally been by dumb terminals over proprietary communications media.
- **Resource Pooling** using a multi-tenant model with different resources dynamically assigned and unassigned. Again, in a traditional Mainframe environment this is only realised with a team of systems programmers and operators.
- **Rapid Elasticity** or the ability to scale resource up (or down) quickly and transparently to the end user. In a Cloud environment this is achieved through use of ubiquitous and cheap computing units (servers). In a Mainframe setting this is absolutely not the case – additional computing resource is slow, expensive and complicated to provision.

So it can be seen that the main differences between the traditional mainframe environment and the Cloud environment are based around open standards and ubiquitous availability of resources (communications, processing and Operating systems) plus automatic scaling and provision of services without human intervention.

It can be argued that this has distinct security implications; in the Cloud environment things can be made to happen automatically, in a standardised way, versus in a mainframe environment where most things are locked down and require a (human) gatekeeper. This is worthwhile to keep in mind as we examine in greater detail the most common risks in the Cloud environment. Risk 16, Compromise of Service Engine, on Page 57, is particularly relevant to this.

21
2.9 Detailed Identification of Cloud Components

Drawing on the ‘Essential Characteristics’ introduced in 2.8, it is necessary to give some further granularity around the risks in that could be inherent in these mechanisms.

Figure 3 below is taken from a paper entitled *Understanding Cloud Computing Vulnerabilities* by Grobauer et al. (IEEE, 2013) [10]. It shows in schematic form the various components that make up a cloud solution, including those that are specific to cloud (in green), those that are in supporting IT infrastructure (and might be present whether or not the solution was Cloud based (in brown), and those that are present on the consumer side of the Cloud solution (in blue).

The paper and the diagram are drawn from work done by IBM (*Towards a Unified Ontology of Cloud Computing*, Yousef et al, Grid computing Environments Conference proceedings) 2008 [11] and also clearly shows key components related to self-provisioning, resource pooling and resource elasticity that were defined as part of the NIST definition of Cloud Computing [3] and whose mechanisms and management offer a significant target for Cloud attackers as we will see later on for Risk 16, Compromise of Service Engine on Page 57 and Risk 10, Management Interface Compromise on Page 44.

![Figure 3: Key Cloud Components](image-url)
Chapter 3 Virtualisation and its role in the Cloud

3.1 Introduction to Virtualisation

Virtualisation is the foundation of the modern Cloud environment, and without it, it is debatable if Cloud penetration would be anywhere near as high as it is today. Even if it were, it would undoubtably be much more expensive.

On the face of it, this adds more complexity and with it, risk. However, in this chapter, we shall examine this technology and its supposed vulnerabilities, and argue instead that it has evolved into a mature and well trusted platform.

Virtualisation is the ability to run multiple independent software environments (more specifically operating system environments) on a single server platform. This has allowed users of virtualisation technology to maximise the utilisation of their assets (in the form of servers), by making them available to multiple different tenants, while (in theory) maintaining separation and thus security.

3.1.1 Density of Computing Power and cost effective security

At the same time, modern trends in computer processor and server hardware design provide multiple concurrent CPU 'cores' running on one hardware processor package. Blade servers also package multiple servers (each with multi core processors) into a single data centre rack unit. Together, these allow extremely high density of virtual machines in a given physical environment.

This further boosts the maximisation of assets and minimisation of costs for the CSP, but also has security implications.

There is an argument to say that this extreme density of computing power in one place means it should be possible to apply adequate security controls to that environment more cost effectively than multiple, private distributed environments (i.e. the non-cloud case). The cost of best of breed technology, tools and personnel who have security as their prime focus can be spread over a larger number of users. This equates to cheaper and perhaps therefore more achievable security per unit of processing power than distributed servers maintained on customer premises, by personnel that have security as only one of their job tasks.

On the other hand, an argument against is that the same concentration of computing power could make an attractive prize for determined hacker (or more likely collective of hackers) who have the necessary resources.
3.2 The Hypervisor.

The main software component of the modern server oriented virtualisation environment (virtualisation itself dates back to the era of mainframe computing) is called a Hypervisor.

This was defined in a 1974 paper by researchers in the field of Grid computing, Pokek & Goldberg (‘Formal requirements for Virtualizable Third Generation Architectures’ [12]). In this paper they examined how the Intel x86 architecture (the building block upon which most modern Server and Desktop hardware is based), could implement operating system virtualisation.

They considered the security advantages of a ‘host’ piece of software that performed security-sensitive instructions on a single processor on behalf of multiple guest operating systems – the Hypervisor. They defined the purpose of the Hypervisor as providing "an environment for programs which is essentially identical with the original machine….programs run in this environment show at worst only minor decreases in speed; and….the Hypervisor is in complete control of system resource”

They went on to define two types of Hypervisor; Type 1, the so called ‘bare metal’ type, where the hypervisor runs directly on the server platform’s hardware and then spawns ‘child’ operating system instance(s), and secondly the Type 2 ‘hosted’ Hypervisor which is loaded by a master or hosting Operating System (OS) instance (for example Microsoft Windows) and which can then load and manage one or more ‘child’ client Operating system instances.

From a Security perspective, The Type 1 Hypervisor tends to be a ‘thinner’ and relatively simple hardware abstraction layer, with no need to share folders, printers clipboards or other data between users, or most of the other functionality we require from a modern operating system. As such, and with a smaller number of lines of code, it can be seen that it presents a smaller attack surface to the outside. Also, any vulnerability in the lower software layers potentially presents a vulnerability to the virtual operating systems above; although both the host operating system and the bare metal hypervisors could contain vulnerabilities, it could be argued that there is more chance of a more widely used and distributed ‘fatter’ general purpose host operating system containing vulnerabilities than a thinner, more specialised bare metal hyper visor. It is for these reasons that the majority of virtualisation environments on the market, and used by CSPs are the Type 1 bare metal hypervisor. Examples of type 1 Hypervisors are VMWARE’s ESXi and Microsoft’s Hyper-V.

3.3 Virtual Machine Management.

Another component of the virtual machine environment, the Virtual Machine Monitor (VMM) provides a mechanism to manage the Virtual Machine itself (comprising OS, user data and applications), allowing different types of OS to
be run independently and simultaneously above a single hypervisor, with the ability to start and stop the Virtual Machine (VM) and take 'snapshots' of the Virtual Machine environment (an easy way to backup and archive the VM, or even transition it to a different platform), and perform other management functions. A schematic example of the resulting software stack from VMWARE is depicted in the diagram below (taken from the VMWARE Virtualisation Overview [13]).

![Diagram](image-url)

**Figure 4: VMWARE virtualisation overview**

### 3.4 Evolution of Virtualisation Security Mechanisms

In the early days of Virtualisation on the Intel architecture, every machine-level CPU call that the guest VM attempted to make was interpreted by the Hypervisor, validated according to the context of the state of the VM (thus potentially intercepting privileged and potentially malicious CPU instructions), translated in binary level instructions and executed on the host’s CPU - so called ‘trap and emulate’[14] (A Comparison of Software and Hardware Techniques for x86 64 Virtualisation, Adams & Ageson).

This changed around 2005/2006 when Intel launched its Virtualization Technology extensions (VT-x) and AMD introduced its Secure Virtual Machine architecture (AMD - V). These features allowed the guest VM to access the CPU directly, except where it was trying to execute a privileged instruction at ring 0 of the CPU (with the potential to directly access and manipulate main memory for example) – where again the Hypervisor would interpret the instruction according to context and allow if appropriate (so-called ‘de-privileging’). The primary benefit of this from a security perspective is that it removes complication from the Hypervisor, thus further reduces the attack surface and gives a smaller trusted computing base (Understanding Intel Virtualisation Technology, Sahgal & Rodgers) [15].
Since this time, other processor extensions have been introduced to isolate and remap Direct Memory Access (DMA) and Interrupts to given Virtual Machines (e.g. Intel’s VT-d), and restrict and isolate VMs with respect to other resources such as graphics adapters, network adapters and other PCIe expansion devices. One can contend that the net result some 10 years later is a de-facto standard set of hardware based (and thus harder to compromise) security mechanisms that underpin software virtualisation environments from a number of different vendors. It further can be argued that this is the reason there are relatively few hypervisor or VMM related vulnerabilities listed in the NIST National Vulnerability Database [16].

3.5 Virtual Networking Since the virtual machines are in theory completely separate, their only possibility to communicate with each other is via networks of some kind. Similarly, they will need to communicate with other VMs on other physical servers, the Internet, and other resources such as Storage Area Networks and Printers.

When a VM communicates with another VM residing on the same Hypervisor, it will do so over IP, but instead of doing so over the physical network, it will do so via a virtual LAN, with Virtual Network adapters and Virtual Switches. In operation, these components operate in the same way as their physical counterparts, but it follows that the same rules and security precautions should be followed in terms of implementing organisation policy in virtual firewall rules, segregation of traffic and segregation of duties. This does not always happen (see SANS Institute top-virtualization-security-mistakes-and-avoid-them – Failure to Coordinate Policy between Virtual Machines and Network Connections [17]).

Some Virtualisation Vendors implement IEEE 802.1q VLAN tagging in their Virtual switches – a layer 2 technology that adds a VLAN identifier to the (virtual) Ethernet frame which the switches further down the transmission path will use to segregate traffic at layer 2, for additional security (see Security of the VMWARE vSphere Hypervisor [18])
3.6 Important Security Research in the area of Virtualisation.

The rapid adoption of virtualisation, both in Cloud and other contexts, together with the migration of so many applications and so much data to the Cloud environment has rightly focussed much attention on finding and exploiting significant vulnerabilities associated with the architecture of Virtualisation.

There are two particularly well publicised and debated proof of concept exploits that got a lot of attention in the period between 2005 and 2010, despite the hardware based protection mechanisms that we have described above also becoming available in that period. However, as we shall argue, it is highly debateable if they would be practical real world exploits, or more hypothetical exercises limited to a laboratory setting.

These two proof of concept exploits had different perspectives on the virtualisation paradigm; 'Blue Pill' examined the possibility of the entire virtualised Cloud platform environment on a given server becoming compromised by a malicious hypervisor below, and thus in control of the bona-fide Hypervisor. ‘Cloudburst’ on the other hand was concerned with data within the Virtualised environment leaking out to the hypervisor via a side channel and thus potentially becoming visible by the operator of the Cloud platform.

3.6.1: Blue Pill

was devised by Joanna Rutkowska, who presented a proof of concept to the 2006 Black Hat conference (Is GameOver() Anyone?) [19], where she showed the potential for another hypervisor to be introduced into a system between the hardware and the existing hypervisor, thus with the theoretical potential to silently compromise the environment(s) running above it. (The name Blue Pill was taken from the science fiction film The Matrix, where the hero takes a blue coloured pill to enter an alternate dimension)

Crucially, however, the main assertion was that the malicious hypervisor could be undetectable by anti-malware measures. Rutkowska demonstrated that most of the available side channel detection methods that could be used to reveal the presence of a rogue hypervisor could be subverted.

For instance, methods to monitor the timing of processor instructions to see if the indicated time gaps were too big, (thus revealing the possibility of the processor performing other tasks in the meantime), were not fine grained enough.

She also demonstrated that processor instruction counters could be manipulated easily to disguise the ‘extra’ instruction counts from the malicious hypervisor.

These assertions have since been hotly contested, with a preponderance of evidence suggesting that although in theory the Blue Pill exploit was possible, a Hypervisor that was actually active and performing some kind
of active monitoring (as opposed to an idle hypervisor just there to prove a point) would create sufficient noise to be detected. Among other places, this has been documented in a paper documenting a number of other ways to detect a rogue hypervisor, by a team including a then senior VMWARE engineer, *Compatibility is Not Transparency: VMM Detection Myths and Realities* (Garfinkel et al.) [20]

Additionally, since this time, UEFI (Unified Extensible Framework Interface) hardware BIOS (basic input output system) has been developed. This allows a tighter coupling of the software hypervisor to the hardware before the OS boot phase, making it harder for an additional malicious software ‘shim’ to be placed between the legitimate hypervisor and the hardware.

This is described the paper by Don Bailey ‘UEFI Hypervisors: Winning the Race to Bare Metal White Paper’ [21]

### 3.6.2 Cloudburst

Cloudburst was presented to the 2009 Blackhat Conference by Kostya Kortchinsky (*CLOUDBURST: A VMWARE A Guest to Host Escape Story*) [22].

This examined the possibility that the virtual memory space mapping of a virtual device driver contained in a virtual machine (each VM guest operating system refers to virtual device drivers that virtualise and thus share the real hardware interfacing drivers among other VMs) could be reversed and read at the hypervisor level.

This would then theoretically allow an individual with the requisite access to the hypervisor (an administrator of a CSP for example) to read data buffers in the CSP customer’s VM.

The concrete example of the vulnerability given by Kortchinsky was that of a video driver. However, it relied on a bug within a VMWARE virtual video driver (which was subsequently patched), to perform the exploit. Thus it can be argued that this was really an exploit linked to a particular software vulnerability, just like any other (that could be found in an operating system for example), as opposed to a new way of exploiting virtualisation *per se*.

The particular video driver used in Kortchinsky’s proof of concept was a 3D video driver, and furthermore Kortchinsky made the point that it should be questioned why a 3D video driver should be necessary anyway in a virtualised environment. Normally such an activity would be better performed on a dedicated gaming, or graphics design workstation environment for performance reasons. This underlines the importance of the same Saltzer & Schroeder (*The Protection of information in Computer Systems*, 1975) [23] design principle of economy of mechanism, that we saw the CPU hardware vendors above, apply to the area of virtualisation.
Although these two famous exploits on Virtualisation technologies could ultimately be argued to be of little real world consequence in the current virtualisation state of the art, a case can be made to say that their scrutiny has raised awareness of the potential risks, possibly also contributed to new technological safeguards such as UEFI BIOS, and re-affirmation that traditional principles of security design are applicable more than ever. As such, they have contributed to the maturity and security of virtualisation as a technology.
Chapter 4 An analysis of Cloud based risks

4.1 Objectives and Methodology.

In the following pages we shall analyse the risks faced by the prospective Cloud Service customer.

The end objective of this work is to determine which risks can be satisfactorily mitigated, which cannot, and the degrees in between. In short, it is hoped to answer a question for those at management level of any organisation considering outsource to the Cloud: what risks can they take steps to avoid and what is likely to remain a potential danger that they may have to accept?

This part of the study seeks to add value to this study via a detailed discussion of each risk, plus proposal and consideration of available mitigations.

The impact and probability of each risk are then re-evaluated compared to the source literature that identified the risk, assuming the mitigations discussed have been applied. In this way it is hoped to show what risks remain problematical, and which can be treated.

My analysis of how effectively these risks can be treated and the implications that may remain is based on application of the knowledge gained during my period of study on the Royal Holloway Information Security MSc, plus twenty years of experience working in the Information Technology sector, and is informed by the literature sources as noted in text.

4.2 Summary results:
A high level graphical representation of the results, depicting mitigated risks in terms of impact and probability is depicted in Figure 6 on page 70, at the end of this chapter.
4.3 Source Literature

There are a number of studies detailing lists of risks applicable to the Cloud, but not necessarily their mitigations. It is not proposed to re-invent such a list of risks but rather to draw upon and analyse what already exists and use this for further analysis.

One of the most detailed statistical analyses of reported Cloud service breaches - *Cloud Computing Vulnerability Incidents* [24] - was carried out by the CSA in 2012. In this study, 11,491 news articles on cloud computing-related outages from 39 news sources between Jan 2008 and Feb 2012 were reviewed to produce a frequency based analysis of relevant security breaches.

When the CSA revisited this subject in 2013, they took a different approach with *The Notorious Nine: Cloud Computing Top Threats in 2013* [25]. Instead of being a statistical study, it sets forth a consensus view from a panel of industry experts on what they felt were the most important risks for Cloud. Thus, as well as an idea of frequency, this gives a better idea of the impact of such events. Other relevant references from CSA, particularly on best practice and governance, is detailed in *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0* [26] and ‘SecaaS Implementation Guidance’ [27].

Gartner has produced research on the subject in 2008 in the form of *Assessing the Security Risks of Cloud Computing* [28] (which was also neatly summarised in the Network World article from 2008: *Gartner: Seven Cloud Computing Security Risks* [29]).

In 2009 the European Network and Information Security Agency (ENISA) produced the report *Cloud Computing: Benefits, Risks and Recommendations for Information Security* [30]. This is drawn from previous CSA and Gartner work and also shows a consensus with the rest of the material mentioned above. We shall therefore use this as a list of applicable risks that we shall discuss and expand upon in this chapter.

Note that ENISA does not propose mitigations for the risks listed in its report. With each risk, they note a non-mitigated risk probability and impact (noted below as ENISA risk rating). For each of the risks detailed I then propose possible mitigations and then re-evaluate the probability and impact of the risk (noted as Mitigated risk rating).
4.3 Policy & Organisational Risks

Risk 1: Provider Lock In

ENISA risk rating: probability HIGH, impact MEDIUM
Mitigated risk rating: probability HIGH, impact MEDIUM

**SUMMARY:** This is risk is greater for SaaS customers. Also, unless the Cloud customer is an organisation with a great deal of buying power, and thus in a position to force a negotiated contract with the provider, it is difficult to mitigate this risk.

Provider Lock In refers to a situation where a Cloud service user is for some reason bound to the CSP they are using. It can be argued the real rating of this risk is quite different, depending on the type of service in question. As we have discussed in Chapter 1, IaaS and PaaS can be viewed a more of a commodity type of service, with many players offering a similar service to the market. The classic example of this would be AWS, or Rackspace, or any number of similar services offering basically the same type of service. In this commodity situation, it can be argued that is relatively easy for a User to switch from one service to another. However, with SaaS, such as a CRM solution for example, the CSP is providing more value add, and the user will have integrated their business processes more tightly with the service which makes a switch from one provider to another much more costly.

In PaaS and IaaS scenarios, the deliverable to the Cloud customer will almost always be commodity based and (de facto) standards led - for example, a Windows Server or Linux operating system environment. What the customer may run on top of this is under their control and thus not really a function of the Cloud. In this case one can argue that swapping one provider of such a computing environment for another should be a relatively trivial exercise.

A key concern with lock in is availability of data; if the customer decides to move provider, how long will they have to migrate data and meta data before the original CSP deletes it?

A CSP will also usually set a minimum contract term, creating a mandatory lock in.

Other consequences of Lock in are that the User will be more exposed to changes in service levels or commercial terms.
Mitigations

- Use of standard, off the shelf products. If a CSP deliverable is based on commodity products, as described above, the choice of providers offering such a service is considerably widened. This should give the user the ability to switch provider with relative ease.

An example of the advantages that Standards can bring in this area is Open Virtual Machine Format (OVF). This is a standard developed among vendors of Virtual Machine Managers (VMM) or Hypervisors that allows a Virtual Machine environment to be portable and usable on different types of VMM. This would allow the customer to transparently take an entire (and easily backed up) Virtual Machine environment from one CSP running one type of VMM (VMWARE for example) to another CSP running XEN (for example).

The motivations behind OVF and the functionality of the standard are described in The Open Virtual Machine Format Whitepaper for OVF Specification published by VMWARE and XENSource [31]. OVF started as a vendor lead consortium but has since been adopted and published as an ISO standard 17203:2011[32] and can thus be a useful benchmark on which to compare CSPs.

- Dual sourcing from two CSPs is unlikely to be a realistic mitigation; the cost overhead of maintaining two providers will likely negate the cost efficiencies of Cloud.

- Legal Risk Management can be used to reduce the amount of upheaval in changing providers. This means a contractually agreed right to extraction of data, and possibly help to transition to a new provider. However, often, especially in a commodity situation where a provider services many customers, and the business model is based on high numbers of tenants paying relatively low price, it is not possible to individually negotiate contracts, and the default model is a ‘click to accept’ standard terms and conditions. The prospective customer should at least review such contract for terms that would lead to lock in, such as onerously long agreement duration or unassured access to data, which would limit the opportunities for a user to switch providers.
Risk 2: Loss of Governance/Compliance Challenges


SUMMARY OF ANALYSIS: It is increasingly possible to find CSPs that have already been audited to relevant standards to increase assurance of governance, or that will allow audit to take place. However, contractual penalties around breach of standards are worth very little to the Cloud Service customer.

If we take Governance as meaning the application of a set of rules to an activity, in engaging a CSP and outsourcing the activity to them, it is certain that we are transferring the act of governance to them.

Whilst we might be sure about the set of rules that should be applied to the activity we are not necessarily sure that the CSP is actually applying those rules, perhaps until it is too late. This will have an effect in almost all imaginable situations, even if we are just using the CSP as cloud storage (knowing where our data is really stored for example) or as an email service (are emails retained for a relevant period of time for example).

The impact of non-compliance can also increase greatly, depending on the type of activity the Cloud User is engaged in. For example, in the Financial Services area, the consequences of not adhering to the required standards, procedures and set of rules can be extreme, to the extent of punitive fines or even exclusion from the activity in question.

Gartner’s Assessing the Security Risks of Cloud Computing [28], summarised in Network World as Seven Cloud Computing Security Risks [29] also makes the point that “customers are ultimately responsible for the security and integrity of their own data” The Cloud provider may be in control, but the Cloud Service user is still responsible. For example, under the UK Data Protection Act 1988 [33], the user is still the Data Controller and thus liable for breaches of it’s code.

To summarise in the problem in one sentence, it is possible to outsource most things, but it is very difficult to outsource responsibility.

Mitigations proposed as a result of this study:

- Standards are probably the most effective way in which to ensure the relevant governance is applied. However, still the problem is knowing if the CSP is actually doing this or not, before it is too late. Ongoing audit can help in this.

This can be accomplished in one of two ways, either that the CSP will certify itself against a given reference standard (for example ISO 27001
or that the customer, or the customer’s agent will perform an audit upon the CSPs operations.

There is a case to say that the former method may well be possible as CSPs recognise the potential to differentiate from their competition and thus increase their business.

This will however usually apply only to CSPs of a certain size (with a customer base big enough to finance such compliance activity) or if the CSP aims to specialise in a certain area (e.g. ecommerce where a high proportion of its potential customers might see a benefit in PCI-DSS compliance).

However, it is arguable that the second method whereby the customer certifies the CSP is not likely to be feasible unless the prospective customer represents a sizeable enough proportion of the CSPs business to justify the activity. If this is not the case, the CSP is unlikely to agree to such individual audits because this is not a scalable way in which to run a business, or because they wish to hide the details of their business for some reason.

- Legal Due Diligence. A way to increase the chances that a CSP will comply to governance is the imposition of contractual penalties that will have a financial impact on the CSP if they prove to be in breach of relevant controls. This is something that can be built into bespoke contracts, but as discussed above is unlikely to be possible for commodity CSP business with the ‘click to accept’ model.

Moreover, a study undertaken by Kuan Hon et al. documented in *Negotiating cloud Contracts: Looking at Clouds from Both sides Now* and published by the Stanford Technology Law Review [35] found that in a study of the individually negotiated Cloud contracts entered into by a sample of 20 representative organisations, most common practice is that the maximum penalty that could be levied by the user on the provider for such breaches would only be some proportion of the fees dues from customer to provider (Page 93), thus bearing no relation to what the real costs of a any such breach may have been. In summary, you may be in a position to mandate a contractual penalty, but in evidence shows that is unlikely to be of much value, should it be needed.

- Voluntary Governance. Some CSPs sign up to voluntary codes of practice, such as the *Cloud Industry Forum Code of Practice* [36] or CSA STAR Registry [37] and this can give a certain level of reassurance regarding the standards to which a CSP would like to be seen to be conformant. However, these are voluntary bodies relying in many cases on self-assessment by their CSP members and it could be argued that there are weaknesses in this model. For example, is there sufficient end user representation in such bodies? What conclusions can be drawn about members who have chosen not to join, or been denied membership?
Certainly, past experience from other sectors does not give a good level of confidence around the legitimacy of such voluntary governance. There are many examples from the financial services industry, or the press and media where self-governance has resulted in opaque rules written and enforced more for the benefit of the members of the body in question rather than third parties wishing to receive assurance. For further on this, see also Risk 6, *Cloud Supply Chain Failures*. 
Risk 3: Loss of Business Reputation Due to co-tenant activities

ENISA risk rating: LOW probability and HIGH impact.
Mitigated risk rating: LOW probability HIGH impact.

**SUMMARY OF ANALYSIS:** There is little that can be done by the Cloud User to mitigate against this risk. Such incidences are rare, but have occurred and resulted in total loss of service.

The most obvious and high impact cause of this would be where a law enforcement agency (LEA) might have reason to investigate a cloud service co-tenant and for forensic purposes obtains a warrant to remove or shutdown necessary infrastructure.

This means service would be denied to the legitimate tenant of the service, and this example is indeed given by ENISA and also cited by other books on the subject (for instance the *Computer and Information Security Handbook*, Vacca J, published by Morgan Kaufmann [38]. However, it is actually quite difficult to find a straightforward example of an entire cloud service being suspended due to the illegal activity of a single tenant, with subsequent shutdown of an entire Service by an LEA.

This may be because one of the issues with Cloud Forensics is the tension between investigating and preserving a crime scene, balanced against reduction of disruption to other service users and the fact that any warrant issued to authorise this will take account that disruption to others, or that other tenants will have already disrupted the crime scene (data on disk or in computer memory for example). Also, there are plenty of ways for the CSP to take down a malicious or suspect cloud tenant and isolate a portion of their data (VM snapshot for example) without taking down an entire service.

A more real possibility would be that of a third party attacker mounting a malicious exploit upon a co-tenant that they wish to target for some reason, which then disrupts otherwise unconnected tenants on the same CSP. This could come in almost any of the forms we will discuss later (see risk 13 on Page 57) such as (distributed) denial of service (DDOS), hypervisor attacks, physical security attacks and so forth.

A well-known example of this would be the case of Smirnow and Surmacki, a pair of Polish cyber criminals who launched a DDOS exploit on British online gambling site but which also disrupted the availability of service for an unnamed and un-connected co-tenant (who later helped in a sting operation to arrest Smirnow and Surmacki) See Casino DDOS duo caged for five years after blackmail buyout threat, The Register 19/12/13 [39]

This risk is partly related to vulnerabilities arising from the use of the shared platform itself due to technological issues around virtualisation. However, as we discussed in Chapter 3, whilst possible, virtualisation technology is mature, widely reviewed, and despite a number of theoretical exploits, seldom seen in the wild. See also risk 8, Isolation Failure.
Mitigations proposed as a result of this study:

- The only sure way to mitigate this kind of risk is to be the only tenant on a cloud service, or where all tenants are known or linked to each other in some way (private/semi private cloud).

However, in many ways, this defeats the object of the cloud - that asset use is being maximised over a large number of participants. Thus especially for many smaller to mid-size cloud customers, is unlikely to be their chosen model.

It can be argued that it is difficult to prevent exposure to this kind of risk because it is unlikely that identities of fellow cloud tenants will be known in full because of commercial confidentiality. In this case, it is impossible to make a judgement about what co-tenant an organisation would consider to be an unacceptable risk. Plus, even knowing the identities of other tenants does not necessarily enable a sound judgement; Size is no indicator - the growing trend of commoditisation in cybercrime means that criminals are seeking a growing volume of smaller targets to grow their revenues and so it is difficult based on this to make a judgement about whom would be a risky co-tenant.
Risk 4: Cloud Service Termination or Failure

ENISA risk rating: unspecified probability and VERY HIGH impact.
Mitigated risk rating: LOW Probability, VERY HIGH impact

**SUMMARY OF ANALYSIS:** With some due diligence around selection of a provider (customer count, financial status, years of service), it is not difficult to reduce the probability of this risk occurring. Similar precautions to risk 1 (provider lock in) can be taken to reduce impact if it does occur.

This risk refers to the possibility of a cloud user’s CSP going out of business, either for reasons of strategic withdrawal or because the Service is no longer viable from a commercial perspective. It can be said that this is a significant risk because of the maturity of the cloud market, and the low barriers to entry.

Mainstream Cloud usage is in some ways a relatively recent phenomenon that has obvious and immediate appeal. Every company’s board of Directors is asking their IT department what their strategy is with respect to Cloud, and every IT vendor’s marketing department feels their product must somehow be able to show some kind of ‘Cloud enablement’ unless they are to be overlooked in favour of their competitors who have already got there.

Additionally, Cloud is a relatively easy business to enter using someone else’s PaaS building blocks and this gives the potential for new CSP entrants to create new cloud services on a tenuous business model that they can deploy easily to test the market and see if there are commercial returns.

The end result of this can lead to a ‘here today, gone tomorrow’ syndrome, with the prospective Cloud Service user in potentially disastrous situation. In the case of a complete business failure of the CSP (as opposed to a strategic withdrawal), the CSP could go bankrupt overnight and be obliged to cease service with no warning to Customers and no chance to remove vital data from the cloud.

**SIDE NOTE:**

For a related example of how CSP business models may not always be focussed on the service customer, see the recent announcement of a trial by the Dutch energy utility Eneco, to deploy Cloud Servers in people’s homes as heating appliances - [http://news.eneco.com/heat-your-home-for-free-with-heating-provided-by-a-computer-server](http://news.eneco.com/heat-your-home-for-free-with-heating-provided-by-a-computer-server) [40]. While this may be interesting from an energy conservation perspective, the data security aspects for the service users are surely questionable.
Mitigations proposed as a result of this study:

- **Due Diligence in Procurement.** As part of a prospective User’s procurement process, they should evaluate a number of cloud providers that are able to fulfil the requirements of the desired service. These shortlisted providers should be ranked on basis of longevity of service, financial construction and backing, so that an informed choice can be made which minimises this risk.

- **Legal Risk Management.** An appropriate contract with the prospective Service provider can lessen the risk involved. Financial penalties imposed if a provider voluntarily withdraws a service, or some form of bond agreed in advance may mitigate the risks of a provider entering bankruptcy proceedings. However, as we have already discussed for Risk 2 on page 37, the likelihood of a provider agreeing to anything much more than the value of the service fees involved is low [35]
Risk 5: Cloud Provider Acquisition

ENISA risk rating: unspecified probability, MEDIUM impact
Mitigated risk rating: MEDIUM probability, LOW impact.

**SUMMARY OF ANALYSIS:** *Due diligence in provider selection can reduce the probability of this risk. If it does happen, the acquiring party has an interest to retain the customer base it has acquired, thus is unlikely to alienate its customers.*

The drivers behind this risk are similar to those for Risk 4 on page 40, Cloud Service Termination or Failure. Namely, an immature market with many new entrants, low barriers to entry and resulting unproven business cases leading to a high degree of churn among providers.

In this case, however, it can be argued that the failing (or leaving) entrant may be attractive to another CSP (to add customer base, broaden an offering, add assets and so forth). Thus there is an acquisition, and the Customer can find themselves contracted to a new provider without much warning.

The potential consequences of this may be that the new provider may try to impose different terms and conditions, service levels, prices or many other factors upon the customer. Other factors could introduce unfavourable organisational changes on the Customer; consider a situation where the contracted CSP is acquired by the competitor of the customer – this could lead to unacceptable commercial risks and a situation where the customer is forced to find a new provider.

**Mitigations proposed as a result of this study:**

- **Legal Risk Management** It can be extremely difficult to predict the probability of an acquisition when entering into an agreement so once again an appropriate contract entered into before doing business with the prospective Service provider can lessen the risk involved after the fact of an acquisition. The prospective customer should look for the ability to terminate a contract immediately and without penalty on such acquisition if it so chooses. Alternatively, a clause which ensures that all terms and conditions would stay the same if ownership of the provider were to change would give some level of continuity of service, perhaps while the customer seeks a new provider. This may only be possible if a contract is negotiated as opposed to the more common ‘click to accept’ contract found on lower end services.
Risk 6: Cloud Supply Chain Failure

ENISA risk rating: LOW probability and MEDIUM impact
Mitigated risk rating: MEDIUM probability and HIGH impact

**SUMMARY OF ANALYSIS:** The customer has no visibility or control below the level at which they have some kind of contract. Therefore there is little or no mitigation the customer can apply, and the impact can be total with each level acts as a multiplier of risk.

The ENISA scoping of this risk only looks at one aspect - the possibility that a CSP will outsource a small part of its service to a sub-contractor, such as identity management or single sign on.

In reality, as we have argued in Chapter 2, section 2.3 on page 14, the actual level of outsourcing that takes place in the Cloud environment is far more significant – increasingly an entire given service is hosted on top of a PaaS or IaaS from another supplier.

While this may not be a problem if the platform supplier is transparent and stable, this may be far more significant if

- there is no visibility of the outsourcing to the Cloud User
- there are no details available about that platform with which to make a judgment about its Security attributes,
- the CSP’s supplier(s) or their practices change on a regular basis potentially leaving the User exposed to risks with no visibility and thus no opportunity to mitigate.

This risk is highly dependent upon trust in the top level CSP to be applying the necessary due diligence to their outsourced provider.

**Mitigations proposed as a result of this study:**

- It can be argued that if a sub-contractor confirms to a given Information Security standard such as ISO 27001 or PCI-DSS, then the top level supplier will take this level of conformance through to its activities.

- **ITU-T X.1500** defines a Cyber Security Information Exchange Framework (CYBEX) [41] through which transparent auditing to a common cloud standard can be achieved. However, it is difficult to find a CSP that advertises conformance to this scheme.

- The CSA Security, Trust and Assurance Register (STAR), [37] assesses and publishes the security measures of CSPs based on a 300 item questionnaire that normalises the security controls defined in a number of standards including ISO 27001, PCI-DSS, NIST, European Data Protection Directive and more, enabling a prospective user to see flow through and equivalence of controls between CSPs that may be in sub contractual relationships.
While the number of participants to the CSA STAR scheme is reasonably large and growing, most of the registered CSPs on the scheme have opted to do this on a self-assessment basis – so it can be argued that it is not necessarily an independent view of a participants security measures.
4.4 Technical Risks

Risk 7: Resource Exhaustion

ENISA risk rating: MEDIUM probability, MEDIUM Impact. Mitigated risk rating: MEDIUM probability, MEDIUM impact.

**SUMMARY OF ANALYSIS:** The user has little visibility of the thresholds and even less control. This means therefore relying on the CSP to stick to their SLAs and enforce the relevant controls. There are thus few mitigations available to the service user, but on the other hand the main impact should be limited to consumption of additional resources as opposed to existing operation.

This risk refers to the possibility that the Service level to the User is degraded through the exhaustion of resources of the CSP’s compute platform; these could be memory (RAM or secondary storage), processor cycles or other resource units that are somehow used as part of the service.

At its most simple this relies on a scoping process within the CSP to ensure that they have sufficient resources to be able to maintain the SLA that they extend to their customers. This process will probably rely on some kind of capacity planning mechanism on the part of the CSP.

At its most complex, as defined in the *NIST Cloud Computing Definition* (see Chapter 2, page 10) [3], the notions of elasticity and dynamic provisioning add a layer of mechanisms to achieve this that can be the target of attack. See also figure 3 page 22

See also risk 13 page 57, concerning economic denial of service (EDoS).

**Mitigations proposed as a result of this study**

- The CSP should have a capacity planning and resource provisioning process that monitors current and anticipated Customer demand and facilitates additional resources in appropriate timeframe to maintain the SLAs

- The CSP should have a mechanism to limit new subscriptions being permitted as the threshold of resource exhaustion approaches. This should include not only denial of new Service customers but also of existing customers increasing their resource utilisation outside of the SLA (by deploying additional Virtual Machine instances for example)

- The CSP should provide a real time reporting mechanism to the customer that provides a dashboard (e.g *AWS CloudWatch* [42]), such that they can themselves monitor resource utilisation on the platform to ensure it stays within SLA. In practice, however, it is questionable if a CSP would allow a
Customer to monitor the usage levels of the entire platform, on the basis of commercial confidentiality, privacy and security of the entire platform.
Risk 8: Isolation Failure

ENISA risk rating: LOW probability and VERY HIGH impact. 
Mitigated risk rating: LOW probability and HIGH impact

**SUMMARY OF ANALYSIS:** *The technology in question is mature and well proven. Certifications (e.g Common Criteria) apply. Standards based controls and policies can be implemented around operation and configuration. However, if breach does apply, impact can be high and not necessarily visible.*

Isolation failure (also known as VM hopping) is the breach of secure boundaries between tenants in a Cloud Service setting, leading to information leakage. One of the key vulnerabilities that could lead to this would be the compromise of Virtual machine environment which we have examined Chapter 3. It was argued that Virtualisation is now a mature technology, underpinned by trusted hardware functionality that reduces the attack surface. Hotly debated theoretical exploits have been devised, but in practice there are few identified vulnerabilities in this technology.

On the other hand, one of the issues with such isolation failure would be knowing if such a breach had occurred. Because such a breach between Virtual Machines would necessarily be at a low level, it would likely be below logging mechanisms, so there would be no incriminating audit trail. Forensic investigations would be hampered by the fact that there would be ‘noise’ from the activities of other tenants that may make it difficult to establish a chain of evidence.

A more likely source of Isolation failure and resulting information leakage would be compromise of Network interfaces between clients, as a result of lack of related policy (in the form of (virtual) firewall rules for example), or bad implementation of that policy. However, it could be said that this vulnerability could also be present in a non-cloud scenario, so could not really be said to be Cloud related *per se.* (Although it may be easier for a fellow cloud tenant to gather information such as IP address ranges or authentication procedures in order to perpetrate such a hack)

An advantage of Virtual Machines we have already discussed is the flexibility in creation, stopping, starting or transferring a VM to another platform. However, one can argue that this also represents a vulnerability. Its relatively convenient to ‘steal’ an entire VM image if you have the right access, and with it goes the entire operating environment which an attacker can then attempt to penetrate at their leisure in a sandbox environment. Obsolete VMs can pose a security risk if they are not securely destroyed. Also, since its easy to stop, start and archive a VM, there is a potential version control issue with anti-virus (AV) measures - a VM could have been archived for a period of time during which the AV measures become outdated – the first job on restart should be update of those AV measures.
Mitigations proposed as a result of this study

- Knowing what kind of virtualisation technology is in use by a prospective CSP can help a customer to judge a risk they may face from isolation failure due to virtual machine compromise. For example, type 1 bare metal hypervisors offer a smaller attack surface.

Vendors of virtualisation technology are increasingly undergoing independent certifications to illustrate their level of security for a given situation.

For instance Common Criteria for Information Technology Security Evaluation (Common Criteria) offer a widely recognised, independent framework for measuring the security of a given product for a given usage scenario (known as Terms of Evaluation or ToE). Evaluation Level 4+ (EAL4+) indicates ‘Methodically Designed, Tested and Reviewed’ for a given ToE, is appropriate to Operating systems (if not specifically Hypervisors) and is a certification level held by a number of Virtualisation Vendors.

More information about specifically what is evaluated in regards to this can be found in Common Criteria Protection Profile BSI-CC-PP-0067 [43]

- Visibility of the CSP’s policy with regard to network traffic restriction and how it is implemented in terms of rules at physical and virtual levels to see if there is any delta between it and the policies of the prospective customers own organisation should give an indication of there is additional risk of isolation failure.

- The CSP should have a strict policy concerning the archiving and re-commissioning of VMs. This should be implemented such that they are securely stored (possibly encrypted for additional security), integrity checked (including AV versioning) when re-commissioned, and securely deleted when no longer required. VMs should be stored securely - or an attacker could compromise a VM which then acts as a Trojan horse to attack other VMs on the same Hypervisor.
Risk 9: Cloud Provider Malicious Insider

ENISA risk rating: probability MEDIUM impact VERY HIGH.
Mitigated risk rating: probability MEDIUM, impact VERY HIGH.

**SUMMARY OF ANALYSIS:** There are a number of policies and tools the CSP can apply to reduce this risk, in handling of personnel, visibility of operations and opportunity to do harm. It can also be argued that number of personnel required per unit of computing is much less in the cloud than the traditional environment, thus the probability of occurrence is lower.

The concept of the insider threat is not by any means exclusive to the Cloud. However, the concentration of computing resources and data potentially available through a single access point, the added level of anonymity compared to the service user and the difficulty in establishing a forensic chain of evidence in the Cloud context make this a potentially rich picking ground for individuals or groups of individuals with the will to exploit this situation.

As we have also touched upon before in chapter 2 section 2.3, the Cloud Supply Chain adds further layers of opacity and ease with which a perpetrator can distance themselves from their victims.

Bishop and Gates (*Defining the Insider threat*, 2008 [44]) defined an insider based on "violation of a security policy using legitimate access and violation of an access control policy by obtaining unauthorized access". Thus, "an individual who is a present of former member of an organization, employee, contractor, partner, vendor or integrator, consultant and auditor who is trusted, who formerly has knowledge, credentials and granted with legitimate access and privileges to organization information systems and services in order to execute organization and business tasks" (*Analysis of Insiders Attack Mitigation Strategies*, Zulkifli & Abawajy 2013 [45]).

**Mitigations proposed as a result of this study**

- By definition this risk category is people related and requires a level of trust in those people working within the CSP. The question is, how and why we should trust in those individuals. This starts in the CSPs hiring process in ensuring they hire appropriate people with a proven track record and history. One way to do this would be with background checks. A prospective Cloud Service customer should satisfy themselves that the CSP does appropriate checks to a relevant level of detail. References are an unreliable way of verifying and individuals background, partly because they are not necessarily objective, but also because there is an increasing trend for organisations to maintain a policy of not giving references for previous employees in order to remove the risk of potential future litigation by the individual’s new employer.
- Suitability checks cannot be 100% reliable for all kinds of reasons including that an individual’s motivation to carry out a malicious act could change over time and circumstance, therefore other ways to prevent malicious acts must be found. These include allocation of least privilege.
such that an individual only has minimum powers needed in order to carry out their job, Separation of duties such that two or more individuals effectively carry out relative checks and balances, and maybe even a two man rule where input from multiple individuals may be need to accomplish a given, sensitive task.

SIDE NOTE
Though not necessarily Cloud related it is debateable if data loss incidents such as the Snowden and Manning revelations would have occurred if a two man rule had been applied to accessing the material leaked by those two individuals.

- Data Loss Prevention and Detection tools may act as a deterrent to Malicious Insiders if the CSP chooses to invest in them. Similarly, a high and visible degree of general event logging and auditability (and crucially the monitoring of such logs) may reduce an individual’s susceptibility to commit such crime.

- Situational Crime Prevention methods have been proposed (Overcoming the Insider: Reducing Employee computer crime through Situational Crime Prevention, Willison & Siponen [46]) which focus on reducing the likelihood of such crime by using controls that increase the effort needed to commit the crime, the risk involved, remove excuses and reduce provocation

  A CSP that can show they have spent time analysing their risks and implementing such controls could be said to engender more trust from a prospective customer than one who has not.

- The principle of Attack Trees (Schneier) [47], can be used to assign a metric to the various steps involved in an exploit according to effort, difficulty and cost needed to perpetrate it. This offers a tool to guide a CSP on where they should spend money and effort on appropriate defences. Such analysis can also help to engender trust in the CSP.

- Logs and reports from intrusion detection tools can provide a visible assurance to the Cloud customer that appropriate steps are taken to minimise this risk.
Risk 10: Management Interface Compromise

ENISA risk rating: MEDIUM probability and VERY HIGH impact. Mitigated risk rating: MEDIUM probability, VERY HIGH impact.

**SUMMARY OF ANALYSIS:** By definition, if an attacker can breach the management interface, they can do almost any kind of damage. However, the CSP and the customer have many possibilities to reduce the risk, primarily via strong authentication, and adherence to secure software design principles.

One of the attractions of the delivery mechanism of Cloud Services is the ability for the customer to self-provision and manage resources at will. It allows the CSP to serve the customer at any time without any front line investment in human resources and thereby reduces their costs. To do this requires some form of management application and user interface.

Such interfaces (see also figure 5 below) give the ability to start, stop, create, delete, snapshot, transfer and any number of other VM related functions, mostly from an easy to use, web based graphical user interface (see the AWS management console diagram below [48]. As well as being offered in traditional PC browser based format, they are offered as mobile device apps for smartphones and tablets. They sometimes have application programming interfaces that enable an administrator to give a subset of the functionality to users, controlled through other programs. In short, a very sophisticated and powerful set of tools, that from a security perspective, offer a massive attack surface to a malicious actor with the necessary skills and intent. Clearly, once an attacker has control of the management console, they can do anything.

![Figure 5: Amazon Web Services Management Console](image-url)
Such rich functionality seems to flies in the face of security best practice in terms of economy of mechanism. However, such features are a competitive differentiator, especially among IaaS and PaaS providers, undeniably useful for the customer and it can thus be said that they are a fact of life for the security manager.

Key vulnerabilities are likely to be browser based issues, protection of data in transit, certificate misuse, and insecure APIs.

In the paper All your Clouds are Belong to us - Security Analysis of Cloud Management Interfaces by Somorovsky et al (2011) [49] the authors describe exploits allowing them to theoretically compromise the VMs of the customers of popular IaaS services including AWS. These exploits were cross site scripting, where it would be possible to steal and re-use console authentication data, and XML signature wrapping – where bogus XML messages used in the console to control aspects of the customer’s environment could be passed off as authentic by using a signature from a previously passed genuine message. These are perhaps old vulnerabilities and probably now fixed, but this serves to illustrate to scope for such issues. As discussed in Chapter One, the number of high profile services that run on such IaaS platforms illustrates how this has the potential to affect the privacy and compromise the data of vast numbers of people.

Mitigations proposed as a result of this study

- CSPs should design management applications to adhere to software design best practice according to the Salzer & Schroeder software design principles [31] of least privilege, segregation of duties, defence in depth, fail safe, economy of mechanism, complete mediation, open design, least common mechanism and identification of weakest link.

- Protection of data in transit, e.g with SSL encryption and authentication

- Strong access controls should be implemented such as the safeguards detailed in the AWS Identity and Access Management Guide [50] These include:
  - Use of signature keys (with appropriate management) for console access
  - Strong passwords (with rotation rules applied)
  - Multi factor authentication (something you have as well as something you know. Such as tokens, biometrics, out of band mechanisms e.g access codes sent by text message etc) are widely supported by CSPs

- Logging, to detect and record access attempts

- Appropriate user ID management (least privilege enforced, deletion of un-needed IDs, IDs not shared, and enforcement of an appropriate user access policy mandated by the Cloud Service user’s Information Security Management System.
Risk 11: Intercepting Data In Transit

ENISA risk rating MEDIUM probability and HIGH impact.
Mitigated risk rating: LOW probability and HIGH impact

**SUMMARY OF ANALYSIS:** Well proven technologies (SSL, IPSec) exist to reduce the risk to acceptable levels, when implemented properly.

Data transfer in the Cloud environment can be split into two different types; that between the CSP and the client, and that within the CSP infrastructure itself (bearing in mind the CSP infrastructure could be geographically distributed, or as discussed before, part of a supply chain ecosystem with multiple underlying providers).

Traffic to Cloud clients is mostly web based, over the Internet – to give the benefits of universal device access (including mobile devices), with no need for proprietary client software. Such web based access of data in transit is usually protected with SSL. This gives Confidentiality and Data Origin Authentication through encryption, and Entity Authentication through digitally signed certificates.

This is the same technology we trust in our everyday life on the Internet (home shopping, home banking and so forth), and is widely and successfully deployed. We also know that this is not completely impregnable (at least from a theoretical point of view), but it can be argued that it can be deemed 'good enough' as long as relevant precautions are taken (see mitigations).

Arguably the biggest commercial risk with SSL based security are the digital Certificates used to provide entity authentication. The Certificate is digitally signed and uses a third party Certificate Authority (CA) to underwrite the identity of the signer.

Such a certificate can be forged, and the chain of trust back to the Certificate Authority can be tenuous to say the least. Arguably the biggest red flag here is that the maximum liability that the CA can be held to in such a failure can be legitimately limited (see European Electronic Signatures Directive 1999/93/EC Article 6) [51]. This means monetary damages can be as little as the value of the service provided by the CA which could easily be disproportionate to the value of the data traffic that a Cloud Service User could be transiting through the Cloud in question.

Intra Cloud traffic is also most likely to take place over the Internet in some form. Such traffic is necessary for a number of reasons such as mirroring of hosting locations to give redundancy (for instance to protect against natural disasters like floods, or utility and telecoms provider failure). It can also provide load balancing and cost savings (from use of cheapest communications links). Other reasons for intra cloud traffic could include Data Dispersal for security purposes. Data Dispersal is a technique that allocates different data fragments onto different cloud storage locations. Different ways
of doing this have been documented in the paper *Information Dispersion over Redundant Arrays of Optimal Cloud Storage* by Spillner et al. [52]

Such Intra Cloud traffic transmission might be performed over private data circuits, but it can be argued that it is more likely to be over the Internet to make maximum use of the CSP’s investment in Internet Service Provider services. Suitable technology to use in this case would be IPSec in Tunnel Mode. IPSec is a standards based, proven method to offer endpoint authentication, integrity protection and replay protection as well as confidentiality of data through Encryption. The IPSec standard offers the ability to use different encryption algorithms and key lengths, which can to chosen to be appropriate to the data being transmitted. IPSec processing overhead can be offloaded to VPN Gateway appliances to create a tunnel between two or more different Cloud Provider geographic locations. This will also allow multiple endpoints on the same networks to use the secure tunnel and is one of the most secure and efficient ways to achieve this.

**Mitigations proposed as a result of this study**

- The Cloud User should undertake due diligence to user their prospective provider uses encryption both between the users and the CSP as well as intra-cloud
- Such encryption should be appropriate in terms of type of encryption algorithm and length of key, in relation to the type of data being transmitted, and the cover time required. This can be determined through information from appropriate authorities such as NIST or ECRYPT (as presented at www.keylength.com) [53]
- Due diligence should be done in terms of use of Certificate Authorities to ensure there is an appropriate level of trust and awareness of any limitation of liability.
Risk 12: Insecure or Ineffective Deletion of Data

ENISA risk rating: MEDIUM probability and VERY HIGH impact. Mitigated risk rating: LOW probability and VERY HIGH impact

SUMMARY OF ANALYSIS: The most effective and easily achievable way to remove this risk is to use self encrypting drives, albeit at a financial cost.

There are multiple issues with persistence of data, once it is in the Cloud. The first is that of knowing where it physically resides. Data may be in multiple locations for purposes of redundancy and availability. It may also be spread around different locations for security reasons when using Data Dispersal techniques. Even in a local context, data may be located in different parts of a Redundant Array of Inexpensive Disks (RAID) in a Storage Area Network. This means it could be difficult or even impossible to determine the precise physical locations of a customer’s data.

Additionally, it is necessary to consider backups; backup data should be archived off in different generations to some kind of secondary storage such as secondary disk arrays or tape. These same backups should be preserved offsite in some way (for disaster recovery purposes. Thus, it is possible to see that even if primary storage is well organised it can easily be the case that the customer start to exist in many different copies in many different places and it thus becomes ever harder to eliminate all of it.

It is also easy to take snapshot images of entire virtual machines – again leading to multiple data copies in different locations. Adding the additional dimension of the Cloud Supply Chain leading to further additional data copies at each level of the chain, increases the risk further.

The second issue is that due to the shared platform nature of the Cloud, data belonging to other tenants may be located on the same disk drive, or even the same partition of a disk drive. Thus, to remove a customer data set for deletion or other purposes is not as simple as removing a disk drive, even if the CSP is able to tell with any certainty where the data is located.

The third issue is that secure physical deletion of data from a drive is not straightforward, and is becoming increasingly difficult with the advent of new drive technologies such as Solid State Disks (SSD).

The reason data deletion is not straightforward is, it can be said, that computer operating systems have been deliberately designed to make it difficult, rather than easy, to lose data.

Starting at the highest level, the simple act of deleting a file does not actually delete the binary representation of the file data on the hard drive, it merely deletes the pointer to the files physical location from the drive’s file index (File
Allocation table or Master File Table in NTFS, possibly the most commonly used file system in the data Server environment. An analogy can be made to say that this is akin to removing the contents or index page from a book, and then saying that the contents of the book have been deleted – this is clearly not the case as the words still remain on the pages of the book.

Back in the computer context, the binary representation of the deleted data will only disappear if it is overwritten by another file, in the case where the operating system allocates the file to the same physical disk location (it might not, if there is plenty of free space on the disk drive). If an attacker comes into possession of the target users hard disk drive, it is relatively easy to bypass the file index and directly analyse the raw data blocks on the disk drive – and indeed many commercial software packages exist to retrieve such ‘deleted’ data. Thus, the only way to really remove the target data is to overwrite the exact same location on the hard drive with alternate data (either all 0’s or all 1’s are often used).

Furthermore, going a layer deeper, to the mechanisms of the magnetic disk drive, it is known that the disk drive heads that write the data to the disk platters are usually misaligned to some degree. This can result in the random data that might be used to overwrite the sensitive data not being written to exactly the same place. This therefore gives a small but feasible opportunity for a skilful attacker with the right tools, to retrieve some or all of the data after a single re-write.

Various different studies have been made of this with one postulated benchmark calling for an overwrite of up to 35 times (Gutmann P, Secure deletion of data from Magnetic and Solid State Media) [54] to achieve total elimination of previous data, but more recent studies disputing this in real world conditions (Overwriting Hard Drive Data: The Great Data Wiping Controversy) [55]. In any case, it is a fact that a number of international military standards call for 3 overwrite passes (U.S DoD, German Federal Government, British InfoSec Standard, Enhanced), although some more commercially oriented standards only call for one pass (UK Infosec Standard 5, Baseline).

Non magnetic, Solid State (Flash) disks, or SSDs are now cheap enough to start being used in a data center environment, however the true deletion of data is no more straightforward with this technology. This is due to the fact that the memory locations of SSDs are prone to wear during use. This has led to the use of a ‘Flash Translation Layer’ which manages the usage of the various locations in the disk to enable their even usage, and duplication of data from worn to good locations. The net result of this is another layer (beyond the operating system) where data is not actually deleted, but rather the pointer to it is changed or removed. This again leads to persistence of the data after deletion. Overwrite is only a partial solution, due to management software in the drive suspending locations marked as no longer usable, even though they may actually contain data. It is also not clear at this point if ‘secure erase’ commands to wipe the entire SSD are consistently implemented by vendors.
There are three aspects to the importance of this as far as real world Cloud Services are concerned. On the one hand, such elaborate but necessary data deletion methods are expensive for the CSP. If they can physically find a given tenant’s data, even overwriting a disk once is time consuming, twice (or investing in a physical hard disk shredder) is even more expensive.

It can be argued that this means that there is an incentive for the CSP not to take such steps for secure deletion. The position of various CSPs with respect to an assurance on data deletion varies.

A study by the Queen Mary University of London Cloud Legal Project [56] into the contractual terms of CSPs revealed a great deal of variance in the way this is treated in the industry. No providers guaranteed the assured deletion of data as part of their standard terms and conditions, a few bespoke contracts for bigger end users added it on a best efforts basis and some charged extra for such a service, again, to larger customers with negotiated contracts.

Secondly, it is the case that disposed of and recycled hardware, including disks containing sensitive data, has turned up back in circulation (see ‘Ghana, Digital Dumping Ground’ [57]). Thus this is a real threat to data security.

Finally, and perhaps most importantly, this issue becomes a legal issue with significant consequences for the Cloud Service User. Data Protection Legislation such as the UK Data Protection Act 1998 (DPA) [33] views the Cloud Service user as the Information Controller, and thus responsible. Serious breaches of the DPA can result in fines of up to £500,000, enough to put many organisations out of business. This is not to mention reputational damage or litigation by individuals in the case of breach of personally identifiable information.

Mitigations proposed as a result of this study

- It is essential for the Cloud Service User to determine the policies of a prospective CSP in relation to data deletion, before entering into an agreement. If there is an opportunity to negotiate this and gain an assurance that the CSP can assure this, or impose liability on the CSP if they fail to do so, this should be taken.
- The most practical and secure mitigation to prevent leakage of data through inefficient deletion, is encryption of the data while it is within the CSP’s infrastructure. However, depending on the level at which encryption is done, vulnerabilities can be introduced either through leakage of data in the clear, or mis-management of keys. Self encrypting drives (SEDs) offer an easy and low risk way to remove this risk. The disk itself does the encryption on board. An encryption key needed to read and write; as soon as this key is removed or deleted the information can no longer be accessed (in practical terms anyway, if appropriate encryption algorithms and key lengths are used). The drawback of this is the expense of SEDs compared to traditional hard drives; the CSP could well agree to use these but is likely to pass the cost on to the customer in some way. Nevertheless, this may be the most cost effective way to handle this risk.
Risk 13: Distributed Denial of Service

ENISA risk rating: MEDIUM probability, HIGH impact  
Mitigated risk rating: LOW probability, MEDIUM impact

**SUMMARY OF ANALYSIS:** Many proven methods of preventing traditional Denial of Service (DoS) exist. Economic DoS (EDoS) is a commercial risk that can be transferred back to the CSP. Cloud InternalDoS (CIDoS) is a largely theoretical attack at this point, with specific and unclear returns.

There are three aspects to Denial of Service in the Cloud environment:

1. The same DoS / DDoS that can affect any computer resource connected to a public network and for which many tools and safeguards exist (firewalls, stateful packet inspection, IPV6).
2. CIDoS Cloud Internal Denial of Service and
3. EDoS, intended to achieve the aim of increasing the costs of the Cloud User or CSP.

Since the first type is mostly not specific to the cloud, and secure networking measures to mitigate it are widely discussed elsewhere, it is not proposed to discuss this in any detail.

CIDoS refers to Cloud Internal Denial of Service and refers to an internal attacker attempting to change the dynamics with a given cloud environment to adversely affect the operation of a given Virtual Machine (VM).

CIDoS uses the automatic load balancing and provisioning principles that are a core part of the Cloud definition. As load increases, some Cloud systems have the functionality that will allow them to balance load and migrate VMs to other servers and activate additional servers as necessary. This activity has a high cost in terms of consumption of host resources and potentially energy resources. If the attacker can keep this process running constantly and put the Cloud infrastructure into a constant state of flux, there is theoretically the potential to cause significant disruption in a high scale ‘utility’ type Cloud Service context.

A paper by Alfari & Wolthusen, *Dynamic Parameter Reconnaissance for Stealthy IDoS Attack [58]* describes a method of monitoring cloud parameters to discover thresholds that precipitate the migration of VMs and so facilitate such an attack. It is unknown if any such attacks have been seen in the wild, or how likely this would be given the sophistication required, but it is true that the impact could be significant in a Utility type environment (of the profile of AWS for example).

EDoS also uses the essential cloud properties of elasticity, self-provisioning and load balancing, but the objective of the attacker is to focus the effect on the commercial consequences.
A large number of CSPs have a commercial model of pay per use that offers the customer extreme flexibility and best use of financial resources, and usually has some kind of CPU cycle metric at the heart of the charging model.

The vulnerability is simply that the attacker maliciously forces the usage of the innocent Cloud Service user up, thus costing them more money, and in extreme case Denial of Service either due to lack of funds, viability or exceeding some threshold set by the service provider. The attack is most likely to be perpetrated via a failure of authentication of Identity at some level, or less likely by internal compromise of hypervisor/VMs (similar to CDoS). The main problem for the user and CSP is that a spike in demand for resources could easily be legitimate to cover a peak in user demand – and thus monitoring of parameters for spikes alone is unlikely to be reliable.

**Mitigations proposed as a result of this study**

- The CSP should have monitoring tools such as stateful packet inspection, intrusion detection and prevention and related policies in place to detect suspicious rise in activity and carry out necessary investigations.
- The CSP should indemnify the Cloud Service User against malicious consumption of resources, as a contractual condition.
- Cloud Service user should look for a billing mitigation such as increasing their level of usage for free for a buffer period, or giving notification and a grace period to pay for unpredicted peaks, giving the user time to investigate (see comments at http://rationalsecurity.typepad.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-service-to-edos-economic-denial-of-sustaina.html) [59]
Risk 14: Loss of Encrypton Keys

ENISA risk rating: LOW probability and HIGH impact.
Mitigated risk rating: LOW probability and HIGH impact.

**SUMMARY OF ANALYSIS**: Encrypting data is an effective way to address a number of vulnerabilities in a cloud context, so its use becomes more widespread than in a traditional environment. Thus there are more keys, more chances for compromise. Secure ways to handle the keys are being developed.

Encryption can offer the answer to a number of the security risks present in the cloud. For example, the risk of data being compromised by other tenants on the same hardware platform goes away if the user data stored on that platform is encrypted – the attacker may be able to reach the data, but it is of no use to them if its encrypted, and they don’t have the key. It is a slightly different story if the data in question is processed within the cloud, for instance with SaaS – often it will only be possible to process the data in unencrypted form, in which case the data becomes vulnerable again. Sometimes though, it is possible to process the data in encrypted form with techniques such as homomorphic encryption where the data is stored in a format resembling the original (e.g a credit card number retaining the same format but with encrypted digits) enabling it to be processed. Similarly, if data is kept encrypted until it reaches the client desktop outside of the Cloud, data in motion is also protected.

Certain related standards, for instance PCI – DSS, do mandate encryption of sensitive data, and other standards like ISO 27001 recommend encryption of data.)

However, such encryption stands for nothing if the keys are insecure and improperly managed. This is obvious; if keys are kept with data in the Cloud, on the same or logically adjacent servers, or embedded in software, or otherwise kept in the open and accessible to the attacker, the encryption does not provide any protection.

**Mitigations proposed as a result of this study**

- The normal principles of good key management apply such as key separation, use of multiple keys, preferably used only once, such session keys being generated with sufficient entropy from sufficiently secure seeds. However, in the Cloud context, although its necessary to separate they keys from the data, it is also necessary for them to have some level of proximity in order for them to be usable if the data is to be processed within the cloud. This can be solved in a number of ways, which have various different advantages and drawbacks.
- External key management services are a widely used solution, either with completely separate and external key management service, or with a pseudo-separation offered by the Cloud Vendor (for example AWS Key Management Service). However, it can be said that these solutions just shift the task to a separate location but retain many of the risks. There are the same potential issues of trust, supply chain, flawed technology that would apply in the Cloud context. In some ways, the problems are just increased because another vendor is involved with an associated set of similar potential problems.

- Other solutions are use of a split-key solution, where the key is separated into two fragments, one retained and managed externally by the Cloud Customer, and one retained internally within the Cloud on a key management platform within the Cloud Infrastructure. The attacker has to gain access to both key fragments in order to unencrypt the data. This is an implementation of the 'two man' rule. Such a scheme was documented in a paper *How to Share a Secret* by Adi Shamir in 1979 [60]. Such solutions are produced by vendors as 'split key' technology.

- Finally, Trusted Platform Modules (TPM) on server hardware can offer a way to secure keys within the Cloud infrastructure, but in a secure module offering sealed storage and usually some source of entropy for random number generation to generate additional keys. The TPM has no resident software to reduce the risk of malicious software or root kits controlling it, and is read directly via hardware memory locations. Often these are linked to protection in the processor such as Intel Trusted eXecution Technology (TXT) which will prevent un-privileged processes from accessing the TPM. Use of the TPM in virtualised environments is supported, but appears to be inconsistently supported. For example, VMWARE support a hardware TPM in order to measure the integrity of the software stack loaded on the server in question (by storing a hash value). The Hypervisor can use a TPM in this way to store the signature of the stack of a given VM to validate the image and expose tampering (see VMWARE’s *Security of the VMWARE vSphere Hypervisor* [18]).

- However, in this case it does not appear able to expose the TPM to the VM itself. This prevents the VM from using disk encryption with disk encryption packages such as Bitlocker) – see VMWARE blog entry https://communities.vmware.com/thread/515017, accessed 20/7/2015 [61].

- On the other hand, XEN, the Opensource Hypervisor project does appear to offer a Virtual TPM support (see XEN wiki entry: http://wiki.xenproject.org/wiki/Virtual_Trusted_Platform_Module_(vTPM), accessed 20/7/2015 [62]).
Risk 15: Subject of malicious probes or scans

ENISA risk rating: probability MEDIUM and impact MEDIUM. Mitigated risk rating: probability MEDIUM and impact MEDIUM.

**SUMMARY OF ANALYSIS:** well proven methods and tools exist to counter the effects of probing and scanning. If these are properly implemented by the CSP, where the cost of such counter measures can be spread over a larger number of computing resources than in a traditional environment, it can be argued that they will thus be more likely used, so making the cloud more secure.

Network scanners and probes are the standard tools of hackers, both ethical and malicious. They are used to build a picture of the target systems in terms of their network topology, numbers of systems and types of systems (including operating systems and applications).

Such tools (and services) are often based on the same foundations, one of the most popular being nmap, an open source, community developed scanning tool.

nmap sends specially crafted packets to the target systems and analyses the responses to determine a network and machine topology. For instance, to find out address ranges in a network, analyse prompt responses to determine operating system types and scan network ports to enumerate services that would be available on the target machine.

This information can be used as part of an attacker’s due diligence to build a picture and select and launch exploits to utilise known exploits to compromise a system.

Such scanning is equally valid in the cloud context as much as the traditional network scenario. A scan can be launched on a Virtual machine which can return results that gives information about co-tenants. Ristenpart et al. described such an exploit in the paper *Hey You, Get Off My Cloud: Exploring Information Leakage in Third Party Compute Clouds* [63]. In this paper, the authors used nmap, hping and wget tools to build up a network map within an Amazon EC2 Cloud, then use this information to manoeuvre a rogue VM co-resident on the same platform. They were then able to attempt side channel attacks to the target VM.

Such tools and their methods are widely understood. This enables a large amount of preventative work to be done by a CSP at a number of different levels to block or detect such discovery packets. Such detection is at the heart of Intrusion Detection Systems. For instance, a ping is one of the most basic of such discovery packets, that is routinely detected and blocked by system administrators to prevent such scanners getting information. This blocking can take place at various levels, either in perimeter firewalls in the Cloud Infrastructure, or on virtual firewalls between different hypervisors or even virtual machines. However, the fact is that the only real way to eliminate all
such information leakage is to totally block all traffic; this is obviously not a feasible strategy, and therefore all networks have some degree of susceptibility regarding this.

A large amount of work has been done to analyse the context of network traffic to try and determine if a given packets are genuine, or from malicious scanners. The result is the advent of Stateful Packet Inspection firewalls which deny packets depending on application context. Such technology should be deployed by CSPs.

Techniques for obfuscating and decoying attackers in the cloud, when such attacks have been detected, have also been proposed (see *Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud*, Stolfo et al [64]).

It should also be noted that probing and scanning are useful tools in the course of due diligence, to ensure a customer’s Cloud environment is secure. This is recognised by a number of the major CSPs (for instance AWS and Salesforce.com) who allow such testing, but only after notification by the customer that such tests are taking place. This is a sensible precaution which allows the CSP to differentiate between real and test attacks in their intrusion detection systems.

**Mitigations proposed as a result of this study**

- The CSP should deploy and configure firewalls and other Intrusion Detection and prevention devices in accordance with an appropriate policy that is available to the customer. These devices should take account of traffic between VMs as well as at the perimeter of the cloud infrastructure.
- Software should be patched up to date to remove vulnerabilities.
- The Cloud Service customer should take the opportunity to undertake preventative penetration testing (or employ a third party to do it) by agreement with the CSP.
- Intrusion detection alerts should be acted upon, in accordance with a suitable policy. There are plenty of examples where this has not been done, resulting in data breaches.
Risk 16: Compromise of Service Engine

ENISA risk rating: LOW probability and VERY HIGH impact.
Mitigated risk rating: LOW probability and VERY HIGH impact

**SUMMARY OF ANALYSIS:** This concerns extra layers of functionality added by the CSP. The potential for risk and its impact depends upon the complexity added. The major mitigations to this are secure software development principles. The user must trust the CSP on this point.

This risk refers to any CSP mechanisms that manage customer resources, such as billing, provisioning and monitoring/logging. Depending on the functionality offered by the CSP, it could be the hypervisor layer discussed for risk 8 or the management layer discussed in risk 10. See also Figure 3 on page 22.

**Mitigations proposed as a result of this study.**

- Secure software design principles such as economy of mechanism, least privilege and failsafe defaults are the most effective mitigation. It is up to the CSP to use these. The service user has to trust this has been done, perhaps with the aid of a independent software audit, however this is unlikely to be possible for the majority of customers.
Risk 17: Conflicts between Customer Hardening procedures and Cloud environment

ENISA risk rating: LOW probability, MEDIUM impact
Mitigated risk rating: LOW probability, MEDIUM impact

**SUMMARY OF ANALYSIS:** The mechanisms that prevent isolation failure are the biggest protection here; in chapter 3 we have established these to be mature, effective and responsive to standards based controls.

This risk refers to vulnerabilities or mis-management on the customer side that could lead to compromise of other users on the same cloud platform. For example, weak handling of authentication credentials could enable an attacker access to the CSP platform, from where they could make an onward attack to a different tenant on the same platform.

Such a situation is influenced by different types of usage of the platform by different tenants. It can be argued for instance that a consumer using a Cloud Service to store recreational media may deem it unnecessary to use a strong password compared to a commercial user using the same platform to store financial records.

This involves the CSP obliging the Cloud User to adhere to a certain security standard in the interests of all the other tenants. It also means the CSP must orient their own security provisions towards the value of the most sensitive information asset on their platform.

**Mitigations proposed as a result of this study.**

- From the CSP perspective, contractual provisions that commit the Service User to some kind of liability in the event that their negligence leads to a breach of the platform for other users would be a sensible deterrent to lax security standards.

- From the Service User perspective, a sensible precaution is to evaluate the market and customer base at which the CSP targets its services. If the other tenants of the platform have a similar interest in preventing loss or other breach, the likelihood of such risks occurring will be lower than if there is a very mixed customer base using the platform.
Risk 18: Subpeona and E-discovery

ENISA risk rating: HIGH probability and MEDIUM impact.
Mitigated risk rating: MEDIUM probability, MEDIUM impact.

SUMMARY OF ANALYSIS: Many of the issues around this risk also apply to non-cloud environments and thus the Cloud User has the same responsibilities around data retention as the non-cloud user. Furthermore, the same controls a CSP should implement around disaster recovery would serve in the unlikely event an LEA did seize an entire cloud, thus denying service to co-tenants.

This risk describes the necessity for an organisation to make information available for evidential reasons during legal or regulatory proceedings. For instance, in some legal systems, in the event of litigation, it is the case that one side must make available material information, whether or not it is requested. This obliges organisations to keep information such as email available for this purpose for an extended length of time.

The major cloud specific danger is in the case of forensic investigations; it may be that an entire hardware platform needs to be seized for detailed investigation. This obviously has much more potential for disruption to co-tenants. It is unlikely an LEA would seize an entire cloud platform (as opposed to a copy of the information held on it); partly because of reasons of disruption to others, but mainly because the advantage they would gain would be questionable (see Overcast: Forensic discovery in Cloud Environments, Wolthusen, S) [65].

Concerning availability of archived information, Certain sources make much of the risks around this topic (see CSA’s Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, domain 3.3 [9]), however such a problem will still exist for an organisation whether or not it is using a Cloud Service to fulfil the relevant services. It could be said that this is not really a cloud risk in itself. In fact, it may well be that the various attributes of the cloud make it easier to access and retain such information in a known, officially sanctioned and adequately maintained repository, compared to the alternatives – such as non-sanctioned personal clouds, or retention of the relevant information on individual user’s hard disks – where the issue then becomes one of asset identification and tracking.

Mitigations Identified as a result of this study

- Controls should exist to ensure either the CSP and/or the Service User take adequate steps to retain data to mitigate risks such as Risk (1), Provider Lock in, Risk (2) Cloud Service Termination or Failure.
- The same controls that exist for non-cloud contexts to ensure retention and classification of data locations (or their equivalents) should be used in the cloud context.
Risk 19: Risk from Changes of Jurisdiction

ENISA risk rating: Probability VERY HIGH and impact HIGH.
Mitigated risk rating: Probability: MEDIUM, impact HIGH

**SUMMARY OF ANALYSIS:** Many CSPs are now transparent about where data is held for this very reason. Secondly, encryption or anonymization of the data in question can provide an effective mitigation to this risk.

This particular risk is concerned with the risk and unpredictability around certain jurisdictions in which a CSP may choose to hold data, rather than any concerns related to Data Protection (covered in risk 20). This means that a LEA of a certain jurisdiction may choose to seize and/or use certain information in a way that would be at odds with the laws or intentions of the Cloud User’s home or operational jurisdiction. Examples of this would be use of information for political or anti-competitive purposes.

One of the main vulnerabilities could be that a CSP would move the data into such an unfavourable jurisdiction without knowledge of the cloud user, perhaps in a bid to reduce their costs. Such jurisdiction may represent a risk for the cloud service user.

**Mitigations proposed as a result of this study**

- The Cloud User should ensure that there is transparency around the locations in which the CSP warehouses its data, and that it is contractually obliged not to change these locations without explicit consent of the user.
- The safest and simplest way for the Cloud User to be assured that this risk does not carry any impact would be to ensure it is encrypted when stored. If this is not possible, other means of data anonymization, such as masking, pseudonymisation or aggregation. (see Anonymisation: Managing data protection risk code of practice from the Information Commissioners Office [66]) can be used to mitigate.
Risk 20: Data Protection Risks

ENISA risk rating: HIGH probability and HIGH impact.
Mitigated risk rating: MEDIUM, impact HIGH

**SUMMARY OF ANALYSIS:** Anonymisation of data can be an acceptable measure to enable cloud storage and processing of PII. Auditable standard ISO 27018 enables a CSP to act as data processor on behalf of the Cloud Customer.

This risk concerns the observation of Data Protection legislation such as the 1988 *Data Protection Act* (UK) [33] or the *European Data Protection Directive (95/46/EC)* [67].

Under such legislation, the Cloud service user is defined as being a ‘Data Controller’ and as such is obliged by law to observe eight principles in respect of personal information, key among which is the prohibition of transfer of the data outside of ‘safe harbour’ country (EU or other designated countries such as the United States).

The risk for the Service User is similar to that in Risk 19, (Changes in Jurisdiction), in that if the CSP re-locates information without knowledge of the user, or in some other way compromises its security, it is the service user, as Data Controller, that will become liable.

However, if measures are taken to protect or anonymise the data, the data then becomes free of the obligations in the DPA or European Directive (see page 10 of the *Information Commissioners Anonymisation Code of Practice* [66]. Such measures include encryption (the code of practice specifically mentions AES, as a ‘non-probabilistic’ method of encryption – page 67).

**Mitigations proposed as a result of this study**

- Encryption of relevant data
- Anonymisation of relevant data
- In the event that data is or must be left as personally indentifiable (PII), ISO standard 27018 (an extension of 27001) defines an auditable governance framework to allow the CSP to process PII on behalf of the Cloud customer.
Risk 21: Licensing Risks

ENISA risk rating: MEDIUM probability and MEDIUM impact. Mitigated risk rating: probability LOW, impact LOW.

**SUMMARY:** Flexible licensing agreements with software vendors can mitigate this risk. If this is not possible, auditing and appropriate controls in management systems can address the risk instead (or in addition).

This risk refers mainly to the possibility that on demand resource provision will result in licensed software resources being consumed automatically, beyond the bounds of the Cloud User’s licensing agreements, without their knowledge, and thus expose them to intellectual property disputes. In particular, the ability to automatically spawn new VMs may result in the concurrent use limit of licences being exceeded.

**MITIGATIONS**

- Appropriate licencing agreements can be drafted with vendors to take account of momentary peaks in capacity and licences.
- Audit controls should be applied to ensure usage is monitored and kept within boundaries
- Management controls can be applied to prevent resource usage beyond specified limits.
4.5: Cloud Risk Matrix

The diagram below depicts the risks discussed in this Chapter in terms of impact and probability, with the proposed mitigations applied.

- **Figure 6: Mitigated Cloud Risk overview**
- The key take away of this is three categories of risk represented in red (top right), blue, and green (bottom left). In essence:
  - **Green** is low risk, easily or cost effectively treated.
  - **Blue** is high risk, but treatable with appropriate controls and tools.
  - **Red** is high risk, but difficult or impossible to treat – requiring risk acceptance or avoidance
Chapter 5 Conclusions

Following the conclusion of this study, the author is considerably more optimistic about the security of Cloud, than he was before the study started. Many of the risks can be quite adequately dealt with using well proven technology building blocks, tools and controls that are already available today.

In fact, there is case to say that security can be better and more cost-effectively implemented in the Cloud, leading to a more secure environment than the traditional model of data islands residing on customer premises. A per user analysis of the cost of Security measures in the Cloud compared to on premise environments may be an interesting area for further study.

However, the potential Cloud user must also be aware there are some significant risks around loss of control and governance in the Cloud that do not have complete mitigations. Summing this up in one sentence: it is possible to outsource almost everything, but it is very difficult to outsource responsibility.

This gives rise to some recommendations for those looking to use the Cloud, and for those concerned with the study and improvement of its Security:

The Cloud service users own organisation must be take some responsibility to reduce or monitor certain risks. It is not advisable to take a hands-off approach – there is a necessity to manage the supplier and hold them to account as necessary in order to maintain security.

As a consequence, the total savings gained by using a Cloud service should not be put straight back to the organisation’s bottom line – it is necessary to spend some of that saving on management and risk mitigation.

To get adequate assurance, it is necessary to ensure the chosen provider implements certain tools and technologies that will cost extra money and may limit choice of provider. For example, encryption of data within the cloud costs more than leaving the data unencrypted and also adds complication. However, it is the safest way to remove some of the risks around data protection, data leakage and persistence of data. Such cost is likely to be passed back to the Cloud service user. Thus, the Cloud user should be prepared to pay extra for a secure service – the cheapest Cloud provider is not always the most secure.

Contracts are not always an effective management tool. This is partly because standardised ‘click to accept’ contracts with unfavourable terms for users are widely used, but also because they have limited financial remedy. The concept of the Cloud supply chain looks set to increase, bringing with it a loss of transparency and increased risk.

There seems to be a positive correlation between provider size on the one hand and standards adherence, transparency around security provisions, and
the ability for the customer to audit the supplier on the other. Perhaps such suppliers take more precautions because they have more to lose. This area may be deserving of further study.

The number and applicability of standards to Cloud appears to be improving and a good way to engender trust in a provider. However, the majority of applicable standards were not originally developed with Cloud in mind and it would be a useful area of specific study to evaluate how well such standards correlate to Cloud and what the gaps might be.
Bibliography


ISO standard for Virtualisation

[33] United Kingdom Information Commissioners Office: Data Protection Act 1998

[34] ISO: 27001 Information Security Management Standard

Stanford Technology Law Review Volume 16 number 1 fall 2012

http://cloudindustryforum.org/downloads/CIF%20CoP%20Document%201_An%20Executive%20Briefing_(1.0).pdf
accessed 22/8/2015

[37] Cloud Security Alliance: Security Trust & Assurance Registry
https://cloudsecurityalliance.org/star/
accessed 22/8/2015


[39] John Leyden: The Register Casino DDOS duo caged for five years after blackmail buyout threat, 2013 The Register
http://www.theregister.co.uk/2013/12/19/casino_cyber_extortionists_jailed/
Accessed 30/06/2015

[40] Eneco: Dutch companies try warming homes with cloud servers, 24/03/2015 Eneco
http://news.eneco.com/heat-your-home-for-free-with-heating-provided-by-a-computer-server
accessed 30/06/2015


[42] Amazon: Amazon Cloudwatch, 2015 Amazon
http://aws.amazon.com/cloudwatch/
accessed 03/07/2015
https://www.commoncriteriaportal.org/
accessed 10/07/2015

https://web.cs.dal.ca/~gates/papers/csiirw08.pdf (conference proceeding)
accessed 22/8/2015


[47] Schneier, B: Attack Trees, 1999 SANS Institute

[48] Amazon: AWS Console screenshot, 2015 Amazon
accessed 15/07/2015

[49] Somorovsky et al. :All your Clouds are Belong to us - Security Analysis of Cloud Management Interfaces, 2011 CCSW (conference proceeding)

accessed 22/8/2015


[53] Damien Giry, Bluekrypt
www.keylength.com
accessed 16/07/2015

[54] Gutmann, P: Secure deletion of data from Magnetic and Solid State Media, 1996, Usenix

http://www.vidarholen.net/~vidar/overwriting_hard_drive_data.pdf
accessed 22/8/2015
[56] Millard, C: Cloud Computing Law, Jan-13 Oxford University Press
Chapter 3 P39

[57] Peter Klein: Ghana; Digital Dumping Ground, 2009University of
British Columbia Graduate School of Journalism
http://www.pbs.org/lineworld/stories/ghana804/video/video_index.h
ml
accessed 17/12/2015

[58] Alarifi & Wolthusen Dynamic Parameter Reconnaissance for Stealthy
IDoS attack within Cloud Systems, 2014 CCS 2012 (conference
proceeding)

http://rationalsecurity.typepad.com/blog/2008/11/cloud-computing-
security-from-ddos-distributed-denial-of-service-to-edos-economic-
denial-of-sustaina.html
accessed 18/07/2015

[60] Adi Shamir: How to Share a Secret, 1979 Massachusetts Institute of
Technology
Communications of the ACM
November 1979 Volume 22 number 11

[61] VMWARE: "Is it possible to get the TPM chip be emulated, or can a
pass-through be created somehow?" (VMWARE blog) 07/07/2015
https://communities.vmware.com/thread/515017
accessed 20/07/2015

[62] XEN project: vTPM wiki.xenproject.org, 11/03/2015 XEN wiki
http://wiki.xenproject.org/wiki/Virtual_Trusted_Platform_Module_(vTPM
)
accessed 20/07/2015

Information Leakage in Third-Party Compute Clouds" CCSconference
proceeding November 9-13 2009, Chicago, Illinois

[64] Stolfo et al. Fog Computing: Mitigating Insider Data Theft Attacks in the
Cloud,2012 IEEE Computer SocietyS Security and Privacy workshop
(conference proceedings)

[65] Wolthusen, S : Overcast - Forensic Discovery in Cloud Environments,
2009 Fifth International Conference on IT Security Incident
Management and IT Forensics (conference proceeding)

[66] UK Information Commisioners Office : Anonymisation: Managing data
protection risk code of practice , Nov-12 UK ICO
https://ico.org.uk/media/1061/anonymisation-code.pdf
accessed 30/07/2015
European Commission 1995