

# ENISA – Cloud Computing Security Strategy

Dr Giles Hogben

European Network and Information Security Agency (ENISA)

# What is Cloud Computing?

---



Isn't it just old hat?

# What is cloud computing – ENISA's understanding

---

- Cloud computing is not a *new technology*.
- Cloud computing is a new business model
- It is a way of delivering computing resources

---

# 50,000 Machines for 1 Minute

cost ~ the same as

1 machine for 1 year

Overview

**Amazon EC2**

Navigation

> **EC2 Dashboard**

IMAGES & INSTANCES

> **Instances**

> **AMIs**

> **Bundle Tasks**

ELASTIC BLOCK STORE





> **Volumes**

> **Snapshots**

My Instances

 Launch Instances
  Reboot
  **Terminate**
 Connect
  Output
  Password

Viewing: All Instances  1 to 4 of 4

	Instance	AMI ID	Security Groups	Type	Status
<input checked="" type="checkbox"/>	 i-c4b829ad	ami-16cf287f	elasticbamboo	c1.medium	 running
<input checked="" type="checkbox"/>	 i-4b32a322	ami-2b5fba42	elasticbamboo	m1.small	 running
<input checked="" type="checkbox"/>	 i-4a35a423	ami-2b5fba42	elasticbamboo	m1.small	 running
<input checked="" type="checkbox"/>	 i-164cd87f	ami-8ffa1de6	elasticbamboo	m1.small	 running

Amazon EC2    Amazon Elastic MapReduce    Amazon CloudFront

### Navigation

**Region:** US-East ▾

- ▶ **EC2 Dashboard**
- INSTANCES
- ▶ **Instances**
- IMAGES
- ▶ **AMIs**
- ▶ **Bundle Tasks**
- ELASTIC BLOCK STORE
- ▶ **Volumes**
- ▶ **Snapshots**

### Amazon Machine Images

Launch
 Register New AMI
 De-register
 Permissions

**Viewing:** All Images ▾ All Platforms ▾

	AMI ID	Manifest
<input type="checkbox"/>	ami-0022c769	level22-ec2-images/ubuntu-7.04-feist
<input type="checkbox"/>	ami-005db969	alestic-64/ubuntu-8.04-hardy-base-64
<input checked="" type="checkbox"/>	ami-005dba69	rbuilder-online/new-example-1-x86_64
<input type="checkbox"/>	ami-005eba69	kaavo-ntier-db/imod-ntier-32bit-FC-DI
<input type="checkbox"/>	ami-00e70069	abami/image.manifest.xml
<input type="checkbox"/>	ami-0118fe68	citrix-c3-lab/XenApp5.0_32bit_v1.1.m
<input type="checkbox"/>	ami-0129cc68	cer-64-centos5_10-1/image.manifest.
<input type="checkbox"/>	ami-0146e169	repositio-edge-2.14-ec2-public-ami

```

c:\ec2\bin>ec2-authorize default -p 3389 -s 62.158.114.177/32
GROUP          default
PERMISSION     default  ALLOWS  tcp     3389    3389    FROM    CIDR
62.158.114.177/32

c:\ec2\bin>ec2-describe-instances i-f779c59e
RESERVATION    r-5d52f134    193138642160    default
INSTANCE       i-f779c59e    ami-e3698d8a    ec2-67-202-27-255.compute-1.amaz
onaws.com      domU-12-31-39-02-4D-C1.compute-1.internal    running  gsg-keyp
air            0            m1.small        2008-12-06T11:41:46+0000    us-east-
ia            windows

c:\ec2\bin>ec2-terminate-instances i-f779c59e
INSTANCE       i-f779c59e    running shutting-down

c:\ec2\bin>ec2-describe-instances i-f779c59e
RESERVATION    r-5d52f134    193138642160    default
INSTANCE       i-f779c59e    ami-e3698d8a    terminated
gsg-keypair    0            m1.small        2008-12-06T11:41:46+0000
                windows

c:\ec2\bin>
c:\ec2\bin>ec2-describe-images -o self -o amazon ! findstr /i windows
IMAGE         ami-e3698d8a    ec2-public-windows-images/Server2003r2-i386-Win-v1.02.ma
public        i386          machine         windows
IMAGE         ami-e5698d8c    ec2-public-windows-images/Server2003r2-i386-WinAuth-v1.0
public        i386          machine         windows
IMAGE         ami-ed698d84    ec2-public-windows-images/Server2003r2-x86_64-Win-v1.02.
public        x86_64       machine         windows
IMAGE         ami-ec698d85    ec2-public-windows-images/Server2003r2-x86_64-WinAuth-v1
public        x86_64       machine         windows
IMAGE         ami-e4698d8d    ec2-public-windows-images/SqlSvrExp2003r2-i386-Win-v1.02
public        i386          machine         windows
IMAGE         ami-e7698d8e    ec2-public-windows-images/SqlSvrExp2003r2-i386-WinAuth-v
public        i386          machine         windows
IMAGE         ami-ef698d86    ec2-public-windows-images/SqlSvrExp2003r2-x86_64-Win-v1.
public        x86_64       machine         windows
IMAGE         ami-ee698d87    ec2-public-windows-images/SqlSvrExp2003r2-x86_64-WinAuth
public        x86_64       machine         windows
IMAGE         ami-e1698d88    ec2-public-windows-images/SqlSvrStd2003r2-x86_64-Win-v1.
public        x86_64       machine         windows
IMAGE         ami-e0698d89    ec2-public-windows-images/SqlSvrStd2003r2-x86_64-WinAuth
public        x86_64       machine         windows

c:\ec2\bin>ec2-describe-images -o self -o amazon ! findstr /i windows

```

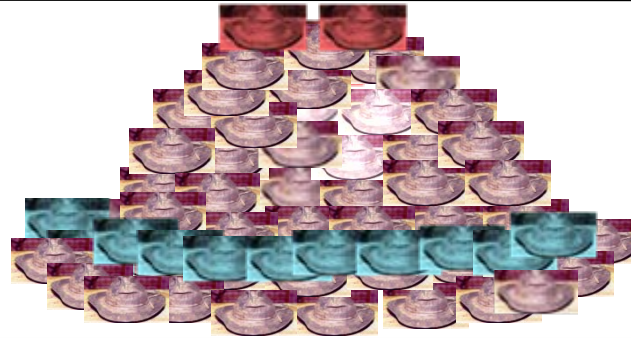


# What is cloud computing – ENISA's understanding

---

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





	US – N. Virginia	US – N. California	EU – Ireland
<b>Standard On-Demand Instances</b>		<b>Linux/UNIX Usage</b>	<b>Windows Usage</b>
Small (Default)		\$0.095 per hour	\$0.12 per hour
Large		\$0.38 per hour	\$0.48 per hour
Extra Large		\$0.76 per hour	\$0.96 per hour
<b>High-Memory On-Demand Instances</b>		<b>Linux/UNIX Usage</b>	<b>Windows Usage</b>
Extra Large		\$0.57 per hour	\$0.62 per hour
Double Extra Large		\$1.34 per hour	\$1.44 per hour
Quadruple Extra Large		\$2.68 per hour	\$2.88 per hour
<b>High-CPU On-Demand Instances</b>		<b>Linux/UNIX Usage</b>	<b>Windows Usage</b>
Medium		\$0.19 per hour	\$0.29 per hour
Extra Large		\$0.76 per hour	\$1.16 per hour

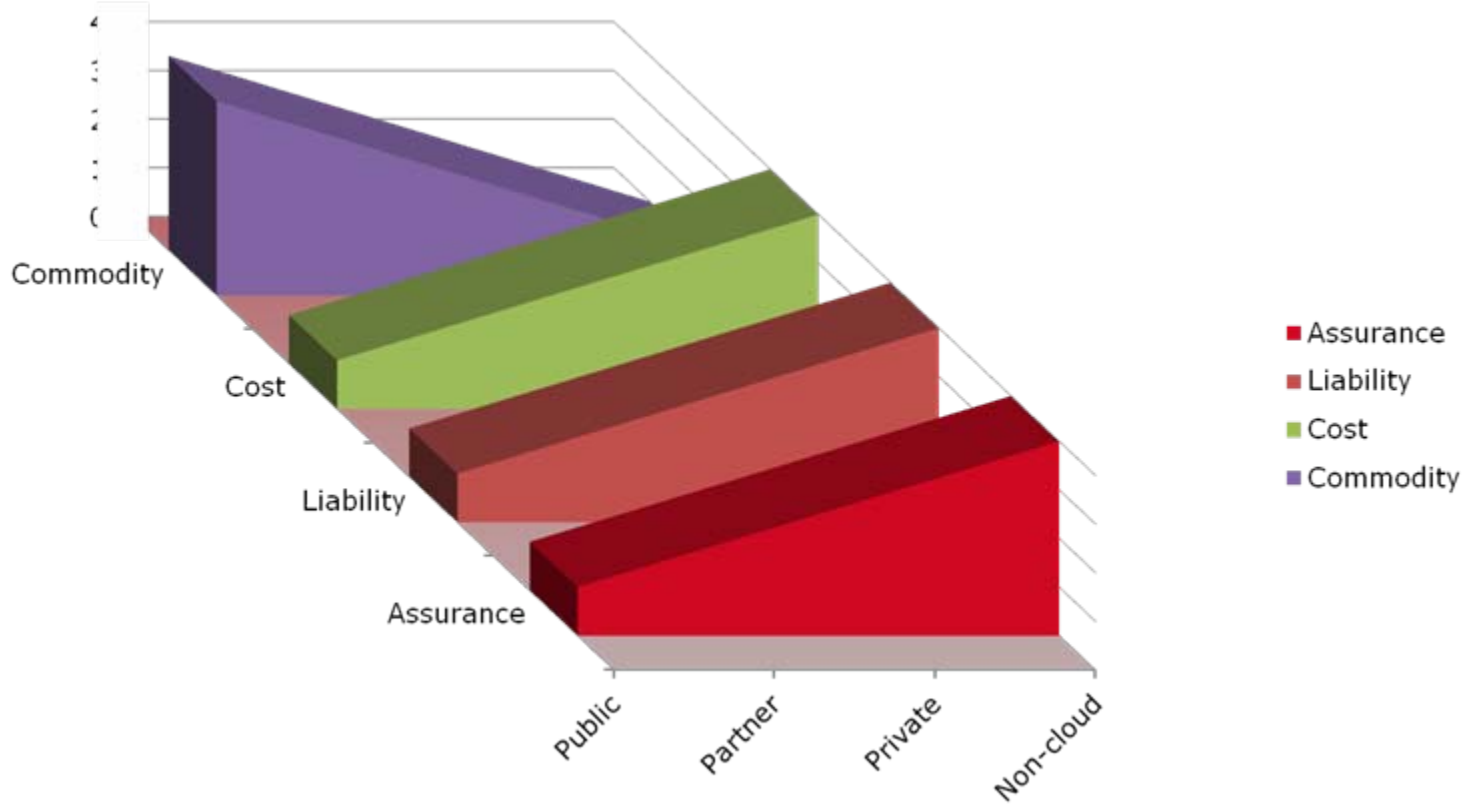
Which you can rent by the hour



Server Size	Disk	Bandwidth Limit	Hourly Charge
512MB	20GB	20 Mps	\$0.04
1GB	40GB	30 Mps	\$0.08
2GB	80GB	40 Mps	\$0.16
4GB	160GB	50 Mps	\$0.32
8GB	320GB	60 Mps	\$0.58
15.5GB	620GB	70 Mps	\$1.08

Which can resize (up and down) to your requirements

# Types of cloud



# What is cloud computing – ENISA's understanding

---

- Cloud computing is a new business model
  - It is a way of delivering computing resources
- Cloud computing is not a *new technology*.

# ENISA Cloud Computing Objectives

---

Help business and governments to gain the cost benefits of cloud computing.



While avoiding exposure to excessive NIS risks.

# Reaching the objectives

---

## ENISA Deliverables and Ongoing Activities

- Cloud Computing: Benefits, Risks and Recommendations for Information security 2009

<http://is.gd/cem9H>

- Assurance framework 2009
- Research Recommendations 2009
- Common Assurance Maturity Model (CAMM) consortium 2010
- Gov-cloud security and resilience analysis (2010)
- 2011 (proposed) procurement and monitoring guidance for government cloud contracts.

# Cloud Computing: Benefits, Risks and Recommendations for Information security





# Security Benefits

# 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

---

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

# Improved management of updates and defaults

---

- **Updates** can be rolled out 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.

# The Risks



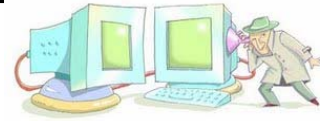
# Very high value assets

- Most risks are not new, but they are amplified by resource concentration
  - Trustworthiness of insiders.
  - Hypervisors - hypervisor layer attacks on virtual machines are very attractive.
  - More Data in transit (Without encryption?)
  - Management interfaces – big juicy targets



# Isolation failure

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



# RESOURCE EXHAUSTION

## o Overbooking

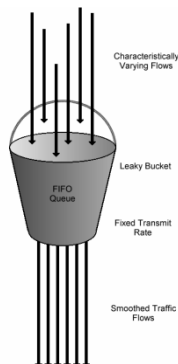


## Underbooking

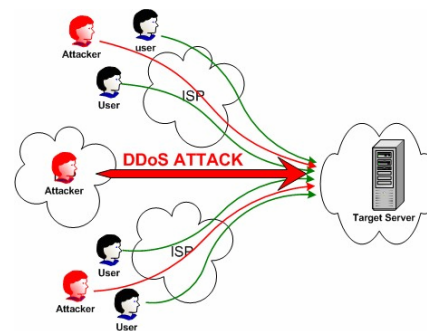


## Caused by:

### Resource allocation algos



### Denial of Service



### Freak events



# Key management

---

- Key management is (currently) the responsibility of the cloud customer.
- Key provisioning and storage is usually off-cloud
- One key-pair per machine – doesn't scale to multiple account holders/RBAC.
- Credential recovery sometimes available through management interface (protected by UN/PWD by)
- Copies of VM images may contain keys if not well-managed.



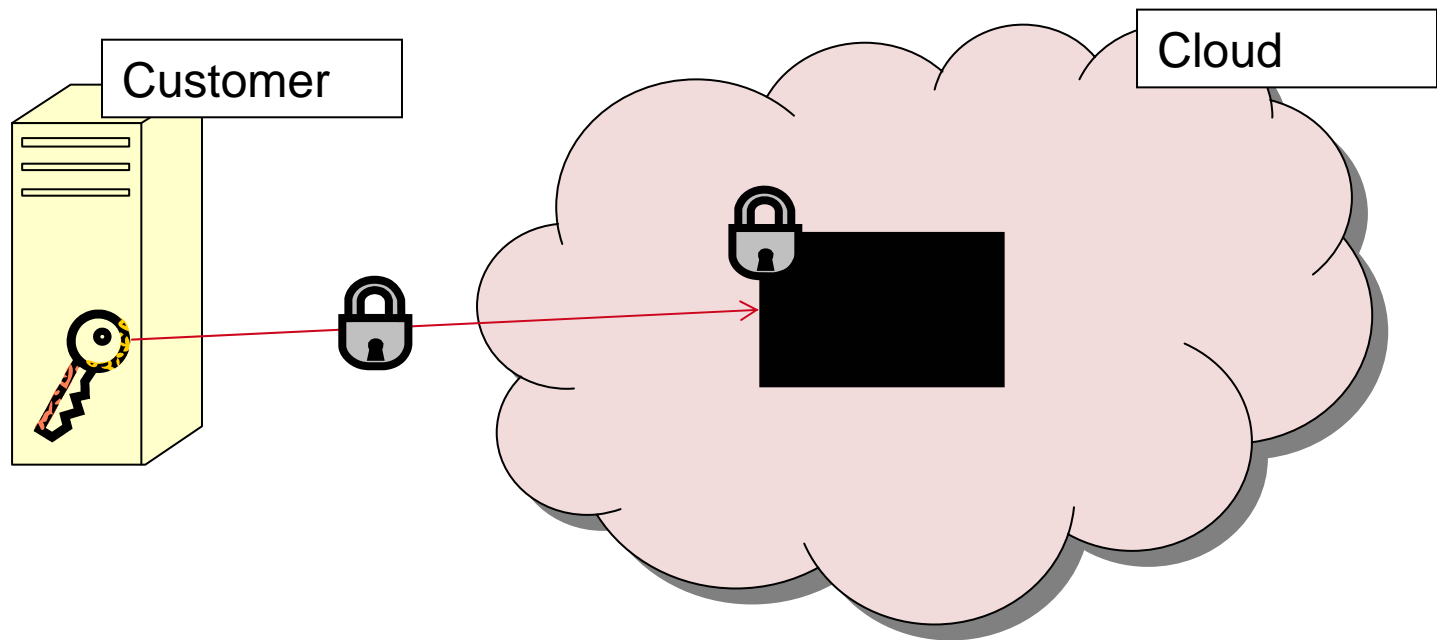
# Key management 1

---

- Key storage and provisioning almost impossible to do on-cloud with current technologies
  - HSM's don't scale to the cloud
  - PKCS#10,11 don't talk cloud
  - Revocation is even more complicated.

# Encryption: Data must be processed in cleartext (most operations).

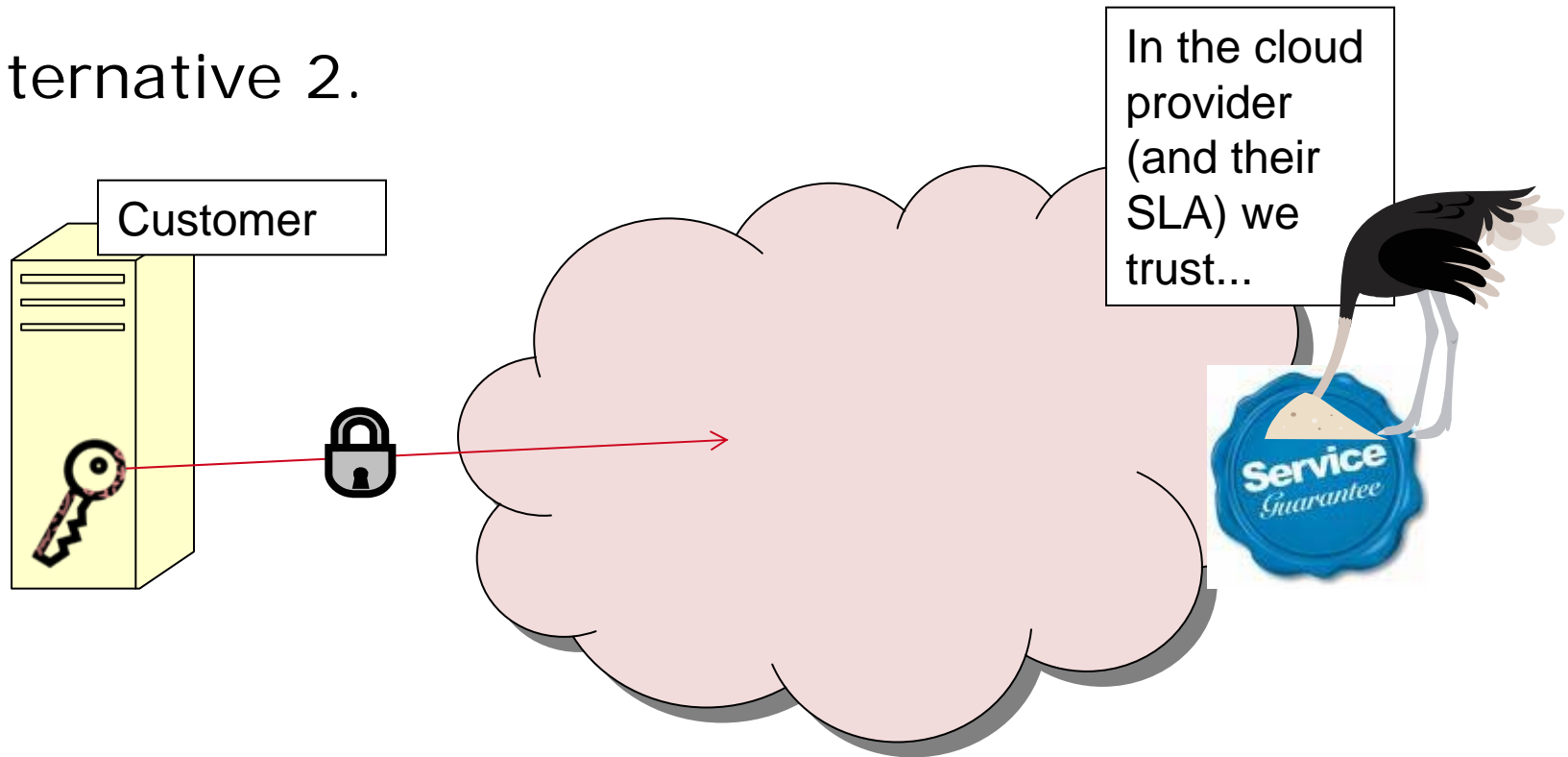
- Alternative 1. – HARD TO IMPLEMENT!



**=> If you want to do anything useful with cloud computing, you have to trust the provider.**

# Data storage and processing without security guarantees?

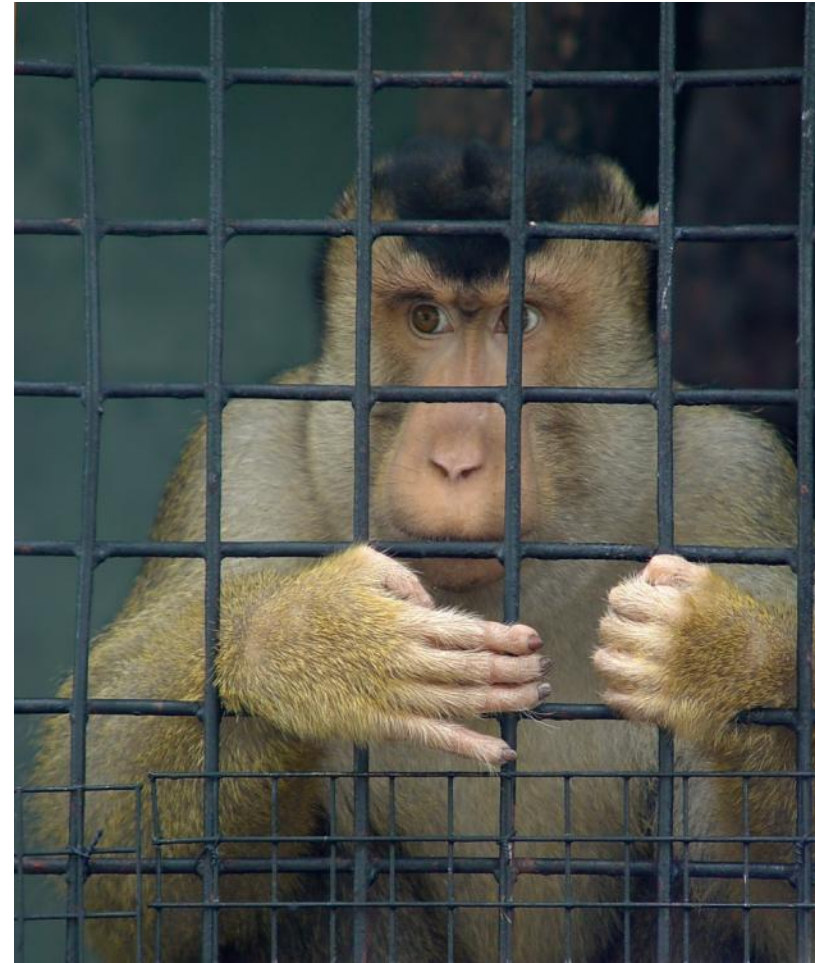
- Alternative 2.



Trust the cloud provider

# 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 e.g.:
  - 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?)



# 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**

# Somebody else's problem (SEP) syndrome

---

*"Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there, it is protected by the same strong security mechanisms that protect thousands of customers using Amazon's services"* (Thanks to Craig Balding, cloudsecurity.org for spotting this)

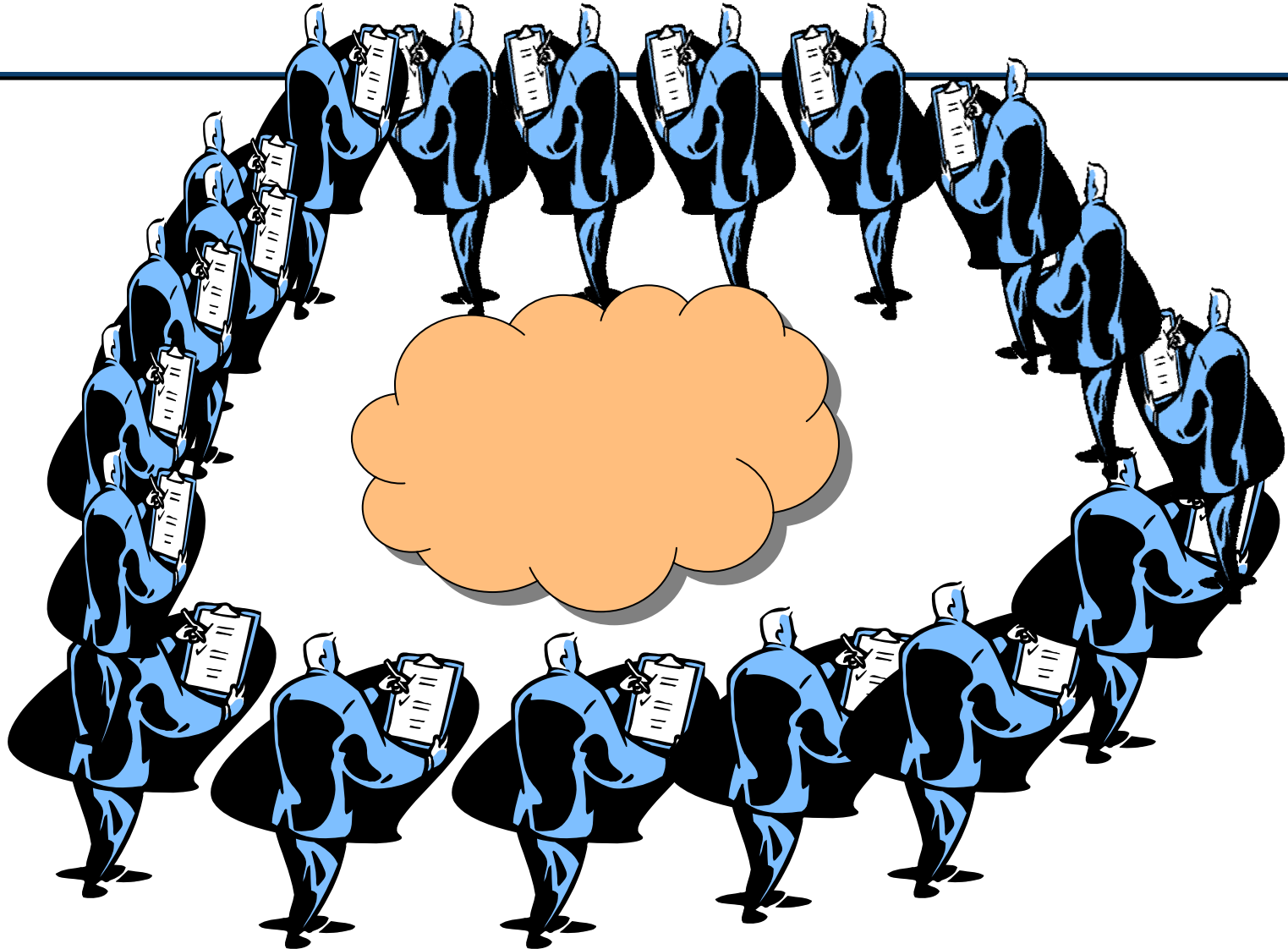
- “YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA.”
- *“You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you.”*

# 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

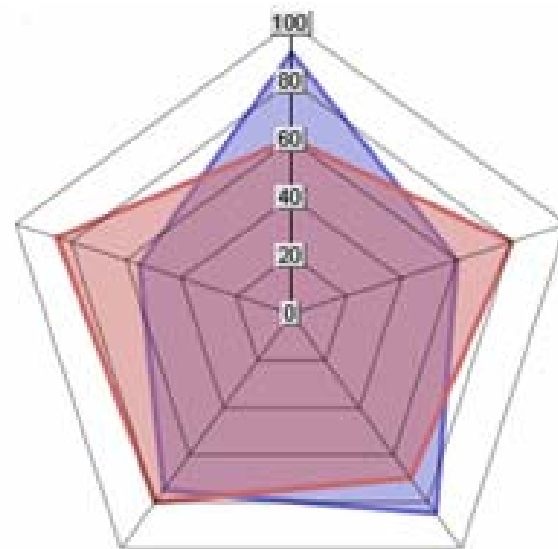
# Assurance Overload



# Common Assurance Maturity Model (CAMM)

A minimum baseline for:

- Comparing cloud (and 3<sup>rd</sup> party) offers
- Assessing the risk to go Cloud
- Reducing audit burden and security risks



# Common Assurance Maturity Model (CAMM)

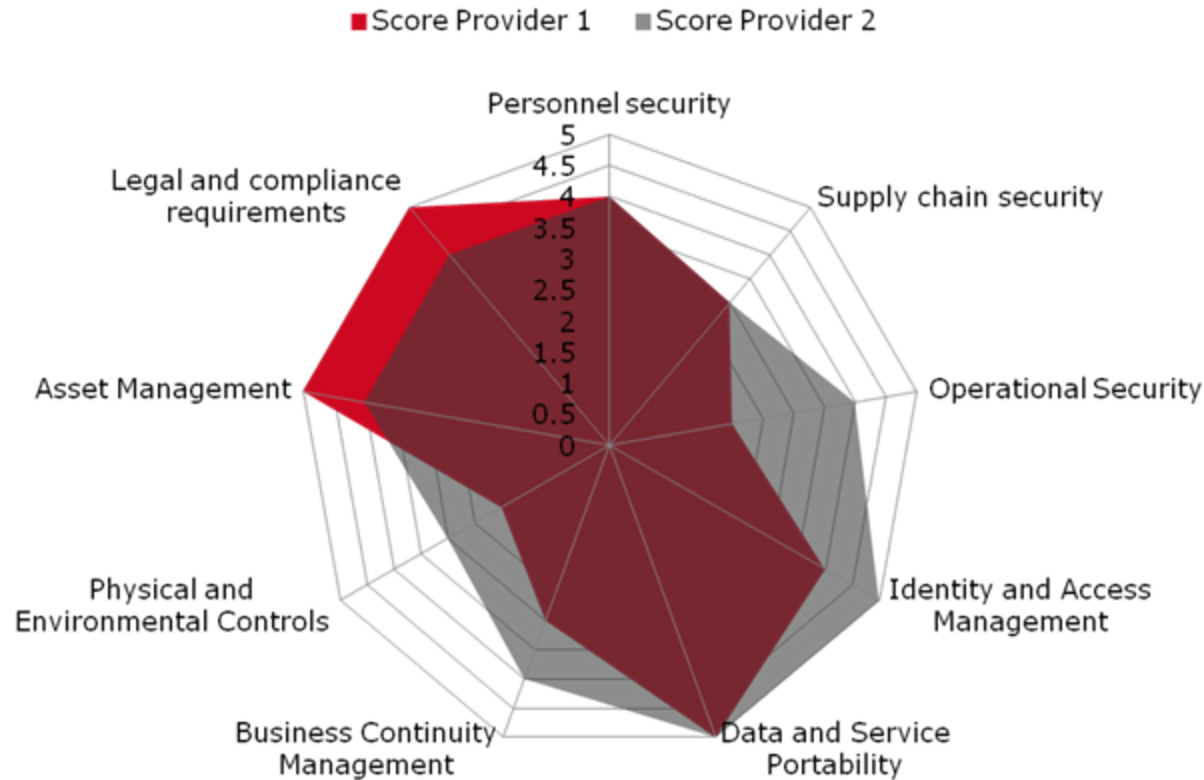
---

## An example

- **Network architecture controls**
- Well-defined controls are in place to mitigate DDoS (distributed denial-of-service) attacks e.g.
  - Defence in depth (traffic throttling, packet black-holing, etc..)
  - Defences are in place against 'internal' (originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks.
- Measures are specified to isolate resource usage between accounts for virtual machines, physical machines, network, storage (e.g., storage area networks), management networks and management support systems, etc.
- The architecture supports continued operation from the cloud when the customer is separated from the service provider and vice versa (e.g., there is no critical dependency on the customer LDAP system).

# 2010 – CAM framework aims at provider benchmarking on security

## Provider Comparison Chart



# Governments and the Cloud



- Gov Agencies and Public Organizations around the globe are moving non-critical applications towards a "cloud approach".
- Some governments (e.g. Korea) are even offering public cloud infrastructure as an innovation platform.
- In Europe we have some fast adopters, i.e. Denmark and UK, announcing/planning to move into the cloud.



## Inside the G-Cloud: Whitehall's grand cloud computing plan unveiled

Government CIO on adding SaaS to public sector IT

5 Comments | Print

By Nick Heath, [28 January 2010 12:40](#)

**NEWS** An ambitious project to create a secure government aiming to slash hundreds of millions of pounds from public

### DK: Public discussion in implementing cloud computing services in the Danish public sector

☆☆☆☆☆

1521 Visits

Posting Date 5 August 2009

Last Edited Date 17 August 2009

Country Denmark

Domain eGovernment

Topic Efficiency & Effectiveness, Benchmarking | Services for Citizens | Infrastructure | User-centric Services

Submitted By ePractice Editorial Team (EUROPEAN DYNAMICS SA) | Belgium

cloud computing | infrastructure | policy | eservice | citizen | user-centric | modernisation | Strategy | interoperability | eParticipation | data-protection

In July 2009, the [Local Government Denmark \(KL\)](#) along with the [National IT and Telecom Agency](#) launched a debate on the potential use of cloud computing services in the public sector. The [public discussion](#) will primarily focus on the benefits as well as the obstacles in implementing cloud computing in the Danish public sector.

 U.S. General Services Administration

WHAT GSA OFFERS

[Buildings & Real Estate](#)

[Products & Services](#)

[Policy & Regulations](#)

DOING BUSINESS WITH GSA

[Purchasing Programs](#)

[Real Estate Services](#)

LEARN MORE

[How We Help](#)

[About](#)

[Home](#) > [Newsroom](#) > [News Releases](#) > [Obama Administration Launches GSA Cloud Storefront](#)

## Obama Administration Launches GSA Cloud Storefront Apps.gov

GSA's *USA.gov* showcased as government using technology smarter, better, and faster

GSA # 10634

# 2010-11 – Supporting EU Governments in Cloud Migration

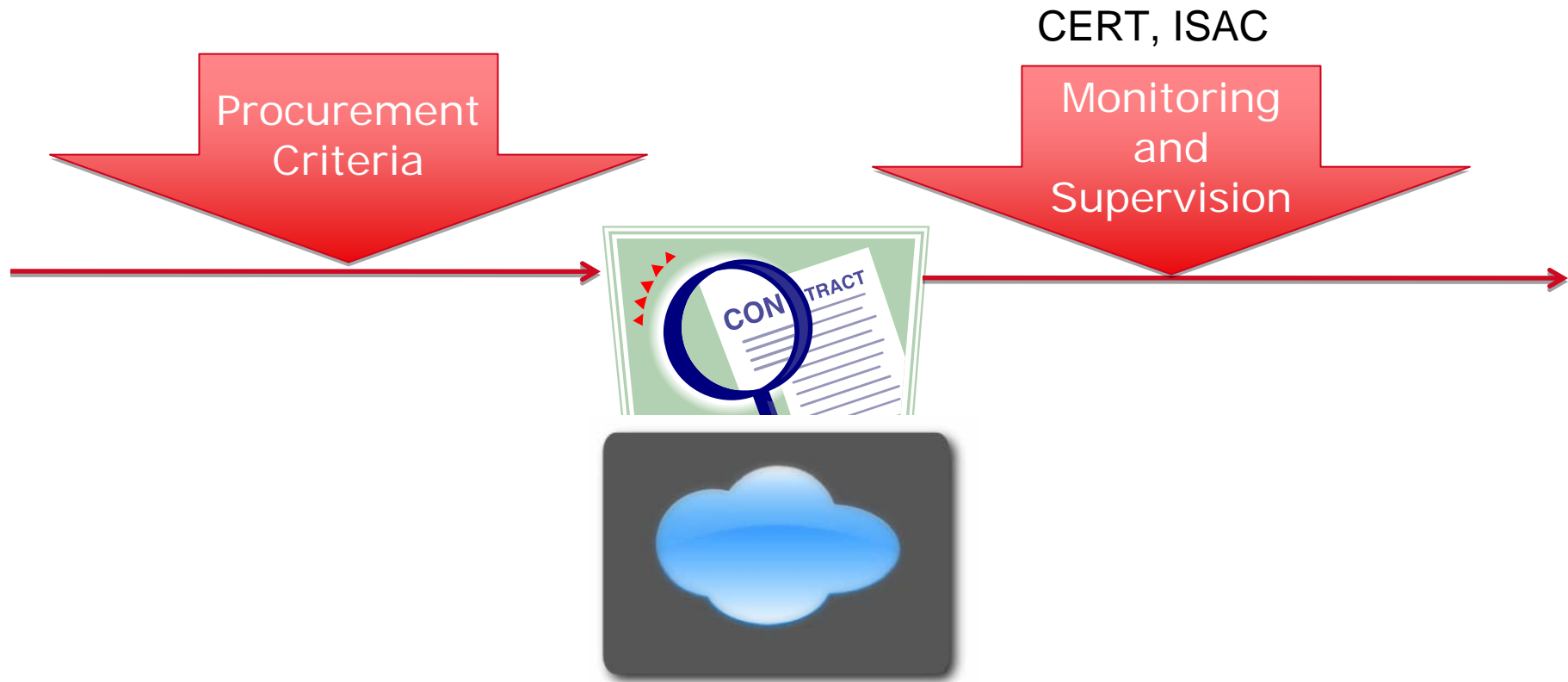
## Government towards the Cloud: impact on service security & resilience

ENISA aims to:

- ✓ **analyze and evaluate** the impact of cloud computing on the **resilience** and **security** of GOV services.
- ✓ **provide recommendations** and good practices for European Members State planning to migrate to cloud computing .



# 2011 – procurement and monitoring guidelines



# Conclusions

---

- Cloud computing *can* represent an improvement in security for non-critical applications and data.
- But transparency is crucial: customers must be given a means to assess and compare provider security practices
- Much more effort is required to achieve security levels required for higher assurance applications in the cloud
- For once we can build security in by design, let's not miss the chance

## Contact

Dr Giles Hogben  
Secure Services Programme Manager

European Network and Information Security Agency

Giles.hogben@enisa.europa.eu  
[www.enisa.europa.eu](http://www.enisa.europa.eu)