



Cloud Computing

BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY

DANIELE CATTEDDU, CISM, CISA
EUROPEAN NETWORK AND INFORMATION SECURITY
AGENCY

PHILIPPE MASSONET, CETIC, BELGIUM
(philippe.massonet@cetic.be)



Presentation Overview

- ★ What is it?
- ★ **Good News: Security Benefits of Cloud Computing**
- ★ **Bad News: Security Risks of Cloud Computing**
- ★ Recommendations





What is Cloud Computing?

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



Key characteristics

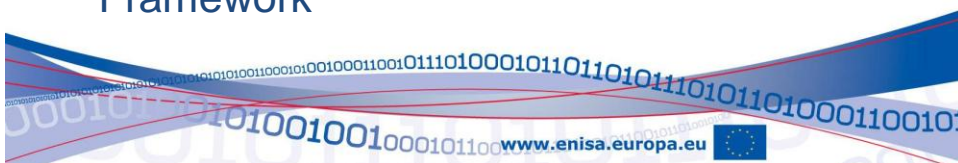
- ★ Highly **abstracted** resources
- ★ Near **instant scalability** and flexibility
- ★ Near **instantaneous provisioning**
- ★ **Shared resources** (hardware, database, memory, etc...)
- ★ **'Service On demand'**, usually with a **'pay as you go'** billing system
- ★ **Programmatic management** (e.g. through WS API)





ENISA Risk Assessment of Cloud Computing Technologies

- ★ Scenario description - selected scenarios:
 - ★ SME Migration
 - ★ Resilience
 - ★ Government eHealth
- ★ Analysis of risks (Assets, Vulnerabilities, Threats)
- ★ Recommendations
- ★ Using ENISA Emerging and Future Risk Framework



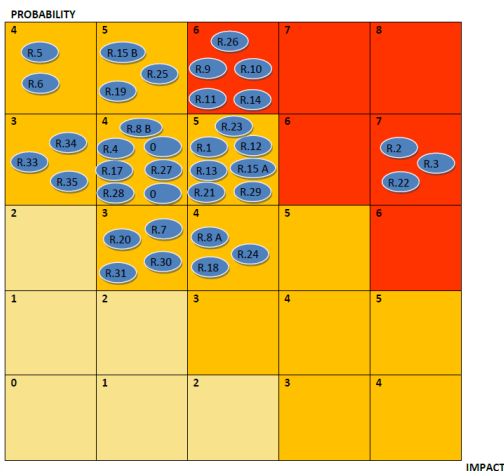
Our Expert Group

- | | |
|---------------------|--|
| ★ Baker & McKenzie | ★ Department of Health, UK |
| ★ British Telecom | ★ Reservoir Project |
| ★ Cloudsecurity.org | ★ RSA |
| ★ Google | ★ Spire Security |
| ★ HP | ★ Symantec |
| ★ Kaspersky | ★ The Israeli Association of GRID Technologies (IGT) |
| ★ IBM | ★ Virtualization.info |
| ★ Microsoft | |





Methodology: Risk Distribution

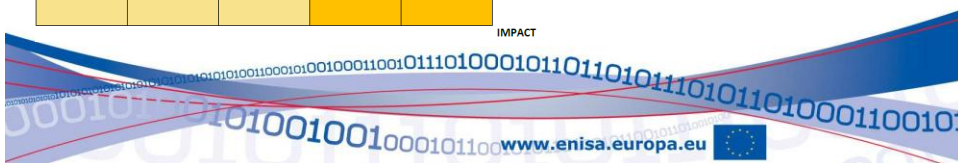


Types of risk:

- Policy and organisational
- Technical
- Legal

For each risk:

- prob. and impact level (ISO/IEC 27005)
- ref. to vulnerabilities
- ref. to affected assets
- level of risk



Example Scenario





SME Scenario: Security risks for an SME migrating to the cloud.

Name: Clean Future

Business Sector: Photovoltaic

Based in: Germany with 3 branch offices in Europe

Employees: 93 people and between 10 and 30 contractors (interim agents, sales representatives, consultants, trainees, etc.).

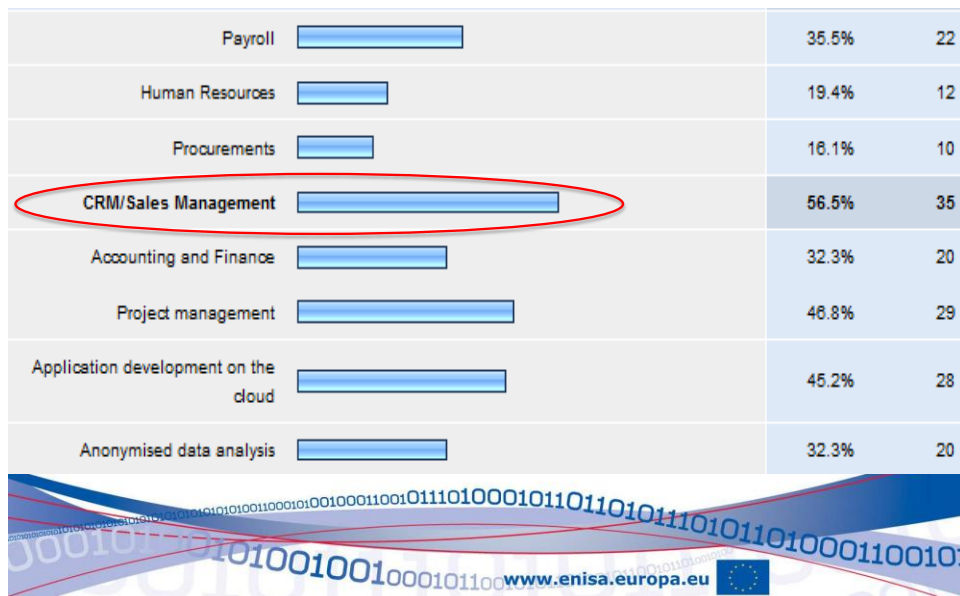


SME's - Reasons for adoption

Remove economic/expertise barriers impeding to modernize business processes by the introduction of Information Technology		29.5%	18
Avoiding capital expenditure in hardware, software, IT support, Information Security by outsourcing infrastructure/platforms/services		70.5%	43
Flexibility and scalability of IT resources		67.2%	41
Increasing computing capacity and business performance		34.4%	21
Diversification of IT systems		8.2%	5
Local and global optimisation of IT infrastructure through automated management of virtual machines		26.2%	16
Business Continuity and Disaster recovery capabilities		55.7%	34
Assessing the feasibility and profitability of new services (i.e. by developing business cases into the Cloud)		31.1%	19
Adding redundancy to increase availability and resilience		29.5%	18
Controlling marginal profit and marginal costs		14.8%	9



SME's - Business Processes Considered

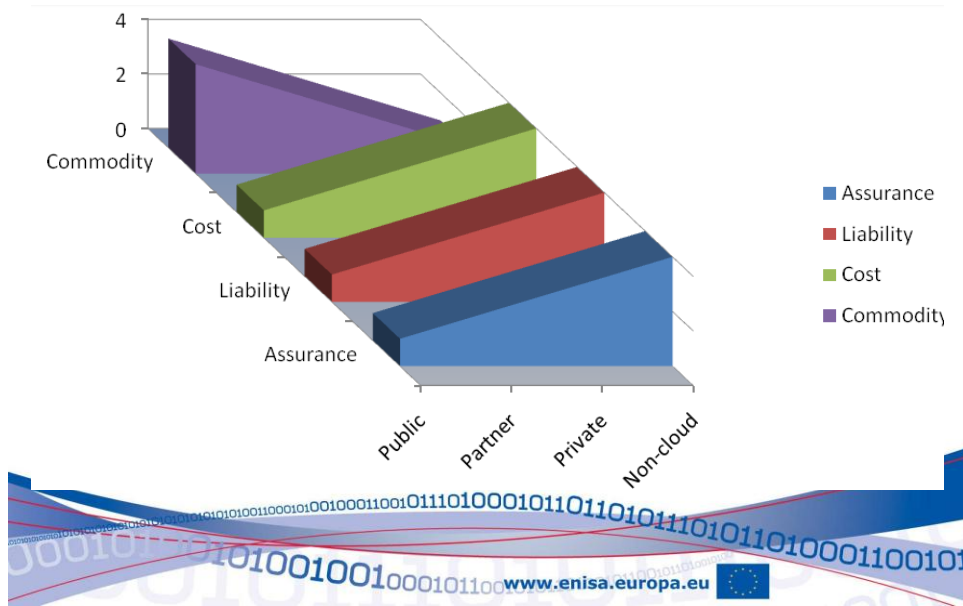


SME's: Main Concerns

	Not Important	Medium Importance	Very Important	Showstopper	Rating Average	Response Count
Privacy	0.0% (0)	12.3% (7)	43.9% (25)	43.9% (25)	3.32	57
Availability of services and/or data	1.8% (1)	10.9% (6)	47.3% (26)	40.0% (22)	3.25	55
Integrity of services and/or data	0.0% (0)	13.0% (7)	42.6% (23)	44.4% (24)	3.31	54
Confidentiality of corporate data	1.8% (1)	3.6% (2)	30.9% (17)	63.6% (35)	3.56	55
Repudiation	2.1% (1)	41.7% (20)	47.9% (23)	8.3% (4)	2.63	48
Loss of control of services and/or data	3.8% (2)	20.8% (11)	47.2% (25)	28.3% (15)	3.00	53
Lack of liability of providers in case of security incidents	2.0% (1)	25.5% (13)	43.1% (22)	29.4% (15)	3.00	51
Inconsistency between trans national laws and regulations	11.8% (6)	43.1% (22)	23.5% (12)	21.6% (11)	2.55	51
Unclear scheme in the pay per use approach	14.0% (7)	46.0% (23)	24.0% (12)	16.0% (8)	2.42	50
Uncontrolled variable cost	4.1% (2)	36.7% (18)	46.9% (23)	12.2% (6)	2.67	49
Cost and difficulty of migration to the cloud (legacy software etc...)	14.3% (7)	53.1% (26)	22.4% (11)	10.2% (5)	2.29	49
Intra-clouds (vendor lock-in) migration	8.3% (4)	37.5% (18)	35.4% (17)	18.8% (9)	2.65	48



General Perception of Clouds





Economy of Scale



Economies of scale and Security

- ★ All kinds of security measures, are cheaper when implemented on a larger scale.
 - ★ (e.g. filtering, patch management, hardening of virtual machine instances and hypervisors, etc)
- ★ The same amount of investment in security buys better protection.





Other benefits of scale

- ★ Timeliness of response to incidents
- ★ **Multiple locations** by default -> redundancy and failure independence.
- ★ **Edge networks:** content delivered or processed closer to its
- ★ **Staff specialization & experience**
Cloud providers big enough to hire specialists in dealing with specific security threats.



Rapid & smart scaling

The ability to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, to defensive measures (eg, against DDoS attacks) has obvious advantages for resilience





Improved management of updates and defaults

- ★ Updates can be rolled much more rapidly across a homogenous platform
- ★ Default VM images and software modules can be updated with the latest patches and security settings.
- ★ Snapshots of virtual infrastructure (in IaaS) to be taken regularly and compared with a security baseline.





WARNING!!

The impact of a threat in the Cloud can be amplified by resource concentration



Very high value assets

- ★ More Data in transit (Without encryption?)
- ★ Federated IdM/Authentication (can take down multiple systems)
- ★ Management interfaces – big juicy targets:





Very high value assets



- ★ Trustworthiness of insiders.
- ★ Hypervisors- hypervisor layer attacks on virtual machines are very attractive.
 - ★ No known compromise without access to the hypervisor at this time.
 - ★ BUT – any attacks on hypervisor (even internally) are extremely high impact.
 - ★ (See <http://invisiblethingslab.com/bh08/part3.pdf>)



Example Risks



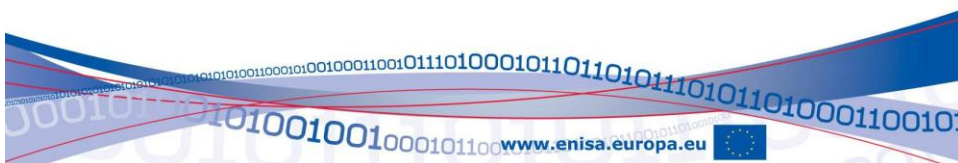


CAVEAT!!



Cloud-based defences can be more robust, scalable and cost-effective, but..

the massive concentrations of resources and data present a more attractive target to attackers



Lock in

- ★ Few tools, procedures or standard formats for data and service portability.
- ★ Difficult to migrate from one provider to another, or to migrate data and services to or from an in-house IT environment.
- ★ Potential dependency of service provision on a particular CP.





Loss of Governance

- ★ The client cedes control to the Provider on a number of issues effecting security:
 - ★ External pen testing not permitted.
 - ★ Very limited logs available.
 - ★ Usually no forensics service offered
 - ★ No information on location/jurisdiction of data.
 - ★ Outsource or sub-contract services to third-parties (fourth parties?)
- ★ SLAs may not offer a commitment to provide the above services, thus leaving a gap in security defences.



Isolation failure

- ★ Storage (e.g. Side channel attacks)
see <http://bit.ly/12h5Yh>
- ★ Virtual machines
- ★ Entropy pools
(<http://bit.ly/41sliN>)
- ★ Resource use (e.g. Bandwidth)





RESOURCE EXHAUSTION

★ Overbooking



Underbooking

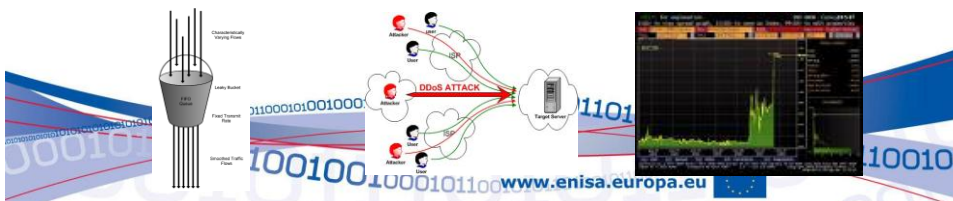


Caused by:

Resource allocation algos

Denial of Service

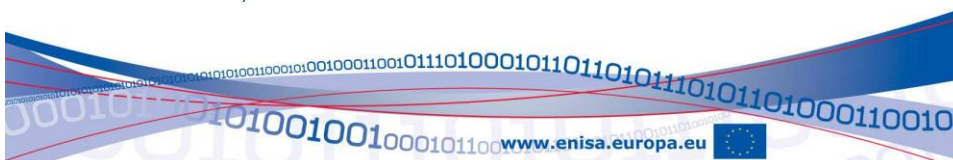
Freak events



Compliance Challenges



- ★ Cloud Provider cannot provide evidence of their own compliance to the relevant requirements.
 - ★ Cloud Provider does not permit audit by the Cloud Customer.
 - ★ In certain cases, using a cloud implies certain kind of compliance cannot be achieved
- therefore
- ★ cloud hosted services cannot be used (i.e. 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)





Supply Chain Failure

- ★ Cloud computing offer as a chain of specialised tasks (in-sourced or outsourced)
- ★ The level of security of chain depends on the level of security of each one of the links.
- ★ Interruption or corruption in the chain,
- ★ Lack of coordination
- ★ Services dependencies (i.e. Identify management)
- ★ Lack of transparency in the contract/ToU



Legal and contractual risks

- ★ **Lack of compliance with EU Data Protection Directive**
 - ★ Potentially difficult for the customer (data controller) to check the data handling practices of the provider
 - ★ Multiple transfers of data exacerbated the problem
- ★ **Data in multiple jurisdictions**, some of which may be risky..
- ★ **Subpoena and e-discovery**
- ★ **Risk Allocation and limitation of liability**
- ★ **Confidentiality and Non-disclosure**
- ★ **Intellectual Property**





Recommendations



Compare risks

Cloud Computing vs.
Traditional solutions.

Transfer the risk

however
not all risks can be transferred:
some damages can't be
compensated





Cloud Information Assurance Maturity Framework

A minimum baseline for:

- ★ **Comparing cloud offers**
- ★ **Assessing the risk to go Cloud**

(also to reduce audit burden)



Cloud Information Assurance Maturity Framework

An example

★ **Resource Provisioning**

- ★ What happens when too many people request resources?
- ★ Will I get my resource request?
- ★ What happens if I don't? Is there a lead time on service levels and changes in requirements?
- ★ How much can you scale up?
- ★ How fast can you scale up?
- ★ How do you handle seasonal effects?





Segregation of Responsibilities

- ★ Check WHO is responsible for WHAT!!!
 - ★ Do not assume your cloud provider encrypts your data.
 - ★ Identity Management System maintenance and management.
 - ★ Configuration Management (Firewall, IDS/IPS, etc)
 - ★ Patching
 - ★ Maintenance
 - ★ Logging
 - ★ etc



Contracts and ToU

- ★ Check contract clauses
 - ★ Intellectual property
 - ★ Confidentiality clause
 - ★ Cloud provider failure/ get-out clauses.
 - ★ Check outsourcing provisions.
- ★ Which legal jurisdictions apply to your data?
- ★ Understand the limited liability clause





Research recommendations

- ★ Certification processes & standards for clouds
- ★ Encrypted processing & Encrypted search
- ★ Maintaining state in live VM's
- ★ Key management
- ★ Load management and resource distribution



Government recommendations

- ★ Public clouds are (usually) not suitable for government applications.
- ★ Clearly define international differences in DP legislation.
- ★ Should there be breach notification requirements on cloud providers?
- ★ Automated means to mitigate problems with different jurisdictions.





The Penultimate Slide

Report available at:

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/>

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/>

<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey>

For more info:

daniele.catteddu@enisa.europa.eu

giles.hogben@enisa.europa.eu

philippe.massonet@cetic.be



The Final Slide



philippe.massonet@cetic.be

<http://www.cetic.be>

