TARGET AUDIENCE

The intended audiences of this report are:

- business leaders, of Small and Medium Entreprices (SMEs) in particular, to facilitate their evaluation and mitigation of the risks associated with adopting cloud computing technologies;
- European policymakers, to aid them in deciding on research policy (to develop technologies to mitigate risks);
- European policymakers, to assist them in deciding on appropriate policy and economic incentives, legislative measures, awareness-raising initiatives, etc, vis-à-vis cloud-computing technologies;
- individuals or citizens, to enable them to evaluate the costs and benefits of using the consumer version of these applications.

Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies. Cloud computing architectures have:

- ***highly abstracted resources***
- ***near instant scalability and flexibility***
- ***near instantaneous provisioning***
- ***shared resources (hardware, database, memory, etc)***
- ***'service on demand', usually with a 'pay as you go' billing system***
- ***programmatic management (eg, through WS API).***

CLOUD COMPUTING - WORKING DEFINITION

This is the working definition of cloud computing we are using for the purposes of this study. It is not intended as yet another definitive definition. Sources for our definition can be reviewed at (5), (6) and (54).

Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies. Cloud computing architectures have:

- highly abstracted resources
- near instant scalability and flexibility
- near instantaneous provisioning
- shared resources (hardware, database, memory, etc)
- 'service on demand', usually with a 'pay as you go' billing system
- programmatic management (e.g., through WS API).

There are three categories of cloud computing:

- **Software as a service (SaaS): is** software offered by a third party provider, available on demand, usually via the Internet configurable remotely. Examples include online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs, etc).
- **Platform as a service (PaaS):** allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine.
- **Infrastructure as service (IaaS):** provides virtual machines and other abstracted hardware and operating systems which may be controlled through a service API. Examples include Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live Skydrive and Rackspace Cloud.

Clouds may also be divided into:

- **public**: available publicly - any organisation may subscribe
- **private:** services built according to cloud computing principles, but accessible only within a private network
- **partner:** cloud services offered by a provider to a limited and well-defined number of parties.

In general, the commodity, cost, liability and assurance of clouds vary according to the following figure:

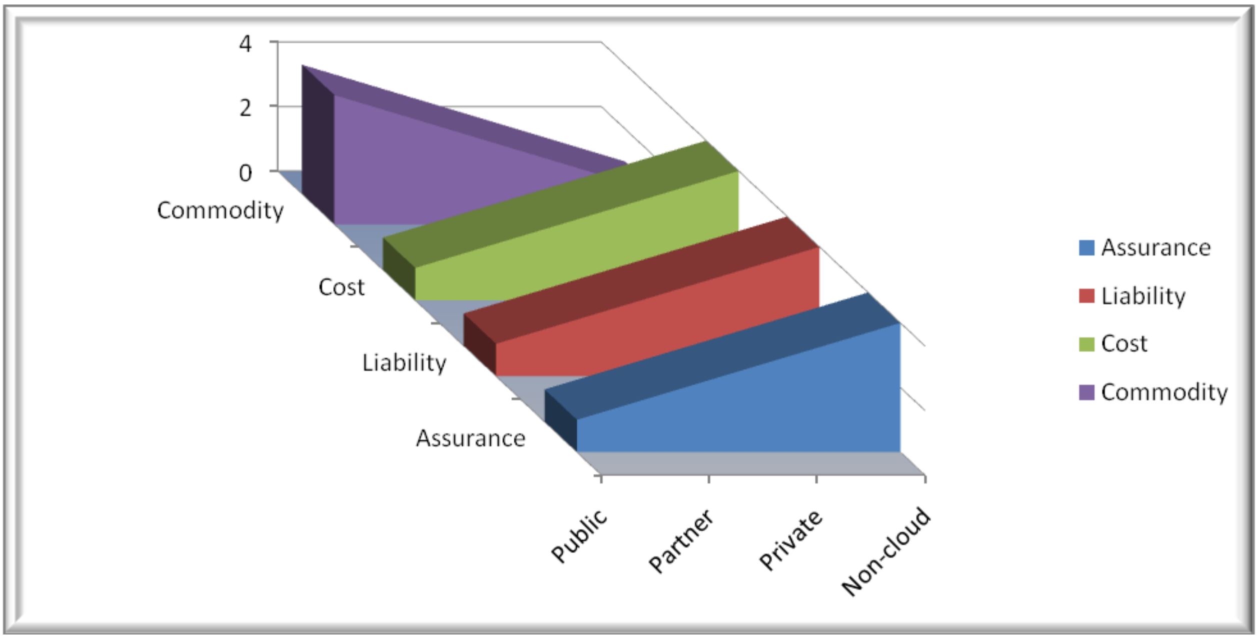


FIGURE 1: FEATURES OF PUBLIC, PARTNER AND PRIVATE CLOUDS

SURVEY OF EXISTING WORK

In compiling this report, we surveyed existing work on cloud security risks and their mitigation, including *Security Guidance for Critical Areas of Focus in Cloud Computing* (Cloud security Alliance (55)) *Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration* (Jericho Forum (56)) and *Assessing the Security Risks of Cloud Computing* (Gartner (57)) in order to understand where to focus its results for maximum added value.

1. SECURITY BENEFITS OF CLOUD COMPUTING

> ***Put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection.***

It is hardly necessary to repeat the many rain-forests' worth of material which has been written on the economic, technical and architectural and ecological benefits of cloud computing. However, in the direct experience of the members of our expert group, as well as according to recent news from the 'real world', an examination of the security risks of cloud computing must be balanced by a review of its specific security benefits. Cloud computing has significant potential to improve security and resilience. What follows is a description of the key ways in which it can contribute.

SECURITY AND THE BENEFITS OF SCALE

Put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection. This includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances and hypervisors, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense. Other benefits of scale include:

- **Multiple locations:** most cloud providers have the economic resources to replicate content in multiple locations by default. This increases redundancy and independence from failure and provides a level of disaster recovery out-of-the-box.
- **Edge networks:** storage, processing and delivery closer to the network edge mean service reliability and quality is increased overall and local network problems are less likely to have global side-effects.
- **Improved timeliness of response**: larger **to incidents:** well-run larger-scale systems, for example due to early detection of new malware deployments, can develop more effective and efficient incident response capabilities.
- **Threat management:** cloud providers can also afford to hire specialists in dealing with specific security threats, while smaller companies can only afford a small number of generalists.

SECURITY AS A MARKET DIFFERENTIATOR

Security is a priority concern for many cloud customers [see the survey: An SME perspective on Cloud Computing] – customers will make buying choices on the basis of the reputation for confidentiality, integrity and resilience, and the security services offered by a provider, more so than in traditional environments. This is a strong driver for cloud providers to improve their security practices and compete on security.

STANDARDISED INTERFACES FOR MANAGED SECURITY SERVICES

Large cloud providers can offer a standardised, open interface to managed security services (MSS) providers offering services to all its customers. This potentially creates a more open and readily available market for security services where customers can switch providers more easily and with lower set-up costs.

The ability to dynamically scale defensive resources on demand has obvious advantages for resilience. Furthermore, the more all kinds of individual resources can be scaled in a granular way, without scaling all of the system resources, the cheaper it is to respond to sudden (non-malicious) peaks in demand.

RAPID, SMART SCALING OF RESOURCES

The list of cloud resources which can be rapidly scaled on demand already includes, e.g., storage, CPU time, memory, web service requests and virtual machine instances, and the level of granular control over resource consumption is increasing as technologies mature.

A cloud provider has the potential to dynamically reallocate resources for filtering, traffic shaping, encryption, etc, in order to increase support for defensive measures (e.g., against DDoS attacks) when an attack is likely or it is taking place. When this ability for dynamic resource reallocation is combined with appropriate resource optimisation methods, the cloud provider may be able to limit the effect that some attacks could have on the availability of resources that legitimately hosted services use, as well as limit the effect of increasing the use of resources by the security defence to combat such attacks. Achieving this requires however that the provider implements adequate coordination of autonomics for security defence and for resource management and optimisation.

The ability to dynamically scale defensive resources on demand has obvious advantages for resilience. Furthermore, the more all kinds of individual resources can be scaled in a granular way, without scaling all of the system resources, the cheaper it is to respond to sudden (non-malicious) peaks in demand.

AUDIT AND EVIDENCE-GATHERING

IaaS offerings support on-demand cloning of virtual machines. In the event of a suspected security breach, the customer can take an image of a live virtual machine – or virtual components thereof – for offline forensic analysis, leading to less down-time for analysis. With storage on tap, multiple clones can be created and analysis activities parallelised to reduce investigation time. This improves the ex-post analysis of security incidents and increases the probability of tracking attackers and patching weaknesses. However, it does presume the customer has access to trained forensic experts (which is not a standard cloud service as of writing).

It can also provide more cost-effective storage for logs, thus allowing more comprehensive logging without compromising performance. Pay as you go cloud storage brings transparency to your audit storage costs and makes adjusting to meet future audit log requirements easier. This makes the process of identifying security incidents as they happen more efficient (7).

Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model.

MORE TIMELY AND EFFECTIVE AND EFFICIENT UPDATES AND DEFAULTS

Virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes; moreover, IaaS cloud service APIs also allow snapshots of virtual infrastructure to be taken regularly and compared with a baseline (e.g., to ensure software firewall rules have not changed) (8). Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model. Finally in PaaS and SaaS models the applications are more likely to have been hardened to run outside the enterprise environment, which makes them likely to be more portable and robust than the equivalent enterprise software (where it exists). They are also more likely to be regularly updated and patched in a centralized fashion minimizing the window of vulnerability.

AUDIT AND SLAS FORCE BETTER RISK MANAGEMENT

The need to quantify penalties for various risk scenarios in SLAs and the possible impact of security breaches on reputation (see Security as market differentiator) motivate more rigorous internal audit and risk assessment procedures than would otherwise be exist. The frequent audits imposed on CPs tend to expose risks which would not otherwise have been discovered, having therefore the same positive effect.

BENEFITS OF RESOURCE CONCENTRATION

Although the concentration of resources undoubtedly has disadvantages for security (see

Risks) it has the obvious advantage of cheaper physical perimiterisation and physical access control (per unit resource) and the easier and cheaper application of a comprehensive security policy and control over data management, patch management, incident management, and maintenance processes. The extent to which those savings are passed on to customers will obviously vary.

2. RISK ASSESSMENT

USE-CASE SCENARIOS

For the purposes of this risk assessment of cloud computing, we analyzed three use-case scenarios:

- An SME perspective on Cloud Computing
- The Impact of Cloud Computing on service resilience
- Cloud Computing and eGovernment (eHealth).)

For the sake of brevity we decided to publish the complete version of the SME use-case scenario (see ANNEX II) and a summary of the resilience and eHealth scenarios (see ANNEX III).

This selection was based on the rationale that in Europe the cloud market is foreseen to have a great impact on new businesses and start-ups, as well as on the way current business models will evolve. Since EU industry is mainly composed by SMEs (99% of companies according to EU sources- (9)) it makes sense to focus on SMEs. Nevertheless, we have included several risks and recommendations which apply specifically to governments and larger enterprises.

For the purposes of this risk assessment of cloud computing, we analyzed three use-case scenarios:

- ***An SME perspective on Cloud Computing***
- ***The Impact of Cloud Computing on service resilience***
- ***Cloud Computing and eGovernment (eHealth).***

The SME scenario is based on the results of the survey: An SME perspective on Cloud Computing (see here), and it is NOT meant to be a road map for companies considering, planning or running cloud computing projects and investments.

A medium-sized company was used as a use-case to guarantee to the assessment a high enough level of IT, legal and business complexity. The aim was to expose all possible information security risks. Some of those risks are specific to medium-sized businesses;, others are general risks that micro or small enterprises are also likely to face when migrating to a cloud computing approach.

The scenario was NOT intended to be completely realistic for any single cloud client or provider but all elements of the scenario are likely to occur in many organisations in the near future.

Risk assessment process

The level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact. The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.

The likelihood of each incident scenario and the business impact was determined in consultation with the expert group contributing to this report, drawing on their collective experience. In cases where it was judged not possible to provide a well founded estimation of the likelihood of an occurrence, the value is N/A. In many cases the estimate of likelihood depends heavily on the cloud model or architecture under consideration.

The following shows the risk level as a function of the business impact and likelihood of the incident scenario. The resulting risk is measured on a scale of 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating:

- Low risk: 0-2
- Medium Risk: 3-5
- High Risk: 6-8

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

We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

3. RISKS

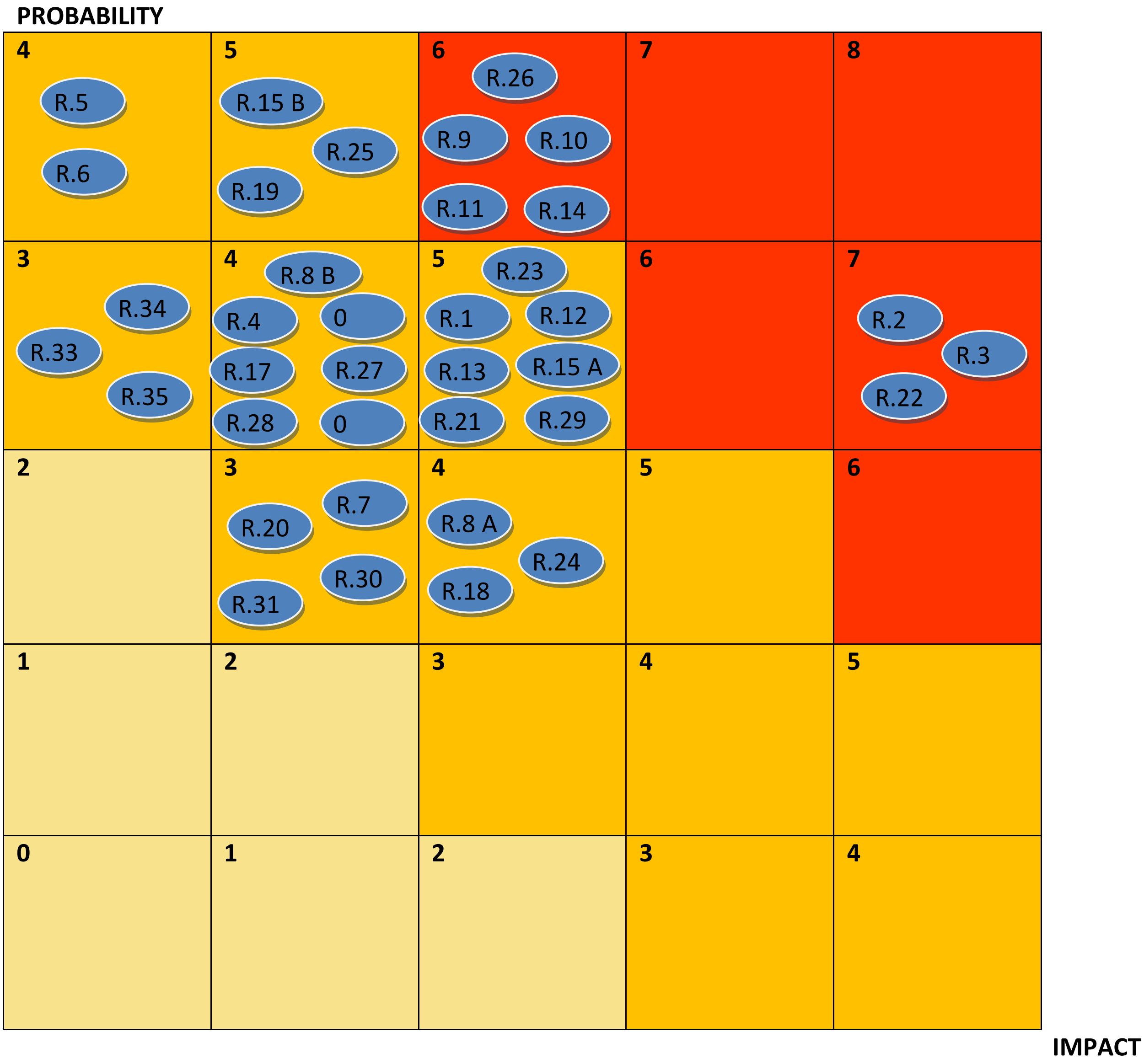
The following points should be noted in relation to the descriptions of risk below:

Risk should always be understood in relation to overall business opportunity and appetite for risk – sometimes risk is compensated by opportunity.

- Risk should always be understood in relation to overall business opportunity and appetite for risk – sometimes risk is compensated by opportunity.
- Cloud services are not only about convenient storage, accessible by multiple devices, but include important benefits such as more convenient communication and instant multi-point collaboration. Therefore, a comparative analysis needs to compare not only the risks of storing data in different places (on premises v the cloud) but also the risks when on premises-data stored on premises – e.g. a spreadsheet - is emailed to other persons for their contributions, against the security issues of a spreadsheet stored in the cloud and open to collaboration between those persons. Therefore, the risks of using cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models.
- The level of risk will in many cases vary significantly with the type of cloud architecture being considered.
- It is possible for the cloud customer to transfer risk to the cloud provider and the risks should be considered against the cost benefit received from the services. However *not all risks can be transferred*: if a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage.
- The risk analysis in this paper applies to cloud technology. It does not apply to any specific cloud computing offering or company. This paper is not meant to replace a project-specific organisational risk assessment.
- The level of risks is expressed from the perspective of the cloud customer. Where the cloud provider point of view is considered, this is explicitly stated.

Therefore, the risks of using cloud computing should be compared to the risks of staying with traditional solutions, such as desktop-based models.

The following table shows the distribution of the risk probabilities and impacts:



PROBABILITY

4 R.5 R.6	5 R.15 B R.25 R.19	6 R.26 R.9 R.10 R.11 R.14	7	8
3 R.34 R.33 R.35	4 R.8 B R.4 0 R.17 R.27 R.28 0	5 R.23 R.1 R.12 R.13 R.15 A R.21 R.29	6	7 R.2 R.3 R.22
2	3 R.7 R.20 R.30 R.31	4 R.8 A R.24 R.18	5	6
1	2	3	4	5
0	1	2	3	4

IMPACT

FIGURE 2: RISK DISTRIBUTION

The risks identified in the assessment are classified into three categories:

- policy and organizational
- technical
- legal.

Each risk is presented in tables which include:

- probability level
- impact level
- reference to vulnerabilities
- reference to the affected assets
- level of risk.

Furthermore, *where meaningful*, we have added a comparative probability and impact cell to compare cloud computing risks and risks in standard IT approaches. We have not included a comparative risk since it is assumed that all the risks selected are higher.

> ***However not all risks can be transferred: if a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage.***

POLICY AND ORGANIZATIONAL RISKS

R.1 LOCK-IN

Probability	HIGH	Comparative: Higher
Impact	MEDIUM	Comparative: Equal
Vulnerabilities	V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

There is currently little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability (although some initiatives do exist, e.g., see. (58)). This makes it extremely difficult for a customer to migrate from one provider to another, or to migrate data and services to or from an in-house IT environment. Furthermore, cloud providers may have an incentive to prevent (directly or indirectly) the portability of their customers services and data.

This potential dependency for service provision on a particular CP, depending on the CP's commitments, may lead to a catastrophic business failure should the cloud provider go bankrupt (see R.5) and the content and application migration path to another provider is too costly (financially or time-wise) or insufficient warning is given (no early warning).

The acquisition of the cloud provider (R.6) can also have a similar effect, since it increases the likelihood of sudden changes in provider policy and non-binding agreements such as terms of use (ToU).

It is important to understand that the extent and nature of lock-in varies according to the cloud type:

SaaS Lock-in

- Customer data is typically stored in a custom database schema designed by the SaaS provider. Most SaaS providers offer API calls to read (and thereby 'export') data records. However, if the provider does not offer a readymade data 'export' routine, the customer will need to develop a program to extract their data and write it to file ready for import to another provider. It should be noted that there are few formal agreements on the structure of business records (e.g., a customer record at one SaaS provider may have different fields than at another provider), although there are common underlying file formats for the export and import of data, e.g., XML. The new provider can normally help with this work at a negotiated cost. However, if the data is to be brought back in-house, the customer will need to write import routines that take care of any required data mapping unless the CP offers such a routine. As customers will evaluate this aspect before making important migration decisions, it is in the long-term business interest of CPs to make data portability as easy, complete and cost-effective as possible.
- Application lock-in is the most obvious form of lock-in (although it is not specific to cloud services). SaaS providers typically develop a custom application tailored to the needs of their target market. SaaS customers with a large user-base can incur very high switching costs when migrating to another SaaS provider as the end-user experience is impacted (e.g., re-training is necessary). Where the customer has developed programs to interact with the providers API directly (e.g., for integration with other applications), these will also need to be re-written to take into account the new provider's API.

PaaS Lock-in

PaaS lock-in occurs at both the API layer (ie, platform specific API calls) and at the component level. For example, the PaaS provider may offer a highly efficient back-end data store. Not only must the customer develop code using the custom APIs offered by the provider, but they must also code data access routines in a way that is compatible with the back-end data store. This code will not necessarily be portable across PaaS providers, even if a seemingly compatible API is offered, as the data access model may be different (e.g., relational v hashing).

- PaaS lock-in at the API layer happens as different providers offer different APIs.
- PaaS lock-in happens at the runtime layer as 'standard' runtimes are often heavily customised to operate safely in a cloud environment. For example, a Java runtime may have 'dangerous' calls removed or modified for security reasons. The onus is on the customers' developers to understand and take into account these differences.
- PaaS also suffers from data lock-in, in the same way as in SaaS, but in this case the onus is completely on the customer to create compatible export routines.

> ***In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues which may affect security. For example ToUs may prohibit port scans, vulnerability assessment and penetration testing. Moreover, there may be conflicts between customer hardening procedures and the cloud environment (see R 20). On the other hand, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defenses.***
>
> ***Moreover the cloud provider may outsource or sub-contract services to third-parties (unknown providers) which may not offer the same guarantees (such as to provide the service in a lawful way) as issued by the cloud provider. Or the control of the cloud provider changes, so the terms and conditions of their services may also change.***

IaaS-Lock-in

IaaS lock-in varies depending on the specific infrastructure services consumed. For example, a customer using cloud storage will not be impacted by non-compatible virtual machine formats.

- IaaS computing providers typically offer hypervisor based virtual machines. Software and VM metadata is bundled together for portability – typically just within the provider's cloud. Migrating between providers is non-trivial until open standards, such as OVF (11), are adopted.
- IaaS storage provider offerings vary from simplistic key/value based data stores to policy enhanced file based stores. Feature sets can vary significantly, hence so do storage semantics. However application level dependence on specific policy features (e.g., access controls) may limit the customer's choice of provider.
- Data lock-in is the obvious concern with IaaS storage services. As cloud customers push more data to cloud storage, data lock-in increases unless the CP provides for data portability.

Common to all providers is the possibility of a 'run on the banks' scenario for a cloud provider. For this scenario, suppose there is a crisis of confidence in the cloud provider's financial position, and therefore a mass exit and withdrawal of content on a first come, first served basis. Then, in a situation where a provider limits the amount of 'content' (data and application code) which can be 'withdrawn' in a given timeframe, some customers will never be able to retrieve their data and applications.

R.2 LOSS OF GOVERNANCE

Probability	VERY HIGH	Comparative: Higher
Impact	VERY HIGH (depends on organization) (IaaS VERY HIGH, SaaS Low)	Comparative: Equal
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V21. Synchronizing responsibilities or contractual obligations external to cloud V23. SLA clauses with conflicting promises to different stakeholders V25. Audit or certification not available to customers V22. Cross-cloud applications creating hidden dependency V13. Lack of standard technologies and solutions V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V14. No source escrow agreement V16. No control on vulnerability assessment process V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use V44. Unclear asset ownership	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	HIGH	

In using cloud infrastructures, the client necessarily cedes control to the CP on a number of issues which may affect security. For example ToUs may prohibit port scans, vulnerability assessment and penetration testing. Moreover, there may be conflicts between customer hardening procedures and the cloud environment (see R 20). On the other hand, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defenses.
Moreover the cloud provider may outsource or sub-contract services to third-parties (unknown providers) which may not offer the same guarantees (such as to provide the service in a lawful way) as issued by the cloud provider. Or the control of the cloud provider changes, so the terms and conditions of their services may also change.

> ***Certain organisations migrating to the cloud have made considerable investments in achieving certification either for competitive advantage or to meet industry standards or regulatory requirements (eg, PCI DSS).***

The loss of governance and control could have a potentially severe impact on the organization’s strategy and therefore on the capacity to meet its mission and goals. The loss of control and governance could lead to the impossibility of complying with the security requirements, a lack of confidentiality, integrity and availability of data, and a deterioration of performance and quality of service, not to mention the introduction of compliance challenges (see R.3).

R.3 COMPLIANCE CHALLENGES

Probability	VERY HIGH – depends on PCI, SOX	Comparative: Higher
Impact	HIGH	Comparative: Equal
Vulnerabilities	V25. Audit or certification not available to customers V13. Lack of standard technologies and solutions, V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V26. Certification schemes not adapted to cloud infrastructures V30. Lack of information on jurisdictions V31. Lack of completeness and transparency in terms of use	
Affected assets	A20. Certification	
Risk	**HIGH**	

Certain organisations migrating to the cloud have made considerable investments in achieving certification either for competitive advantage or to meet industry standards or regulatory requirements (e.g., PCI DSS). This investment may be put at risk by a migration to the cloud:

- if the CP cannot provide evidence of their own compliance to the relevant requirements;
- if the CP does not permit audit by the CC.

Resource sharing means that malicious activities carried out by one tenant may affect the reputation of another tenant.

In certain cases, it also means that using a public cloud infrastructure implies that certain kinds of compliance cannot be achieved and hence cloud hosted services cannot be used for services that need them. For example, EC2 says customers would be hard-pressed to achieve PCI compliance on their platform. So EC2 hosted services cannot be used to handle credit card transactions.

R.4 LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES

Probability	LOW
Impact	HIGH
Vulnerabilities	V6. Lack of resource isolation V7. Lack of reputational isolation *V5.* HYPERVISOR VULNERABILITIES
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery
Risk	**MEDIUM**

Resource sharing means that malicious activities carried out by one tenant may affect the reputation of another tenant. For example, spamming, port scanning or the serving of malicious content from cloud infrastructure can lead to:

- a range of IP addresses being blocked, including the attacker and other innocent tenants of an infrastructure;
- confiscation of resources due to neighbour activities (neighbour subpoenaed).

The impact can be deterioration in service delivery and data loss, as well as problems for the organization's reputation.

R.5 CLOUD SERVICE TERMINATION OR FAILURE

Probability	N/A	
Impact	VERY HIGH	Comparative: Higher
Vulnerabilities	V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A9. Service delivery – real time services A10. Service delivery	
Risk	**MEDIUM**	

As in any new IT market, competitive pressure, an inadequate business strategy, lack of financial support, etc, could lead some providers to go out of business or at least to force them to restructure their service portfolio offering. In other words, it is possible that in the short or medium term some cloud computing services could be terminated.

The impact of this threat for the cloud customer is easily understandable, since it could lead to a loss or deterioration of service delivery performance, and quality of service, as well as a loss of investment.

Furthermore, failures in the services outsourced to the CP may have a significant impact on the cloud customer's ability to meet its duties and obligations to its own customers. The customer of the cloud provider may thus be exposed to contractual and tortuous liability to its customers based on its provider's negligence. Failures by the cloud provider may also result in liability by the customer to its employees.

R.6 CLOUD PROVIDER ACQUISITION

Probability	N/A

Impact	MEDIUM	Comparative: Higher
Vulnerabilities	V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery	
Risk	**MEDIUM**	

Acquisition of the cloud provider could increase the likelihood of a strategic shift and may put non-binding agreements at risk (e.g., software interfaces, security investments, non-contractual security controls). This could make it impossible to comply with the security requirements. The final impact could be damaging for crucial assets such as: the organization's reputation, customer or patient trust, and employee loyalty and experience.

R.7 SUPPLY CHAIN FAILURE

Probability	LOW	Comparative: Higher
Impact	MEDIUM	Comparative: Higher
Vulnerabilities	V31. Lack of completeness and transparency in terms of use V22. Cross-cloud applications creating hidden dependency V46. Poor provider selection V47. Lack of supplier redundancy	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	

Risk	MEDIUM

A cloud computing provider can outsource certain specialised tasks of its ‘production’ chain to third parties. In such a situation the level of security of the cloud provider may depend on the level of security of each one of the links and the level of dependency of the cloud provider on the third party. Any interruption or corruption in the chain or a lack of coordination of responsibilities between all the parties involved can lead to: unavailability of services, loss of data confidentiality, integrity and availability, economic and reputational losses due to failure to meet customer demand, violation of SLA, cascading service failure, etc.

> ***In such a situation the level of security of the cloud provider may depend on the level of security of each one of the links and the level of dependency of the cloud provider on the third party.***

An important example here is where a critical dependency exists on a third party single-sign-on or identity management service. In this case, an interruption of the third party service or of the CP’s connection to the service or a weakness in their security procedures may compromise the availability or confidentiality of a cloud customer or indeed the entire cloud offering.

In general, a lack of transparency in the contract can be a problem for the whole system. If a provider does not declare which core IT services are outsourced - it is not realistic that providers should list the contractors since these may change frequently - the customer is not in a position to properly evaluate the risk he is facing. This lack of transparency could decrease the level of trust in the provider.

TECHNICAL RISKS

R.8 RESOURCE EXHAUSTION (UNDER OR OVER PROVISIONING)

Probability	**A**. Inability to provide additional capacity to a customer: MEDIUM	Comparative: N/A
	B. Inability to provide current agreed capacity level: LOW	Comparative: Higher
Impact	**A**. Inability to provide additional capacity to a customer: LOW/MEDIUM (e.g., at Christmas)	Comparative: N/A

	B. Inability to provide current agreed capacity level: HIGH	Comparative: Same
Vulnerabilities	V15. Inaccurate modelling of resource usage V27. Inadequate resource provisioning and investments in infrastructure V28. No policies for resource capping V47. Lack of supplier redundancy	
Affected assets	A1. Company reputation A2. Customer trust A10. Service delivery A11. Access control / authentication / authorization (root/admin v others)	
Risk	**MEDIUM**	

Cloud services are on-demand services [see Cloud computing - working definition]. Therefore there is a level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections. Inaccurate modelling of resources usage - common resources allocation algorithms are vulnerable to distortions of fairness - or inadequate resource provisioning and inadequate investments in infrastructure can lead, from the CP perspective, to:

- Service unavailability: failure in certain highly specific application scenarios which use a particular resource very intensively (ie, CPU/Memory intensive number crunching or simulation (eg. forecasting stock prices);
- Access control compromised: in some cases it may be possible to force a system to 'fail open' in the event of resource exhaustion. [Ref: CWE-400: Uncontrolled Resource Consumption - Resource Exhaustion (12)];
- Economic and reputational losses: due to failure to meet customer demand.
- The opposite consequences of inaccurate estimation of resource needs could lead to:
- Infrastructure oversize: excessive provisioning leading to economic losses and loss of profitability.

From the cloud customer perspective, a poor provider selection and lack of supplier redundancy could lead to:

- Service unavailability: failure in the delivery (or degrading performance) of services both in real time and not in real time;
- Access control system compromised: put the confidentiality and Integrity of data at risk;

- Economic and reputational losses: due to failure to meet customer demand, violation of SLA, cascading service failure, etc.

Note: this risk could be also a consequence of a DDoS attack (see R. 15) and of misbehaving applications due to poor application compartmentalization in some cloud providers' systems.

Therefore there is a level of calculated risk in allocating all the resources of a cloud service, because resources are allocated according to statistical projections.

R.9 ISOLATION FAILURE

Probability	LOW (Private Cloud) MEDIUM (Public Cloud)	Comparative: Higher
Impact	VERY HIGH	Comparative: Higher
Vulnerabilities	V5. Hypervisor vulnerabilities V6. Lack of resource isolation V7. Lack of reputational isolation V17. Possibility that internal (cloud) network probing will occur V18. Possibility that co-residence checks will be performed	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

Multi-tenancy and shared resources are two of the defining characteristics of cloud computing environments. Computing capacity, storage, and network are shared between multiple users. This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure (e.g., so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks).

Note that the likelihood (probability) of this incident scenario depends on the cloud model considered; it is likely to be low for private

This class of risks includes the failure of mechanisms separating storage, memory, routing, and even reputation between different tenants of the shared infrastructure (eg, so-called guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table, and side channel attacks).

clouds and higher (medium) in the case of public clouds.
The impact can be a loss of valuable or sensitive data, reputation damage and service interruption for cloud providers and their clients.

R.10 CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES

Probability	MEDIUM (Lower than traditional)	Comparative: Lower
Impact	VERY HIGH (Higher than traditional)	Comparative: Higher (aggregate) Comparative: Same (for a single customer)
Vulnerabilities	V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V36. Need-to-know principle not applied V1. AAA vulnerabilities V39. System or OS vulnerabilities V37. Inadequate physical security procedures V10. Impossibility of processing data in encrypted form V48. Application vulnerabilities or poor patch management	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery	
Risk	HIGH	

The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. This can be considered especially important in the case of cloud computing due to the fact that cloud architectures necessitate certain roles which are extremely high-risk. Examples of such roles include CP system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident response. As cloud use increases, employees of cloud providers increasingly become targets for criminal gangs (as has been witnessed in the financial services industry with call centre workers (13), (14)).

R.11 MANAGEMENT INTERFACE COMPROMISE (MANIPULATION, AVAILABILITY OF INFRASTRUCTURE)

Probability	MEDIUM	Comparative: Higher
Impact	VERY HIGH	Comparative: Higher
Vulnerabilities	V1. AAA vulnerabilities V4. Remote access to management interface V38. Misconfiguration V39. System or OS vulnerabilities V48. Application vulnerabilities or poor patch management	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery A14. Cloud service management interface	
Risk	**MEDIUM**	

The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities. This includes customer interfaces controlling a number of virtual machines and, most importantly, CP interfaces controlling the operation of the overall cloud system. Of course, this risk may be mitigated by more investment in security by providers.

The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities.

R.12 INTERCEPTING DATA IN TRANSIT

Probability	MEDIUM	Comparative: Higher (for a given piece of data)
Impact	HIGH	Comparative: Same
Vulnerabilities	V1. AAA vulnerabilities V8. Communication encryption vulnerabilities V9. Lack of or weak encryption of archives and data in transit V17. Possibility that internal (cloud) network probing will occur V18. Possibility that co-residence checks will be performed V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A2. Customer trust A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A23. Backup or archive data	
Risk	**MEDIUM**	

Cloud computing, being a distributed architecture, implies more data in transit than traditional infrastructures. For example, data must be transferred in order to synchronise multiple distributed machine images, images distributed across multiple physical machines, between cloud infrastructure and remote web clients, etc. Furthermore, most use of data-centre hostedting is isimplemented using a secure VPN-like connection environment, a practice not always followed in the cloud context.

Sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks should be considered as possible threat sources.

Moreover, in some cases the CP does not offer a confidentiality or non-disclosure clause or these clauses are not sufficient to guarantee respect for the protection of the customer’s secret information and ‘know-how’ that will circulate in the ‘cloud’.

R.13 DATA LEAKAGE ON UP/DOWNLOAD, INTRA-CLOUD

Probability	MEDIUM (N/A)
Impact	HIGH
Vulnerabilities	V1. AAA vulnerabilities V8. Communication encryption vulnerabilities V17. Possibility that internal (cloud) network probing will occur V18. Possibility that co-residence checks will be performed V10. Impossibility of processing data in encrypted form V48. Application vulnerabilities or poor patch management
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A12. Credentials A13. User directory (data) A14. Cloud service management interface
Risk	**MEDIUM**

This is the same as the previous risk, but applies to the transfer of data between the cloud provider and the cloud customer.

R.14 INSECURE OR INEFFECTIVE DELETION OF DATA

Probability	MEDIUM	Comparative: Higher
Impact	Very HIGH	Comparative: Higher
Vulnerabilities	V20. Sensitive media sanitization	
Affected assets	A5. Personal sensitive data A6. Personal data A7. Personal data - critical	

	A12. Credentials
Risk	**MEDIUM**

Whenever a provider is changed, resources are scaled down, physical hardware is reallocated, etc, data may be available beyond the lifetime specified in the security policy. It may be impossible to carry out the procedures specified by the security policy, since full data deletion is only possible by destroying a disk which also stores data from other clients. When a request to delete a cloud resource is made, this may not result in true wiping of the data (as with most operating systems). Where true data wiping is required, special procedures must be followed and this may not be supported by the standard API (or at all).

There are several different scenarios in which a cloud customer's resources may be used by other parties in a malicious way that has an economic impact.

If effective encryption is used then the level of risk may be considered to be lower.

R.15 Distributed denial of service (DDoS)

Probability	Customer: MEDIUM	Comparative: Lower
	Provider: LOW	Comparative: N/A
Impact	Customer: HIGH	Comparative: Higher
	Provider: VERY HIGH	Comparative: Lower
Vulnerabilities	V38. Misconfiguration V39. System or OS vulnerabilities V53. Inadequate or misconfigured filtering resources	
Affected assets	A1. Company reputation A2. Customer trust A9. Service delivery – real time services A10. Service delivery A14. Cloud service management interface A16. Network (connections, etc)	
Risk	**MEDIUM**	

R.16 ECONOMIC DENIAL OF SERVICE (EDOS)

Probability	LOW
Impact	HIGH
Vulnerabilities	V1. AAA vulnerabilities V2. User provisioning vulnerabilities V3. User de-provisioning vulnerabilities V4. Remote access to management interface V28. No policies for resource capping
Affected assets	A1. Company reputation A2. Customer trust A9. Service delivery – real time services A10. Service delivery
Risk	**MEDIUM**

There are several different scenarios in which a cloud customer's resources may be used by other parties in a malicious way that has an economic impact:

- Identity theft: an attacker uses an account and uses the customer's resources for his own gain or in order to damage the customer economically.
- The CC has not set effective limits on the use of paid resources and experiences unexpected loads on these resources through no malicious actions.
- An attacker uses a public channel to use up the customer's metered resources - for example, where the customer pays per HTTP request, a DDoS attack can have this effect.

EDoS destroys economic resources; the worst case scenario would be the bankruptcy of the customer or a serious economic impact. NOTE: the general asset MONEY is not mentioned in the list.

R.17 LOSS OF ENCRYPTION KEYS

Probability	LOW	Comparative: N/A
Impact	HIGH	Comparative: Higher
Vulnerabilities	V11. Poor key management procedures V12. Key generation: low entropy for random number generation	

Affected assets	A4. Intellectual property A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A12. Credentials
Risk	**MEDIUM**

This includes disclosure of secret keys (SSL, file encryption, customer private keys, etc) or passwords to malicious parties, the loss or corruption of those keys, or their unauthorised use for authentication and non-repudiation (digital signature).

R.18 UNDERTAKING MALICIOUS PROBES OR SCANS

Probability	MEDIUM	Comparative: Lower
Impact	MEDIUM	Comparative: Lower
Vulnerabilities	V17. Possibility that internal (cloud) network probing will occur V18. Possibility that co-residence checks will be performed	
Affected assets	A1. Company reputation A2. Customer trust A9. Service delivery – real time services A10. Service delivery	
Risk	**MEDIUM**	

Malicious probes or scanning, as well as network mapping, are indirect threats to the assets being considered. They can be used to collect information in the context of a hacking attempt. A possible impact could be a loss of confidentiality, integrity and availability of service and data.

R.19 COMPROMISE SERVICE ENGINE

Probability	LOW
Impact	VERY HIGH
Vulnerabilities	V5. Hypervisor vulnerabilities V6. Lack of resource isolation

Affected assets	A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery
Risk	MEDIUM

Each cloud architecture relies on a highly specialized platform, the service engine that sits above the physical hardware resources and manages customer resources at different levels of abstraction. For example, in IaaS clouds this software component can be the hypervisor. The service engine is developed and supported by cloud platform vendors and the open source community in some cases. It can be further customized by the cloud computing providers.

Like any other software layer, the service engine code can have vulnerabilities and is prone to attacks or unexpected failure. An attacker can compromise the service engine by hacking it from inside a virtual machine (IaaS clouds), the runtime environment (PaaS clouds), the application pool (SaaS clouds), or through its APIs.

Cloud providers must set out a clear segregation of responsibilities that articulates the minimum actions customers must undertake.

Hacking the service engine may be useful to escape the isolation between different customer environments (jailbreak) and gain access to the data contained inside them, to monitor and modify the information inside them in a transparent way (without direct interaction with the application inside the customer environment), or to reduce the resources assigned to them, causing a denial of service.

R.20 CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT

Probability	LOW
Impact	MEDIUM
Vulnerabilities	V31. Lack of completeness and transparency in terms of use V23. SLA clauses with conflicting promises to different stakeholders V34. Unclear roles and responsibilities
Affected assets	A4. Intellectual property A5. Personal sensitive data

	A6. Personal data A7. Personal data - critical
Risk	MEDIUM

Customers must realize and assume their responsibility as failure to do so would place their data and resources at further risk.

Cloud providers must set out a clear segregation of responsibilities that articulates the minimum actions customers must undertake. The failure of customers to properly secure their environments may pose a vulnerability to the cloud platform if the cloud provider has not taken the necessary steps to provide isolation. Cloud providers should further articulate their isolation mechanisms and provide best practice guidelines to assist customers to secure their resources.

Customers must realize and assume their responsibility as failure to do so would place their data and resources at further risk. In some cases cloud customers have inappropriately assumed that the cloud provider was responsible for, and was conducting, all activities required to ensure security of their data. This assumption by the customer, and/or a lack of clear articulation by the cloud provider, placed unnecessary risk on the customer's data. It is imperative that cloud customers identify their responsibilities and comply with them.

Cloud providers, by their very nature, are tasked with providing a multi-tenant environment, whether this is via virtualization on a server or the common network shared by the customers. The co-location of many customers inevitably causes conflict for the cloud provider as customers' communication security requirements are likely to be divergent from each other.
Take, for example, the case of two customers on a shared traditional network infrastructure. If one customer wishes the network firewall to block all traffic except for SSH, but another customer is running a web server farm and requires passage of HTTP and HTTPS, who wins? This same type of issue is raised by customers who have competing and conflicting compliance requirements. This type of challenge only worsens as the number of tenants and the disparity of their requirements increase. Therefore, cloud providers must be in a position to deal with these challenges by way of technology, policy and transparency (where appropriate).

LEGAL RISKS

R.21 SUBPOENA AND E-DISCOVERY

Probability	HIGH

Impact	MEDIUM
Vulnerabilities	V6. Lack of resource isolation V29. Storage of data in multiple jurisdictions and lack of transparency about THIS V30 Lack of information on jurisdictions
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7 Personal data - critical A9. Service delivery – real time services A10. Service delivery
Risk	HIGH

In the event of the confiscation of physical hardware as a result of subpoena by law-enforcement agencies or civil suits (15), the centralisation of storage as well as shared tenancy of physical hardware means many more clients are at risk of the disclosure of their data to unwanted parties (16), (17), (18).

At the same time, it may become impossible for the agency of a single nation to confiscate 'a cloud' given pending advances around long distance hypervisor migration.

R.22 RISK FROM CHANGES OF JURISDICTION

Probability	VERY HIGH
Impact	HIGH
Vulnerabilities	V30. Lack of information on jurisdictions V29. Storage of data in multiple jurisdictions and lack of transparency about THIS
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery

Risk	HIGH

Customer data may be held in multiple jurisdictions, some of which may be high risk. If data centres are located in high-risk countries, e.g., those. lacking the rule of law and having an unpredictable legal framework and enforcement, autocratic police states, states that do not respect international agreements, etc, sites... s could be raided by local authorities and data or systems subject to enforced disclosure or seizure. Note that we are not implying here that all subpoena law-enforcement measures are unacceptable, merely that some may be so and that some legitimate seizures of hardware (which appear to be rare)may affect more customers than the targets of a law-enforcement action depending on how the data is stored (19), (20).

R.23 DATA PROTECTION RISKS

Probability	HIGH
Impact	HIGH
Vulnerabilities	V30. Lack of information on jurisdictions V29. Storage of data in multiple jurisdictions and lack of transparency about THISthis
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery
Risk	HIGH

Cloud computing poses several data protection risks for cloud customers and providers.

- It can be difficult for the cloud customer (in its role of data controller) to effectively check the data processing that the cloud provider carries out, and thus be sure that the data is handled in a lawful way. It has to be clear that the cloud customer will be the main person responsible for the processing of personal data, even when such processing is carried out by the cloud provider in its role of external processor. Failure to comply with data protection law may lead to administrative, civil and also criminal sanctions, which vary from country to country, for the data controller.. This problem is exacerbated in the case of multiple transfers of data e.g., between federated clouds. On the other hand, some cloud providers do provide information on the data processing that they carry out. Some also offer certification summaries of their data processing and data security activities and the data controls they have in place, e.g.,. SAS70 certification providers.

- There may be data security breaches which are not notified to the controller by the cloud provider.
- The cloud customer may lose control of the data processed by the cloud provider. This issue is increased in the case of multiple transfers of data (e.g., between federated cloud providers).
- The cloud provider may receive data that have not been lawfully collected by its customer (the controller).

R.24 LICENSING RISKS

Probability	MEDIUM	Comparative: Higher
Impact	MEDIUM	Comparative: Higher
Vulnerabilities	V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A9. Service delivery – real time services A20. Certification	
Risk	MEDIUM	

Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment. For example, if software is charged on a per instance basis every time a new machine is instantiated then the cloud customer's licensing costs may increase exponentially even though they are using the same number of machine instances for the same duration. In the case of PaaS and IaaS, there is the possibility for creating original work in the cloud (new applications, software etc). As with all intellectual property, if not protected by the appropriate contractual clauses (see ANNEX I – Cloud computing – Key legal issues , Intellectual Property), this original work may be at risk.

RISKS NOT SPECIFIC TO THE CLOUD

In the course of our risk analysis, we identified the following threats which are not specific to cloud computing, but should nevertheless be considered carefully when assessing the risk of a typical cloud-based system.

R.25 NETWORK BREAKS

Probability	LOW	Comparative: Same
Impact	VERY HIGH	Comparative: Higher

Vulnerabilities	V38. Misconfiguration V39. System or OS vulnerabilities V6. Lack of resource isolation V41. Lack of, or a poor and untested, business continuity and disaster recovery plan
Affected assets	A9. Service delivery – real time services A10. Service delivery
Risk	MEDIUM

One of highest risks! Potentially thousands of customers are affected at the same time.

R.26 Network management (ie, network congestion / mis-connection / non-optimal use)

Probability	MEDIUM	Comparative: Same
Impact	VERY HIGH	Comparative: Higher
Vulnerabilities	V38. Misconfiguration V39. System or OS vulnerabilities V6. Lack of resource isolation V41. Lack of, or a poor and untested, business continuity and disaster recovery plan	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A9. Service delivery – real time services A10. Service delivery A16 Network (connections, etc)	
Risk	**HIGH**	

R.27 Modifying network traffic

Probability	LOW
Impact	HIGH
Vulnerabilities	V2. User provisioning vulnerabilities V3. User de-provisioning vulnerabilities V8. Communication encryption vulnerabilities V16. No control on vulnerability assessment process
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical

	A9. Service delivery – real time services A10. Service delivery
Risk	MEDIUM

R.28 PRIVILEGE ESCALATION

Probability	LOW	Comparative: Lower
Impact	HIGH	Comparative: Higher (for cloud provider)
Vulnerabilities	V1. AAA vulnerabilities V2. User provisioning vulnerabilities V3. User de-provisioning vulnerabilities V5. Hypervisor vulnerabilities V34. Unclear roles and responsibilities V35. Poor enforcement of role definitions V36. Need-to-know principle not applied V38. Misconfiguration	
Affected assets	A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A11. Access control / authentication / authorization (root/admin v others) A13. User directory (data)	
Risk	MEDIUM	

R.29 SOCIAL ENGINEERING ATTACKS (IE, IMPERSONATION)

Probability	MEDIUM	Comparative: Same
Impact	HIGH	Comparative: Higher
Vulnerabilities	V32. Lack of security awareness V2. User provisioning vulnerabilities V6. Lack of resource isolation V8. Communication encryption vulnerabilities V37. Inadequate physical security procedures	
Affected assets	A1. Company reputation A2. Customer trust A3. Employee loyalty and experience A4. Intellectual property A5. Personal sensitive data	

	A6. Personal data A7. Personal data - critical A8. HR data A11. Access control / authentication / authorization (root/admin v others) A12. Credentials
Risk	MEDIUM

R.30 LOSS OR COMPROMISE OF OPERATIONAL LOGS

Probability	LOW	Comparative: Lower
Impact	MEDIUM	Comparative: Same (for customer)
Vulnerabilities	V52. Lack of policy or poor procedures for logs collection and retention V1. AAA vulnerabilities V2. User provisioning vulnerabilities V3. User de-provisioning vulnerabilities V19. Lack of forensic readiness V39. System or OS vulnerabilities	
Affected assets	A21. Operational logs (customer and cloud provider)	
Risk	MEDIUM	

R.31 LOSS OR COMPROMISE OF SECURITY LOGS (MANIPULATION OF FORENSIC INVESTIGATION)

Probability	LOW	Comparative: Lower
Impact	MEDIUM	Comparative: Same (for customer)
Vulnerabilities	V52. Lack of policy or poor procedures for logs collection and retention V1. AAA vulnerabilities V2. User provisioning vulnerabilities V3. User de-provisioning vulnerabilities V19. Lack of forensic readiness V39. System or OS vulnerabilities	
Affected assets	A22. Security logs	
Risk	MEDIUM	

R.32 BACKUPS LOST, STOLEN

Probability	LOW	Comparative: Lower
Impact	HIGH	Comparative: Same (for customer)
Vulnerabilities	V37. Inadequate physical security procedures V1. AAA vulnerabilities V2. User provisioning vulnerabilities V3. User de-provisioning vulnerabilities	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery A23. Backup or archive data	
Risk	MEDIUM	

R.33 UNAUTHORIZED ACCESS TO PREMISES (INCLUDING PHYSICAL ACCESS TO MACHINES AND OTHER FACILITIES)

Probability	VERY LOW	Comparative: Lower
Impact	HIGH (to have a very high impact it should a target attack (pointing to a specific machine, etc) otherwise the impact should be high.	Comparative: Higher
Vulnerabilities	V37. Inadequate physical security procedures	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A23. Backup or archive data	
Risk	MEDIUM	

Since cloud providers concentrate resources in large data centres, and although the physical perimeter controls are likely to be stronger, the impact of a breach of those controls is higher.

R.34 THEFT OF COMPUTER EQUIPMENT

Probability	VERY LOW	Comparative: Lower
Impact	HIGH	Comparative: Higher
Vulnerabilities	V37. Inadequate physical security procedures	
Affected assets	A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A17. Physical hardware	
Risk	MEDIUM	

R.35 NATURAL DISASTERS

Probability	VERY LOW	Comparative: Lower
Impact	HIGH	Comparative: Higher
Vulnerabilities	V41. Lack of, or a poor and untested, business continuity and disaster recovery plan	
Affected assets	A1. Company reputation A2. Customer trust A5. Personal sensitive data A6. Personal data A7. Personal data - critical A8. HR data A9. Service delivery – real time services A10. Service delivery A23. Backup or archive data	
Risk	MEDIUM	

Generally speaking, the risk from natural disasters is lower compared to traditional infrastructures because cloud providers offer multiple redundant sites and network paths by default.

4. VULNERABILITIES

The following list of vulnerabilities it is not exhaustive but is, however, detailed enough for the purposes of our analysis. It contains both cloud-specific and general information security vulnerabilities.

V1. AAA VULNERABILITIES

A poor system for authentication, authorization and accounting, could facilitate unauthorized access to resources, privileges escalation, impossibility of tracking the misuse of resources and security incidents in general, etc, through:

- insecure storage of cloud access credentials by customer:
- insufficient roles available;
- credentials stored on a transitory machine.

Furthermore, the cloud makes password based authentication attacks (trend of fraudster using a Trojan to steal corporate passwords) much more impactful since corporate applications are now exposed on the Internet. Therefore password-based authentication will become insufficient and a need for stronger or two-factor authentication for accessing cloud resources will be necessary.

V2. USER PROVISIONING VULNERABILITIES

- Customer cannot control provisioning process.
- Identity of customer is not adequately verified at registration.
- Delays in synchronisation between cloud system components (time wise and of profile content) happen.
- Multiple, unsynchronised copies of identity data are made.
- Credentials are vulnerable to interception and replay.

V3. USER DE-PROVISIONING VULNERABILITIES

De-provisioned credentials are still valid due to time delays in roll-out of revocation.

V4. REMOTE ACCESS TO MANAGEMENT INTERFACE

Theoretically, this allows vulnerabilities in end-point machines to compromise the cloud infrastructure (single customer or CP) through, for example, weak authentication of responses and requests.

V5. HYPERVISOR VULNERABILITIES

Hypervisor-layer attacks are very attractive: the hypervisor in fact fully controls the physical resources and the VMs running on top of it, so any vulnerability in this layer is extremely critical. Exploiting the hypervisor potentially means exploiting every VM. The first proof of concept of a layer-below attack against a hypervisor was given by King et al in the paper (21), where the authors introduce the concept of a virtual machine-based Rootkit. By then a few vulnerabilities had been identified in the most popular hypervisors (e.g., (22) and (23)) which can be exploited without administrator access rights at this time, but none of their results had been un-patched at the time of writing.

A typical scenario enabled by exploiting a hypervisor's vulnerability is the so called 'guest to host escape', an example of which is 'Cloudburst', a VMware vulnerability recently discovered and documented in reference (24). Another scenario is 'VM hopping': in which an attacker hacks a VM using some standard method and then – exploiting some hypervisor vulnerability – takes control of other VMs running on the same hypervisor. For more information, see an *Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments*, see (25).

V6. LACK OF RESOURCE ISOLATION

Resource use by one customer can affect resource use by another customer.
IaaS cloud computing infrastructures mostly rely on architectural designs where physical resources are shared by multiple virtual machines and therefore multiple customers.
Vulnerabilities in the hypervisor security model may lead to unauthorized access to these shared resources. For example, virtual machines of Customer 1 and Customer 2 have their virtual hard drives saved in the same shared LUN (Logical Unit Number) inside a SAN. Customer 2 may be able to map the virtual hard drive of Customer 1 to its virtual machine and see and use the data inside it.
Hypervisors used in IaaS clouds offer rich APIs that the cloud provider uses to develop a proprietary management, provisioning and reporting interface that is exposed to its customers. Vulnerabilities in the hypervisor security model or in the 'management interfaces' may lead to unauthorized access to customer information. At the same time a vulnerability at this level may allow an attacker to manipulate the assets inside the cloud facility, provoking denial of service (e.g., shut down of running virtual machines), data leakage (e.g., the copying and transfer outside the cloud of virtual machines), data compromise (e.g., replacement of virtual machines with modified copies), or direct financial damage (e.g., replication and launch of many copies of the virtual machines).
Moreover lack of controls on cloud cartography and co-residence and the cross side channel vulnerabilities (see (26)) can pose serious risks to resources isolation. For example, if resource usage is not independent between Customer 1 and Customer 2, Customer 1 can map Customer 2's resources. This can be done, for example, by using controlled loading of Customer 2's resources while measuring changes in Customer 1's own patterns of resource availability.