Opportunities and Risks in Governmental Cloud Computing

Udo Helmbrecht

Executive Director

European Network and Information Security Agency

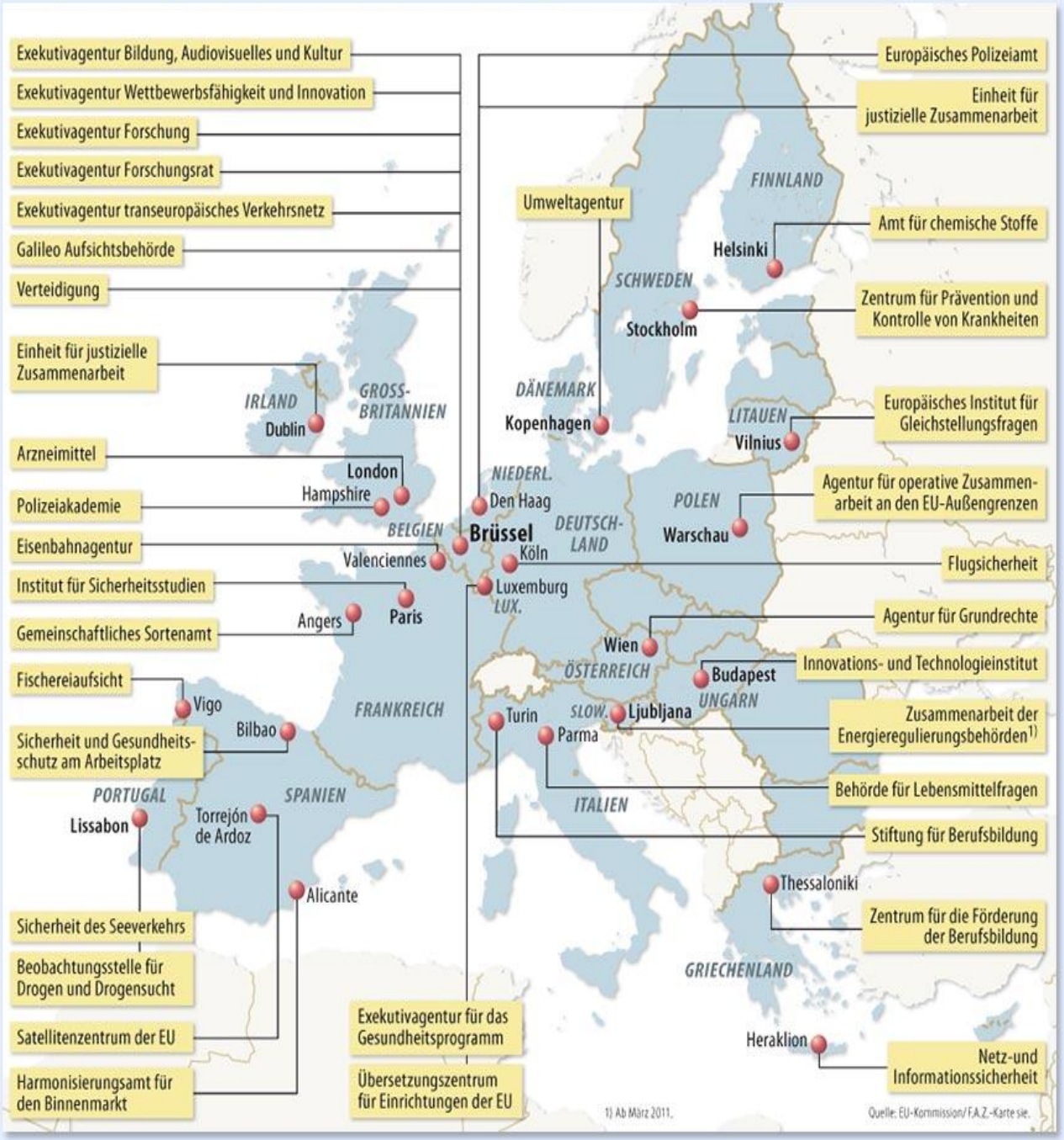
Agenda

- ENISA
- Two dimensions of Cloud computing
- Cloud promises and opportunities and some of their security aspects
- Cloud risks from the ENISA Cloud Computing Risk Assessment study
- A look at special requirements of Governmental information processing
- Conclusions

Commissioners

Commissioner	 Neelie **Kroes** **Vice-President** Digital Agenda	 Cecilia **Malmström** Home Affairs	 Viviane **Reding** **Vice-President** Justice, Fundamental Rights and Citizenship
Directorate-General	**Communications Networks, Content and Technology (DG CONNECT)**	**Home (DG HOME)**	**Justice(DG JUST)**
Agencies	**ENISA**	**FRONTEX** **EUROPOL** **CEPOL** **EMCDDA** **EASA**	**EUROJUST** **FRA (Fundamental Rights)**

Europäische Agenturen und andere Einrichtungen

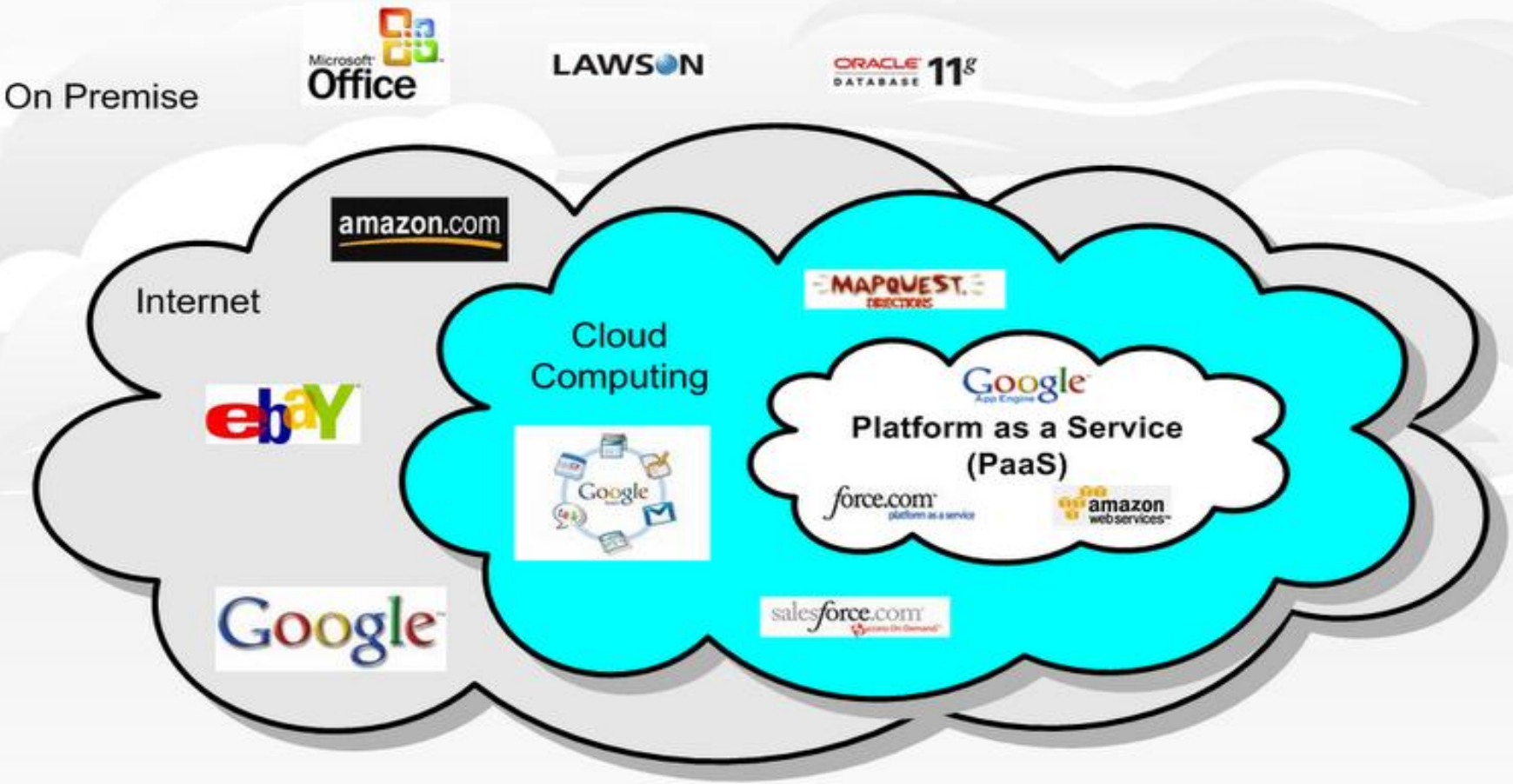


Quelle:
FAZ 2010

About ENISA

- The European Network and Information Security Agency
  - gives advice on information security issues
  - to national authorities, EU institutions, citizens, businesses
  - acts as a forum for sharing good NIS practices
  - facilitates information exchange and collaboration
- ENISA focuses on prevention and preparedness
- Set up in 2004 – mandate to be extended later this year
- Around 65 staff
- Offices in Greece: Branch Office Athens and Seat Heraklion, Crete

Cloud Computing



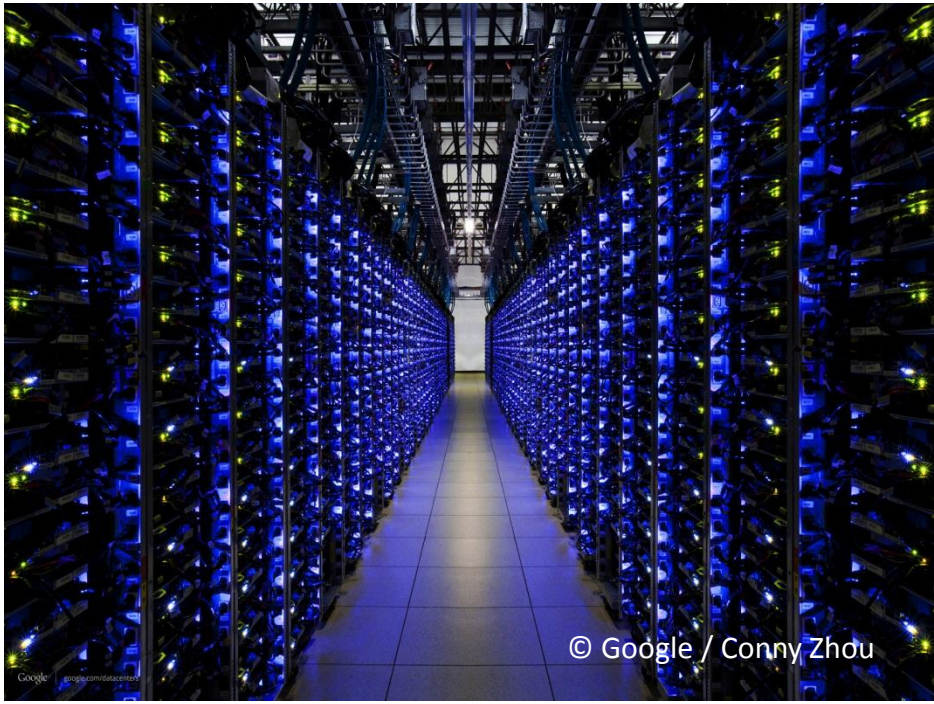
http://www.princeton.edu/~ddix/cloud-computing.html

Cloud Computing is a Business Model

- Cloud computing is a business model – a way of providing IT services.
- Characteristics are
  - Highly standardized services
  - Highly standardized SLAs
- Using such a service is outsourcing
- Cloud SLAs are usually much more standardized than in other outsourcing contracts

Cloud Computing is a Deployment Model

- Cloud computing is a deployment model
- Information processing
  - In a shared environment
  - using shared computing resources
- Resources can be quickly scaled to meet changed demand
- Cloud deployments are usually much more standardized and automated than legacy IT



Cloud opportunities

- Cloud computing makes some important promises with important security aspects
- Security is often cited as a barrier to adopting Cloud
- On the other hand, Cloud computing has the potential to greatly improve the resilience of electronic services

Cloud Computing is “Green”

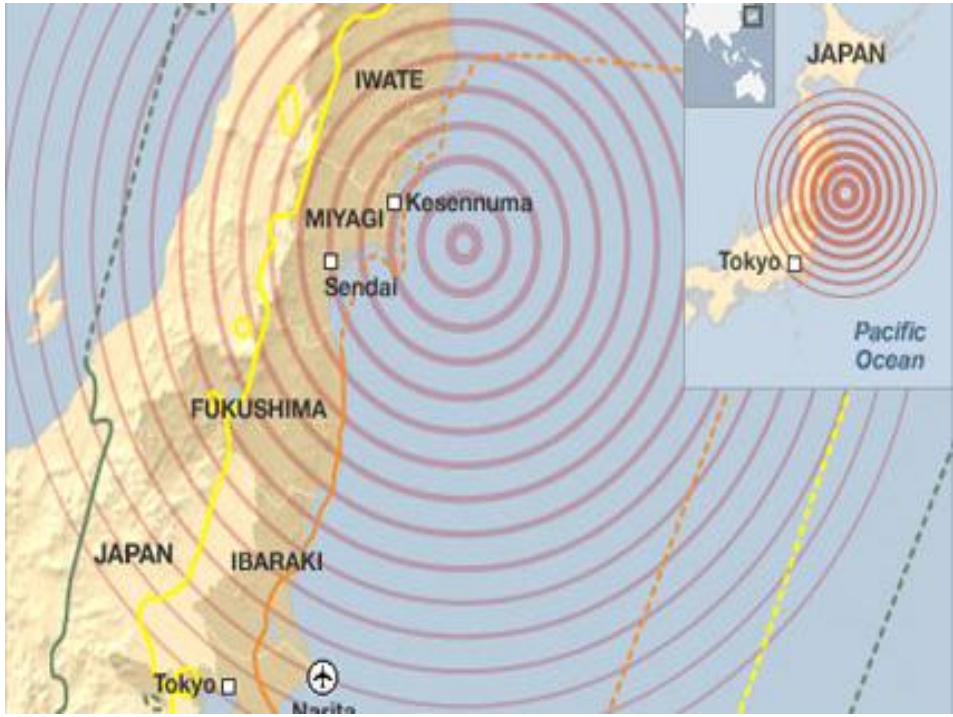
- Cloud computing is “green”: available resources are used much more efficiently
- Legacy IT is not “green” at all – most servers are idle most of the time
- More efficient resource utilization also means cost savings

Cloud Computing Leverages Economies of Scale

- Economies of scale mean a better return on investment
- Economies of scale apply also to investments in security
- Cost of security and resilience measures is spread across customers
- On the other hand, sharing resources requires sufficient isolation
- If isolation fails, large amounts of data are in danger

Cloud Computing is Resilient

- Great example: the 2011 earthquake and tsunami in Japan
- None of the Cloud datacentres in the region went down, while legacy IT did!
- Rescue efforts relied for large part on Cloud resources
- Social networks were used for communication
- Government later advised businesses to stay in the Cloud and not to return to legacy deployments



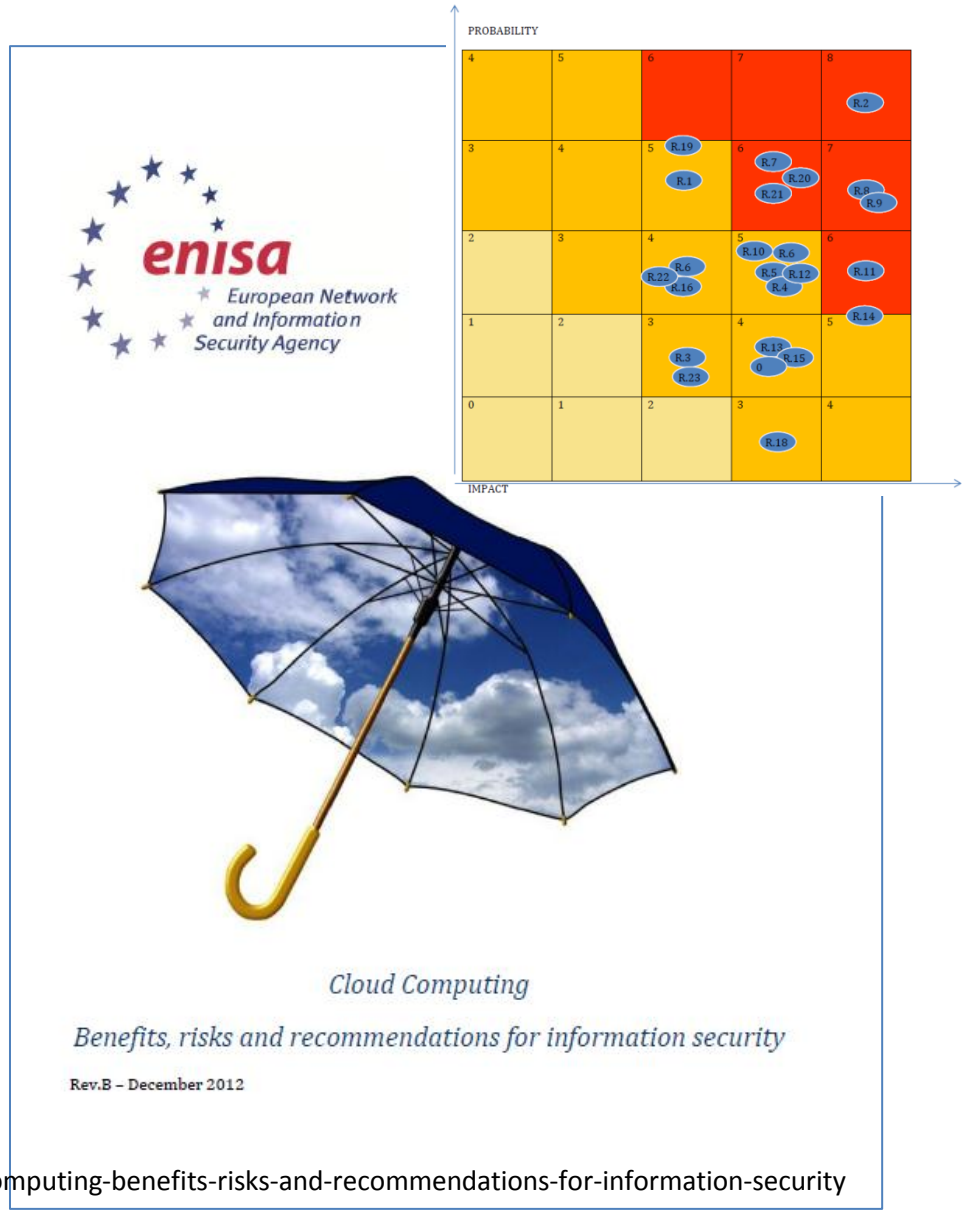
Source: https://cloudsecurityalliance.org/wp-content/uploads/2012/07/Day1_1645_Track1_Session_KatsumiBen_-_IncMan_Katsumi_Ben.pptx

Cloud Risks

- Cloud computing also brings new or changed risks
- Changes in the risk structure will vary between different Cloud users

ENISA's Cloud Risk Assessment

- First assessment of Cloud computing risks published 2009, still widely quoted
- A revision in 2012 concluded that the main risks haven't changed too much
- Risk assessment from the point of view of a single entity (e.g. a SME)
- Most findings apply also to the Governmental IT case
- The Cloud model considered was primarily "Public cloud"
- "Private" and "Community" clouds have different risk profiles



https://resilience.enisa.europa.eu/cloud-security-and-resilience/cloud-computing-benefits-risks-and-recommendations-for-information-security

Top 3 Technical Risks

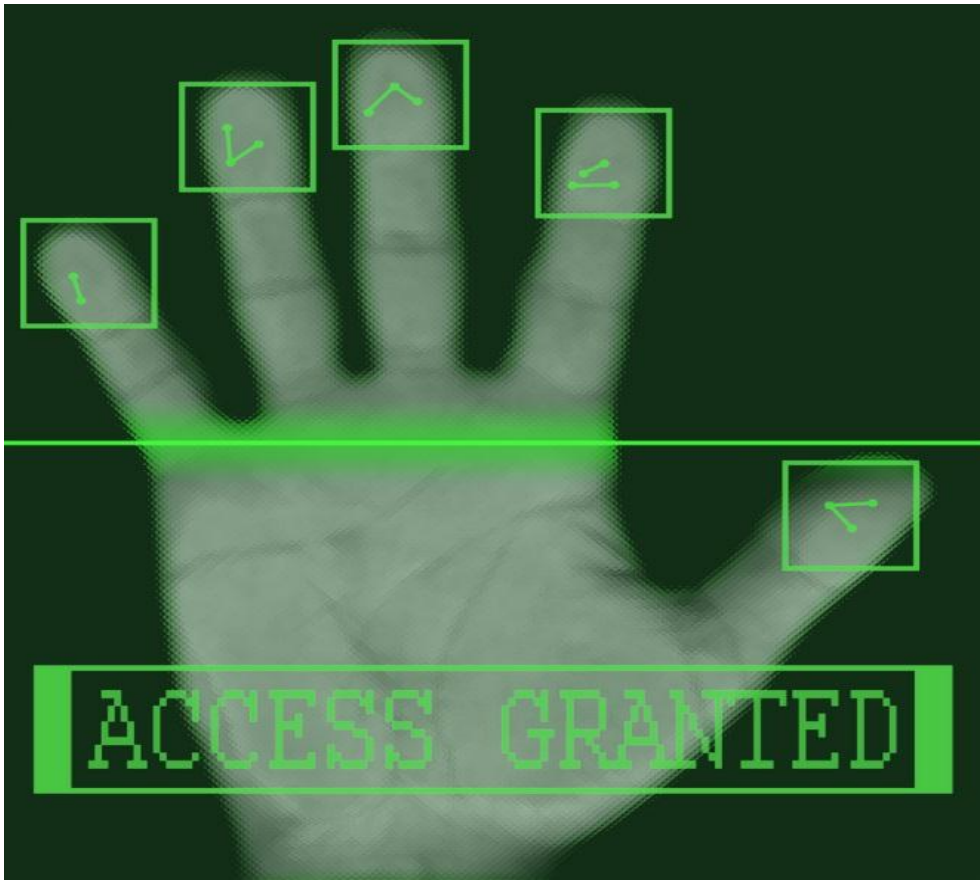
- Isolation failure
- Management interface compromise
- Abuse of high privilege roles

Isolation Failure

- Sharing resources means logical isolation is necessary
- If isolation fails, data and resources can be accessed by others, or even everybody
- There have been numerous incidents in the past, involving practically every well-known Cloud provider

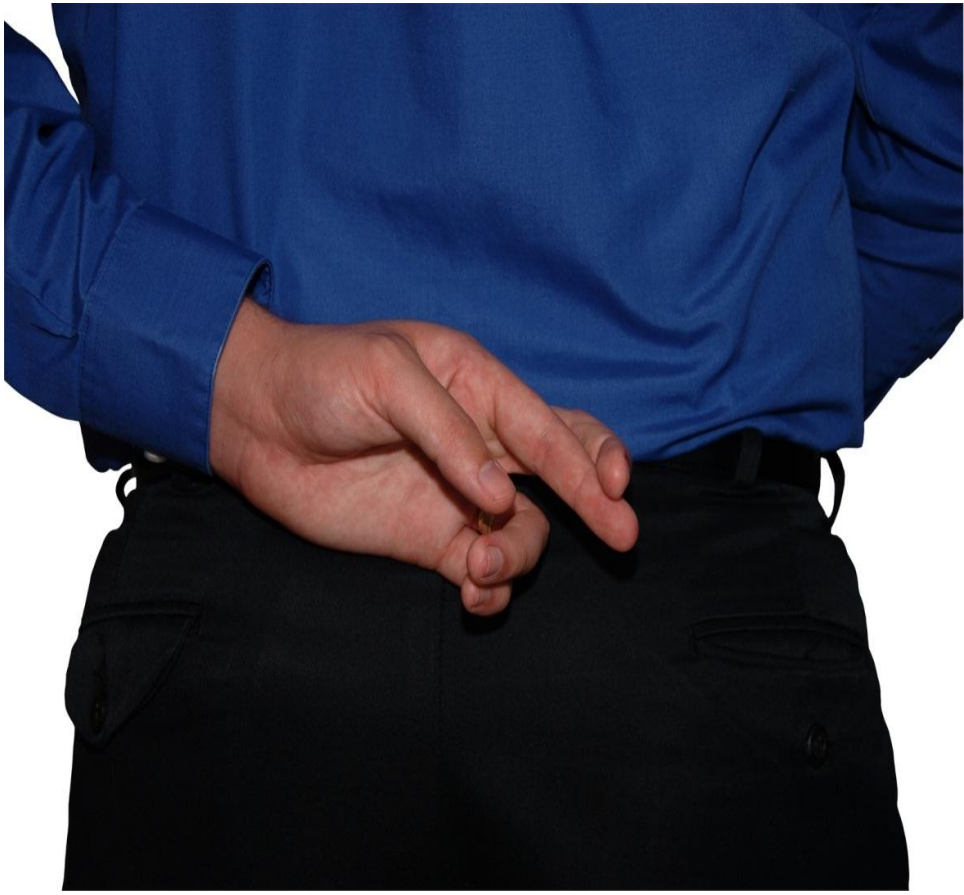
Management Interface Compromise

- Management interfaces of Cloud services have to be accessible from outside
- Identity and access management are particularly important
- Compromising the management interface of a Cloud service means full access to all resources
- Not just holding the keys to the kingdom, but to many kingdoms



Abuse of High Privilege Roles

- Abuse of high privilege roles at the Cloud provider can cause a lot more damage than for a single isolated legacy service
- Auditing and reporting weaknesses can lead to additional damage
- Employees of Cloud providers might become targets of blackmailing attacks



Top 3 Non-technical Risks

- Loss of governance
- Data protection
- Changes of jurisdiction

Loss of Governance

- The Cloud customer necessarily cedes some amount of control to the Cloud provider
- Transfer of control can also affect security
- Examples include:
  - Conflicts between Cloud environment and Customer's security measures
  - Sub-contracting by the Cloud provider
  - Changes in the provider's business strategy, or acquisition of the provider
  - Terms of usage may prohibit certain security techniques

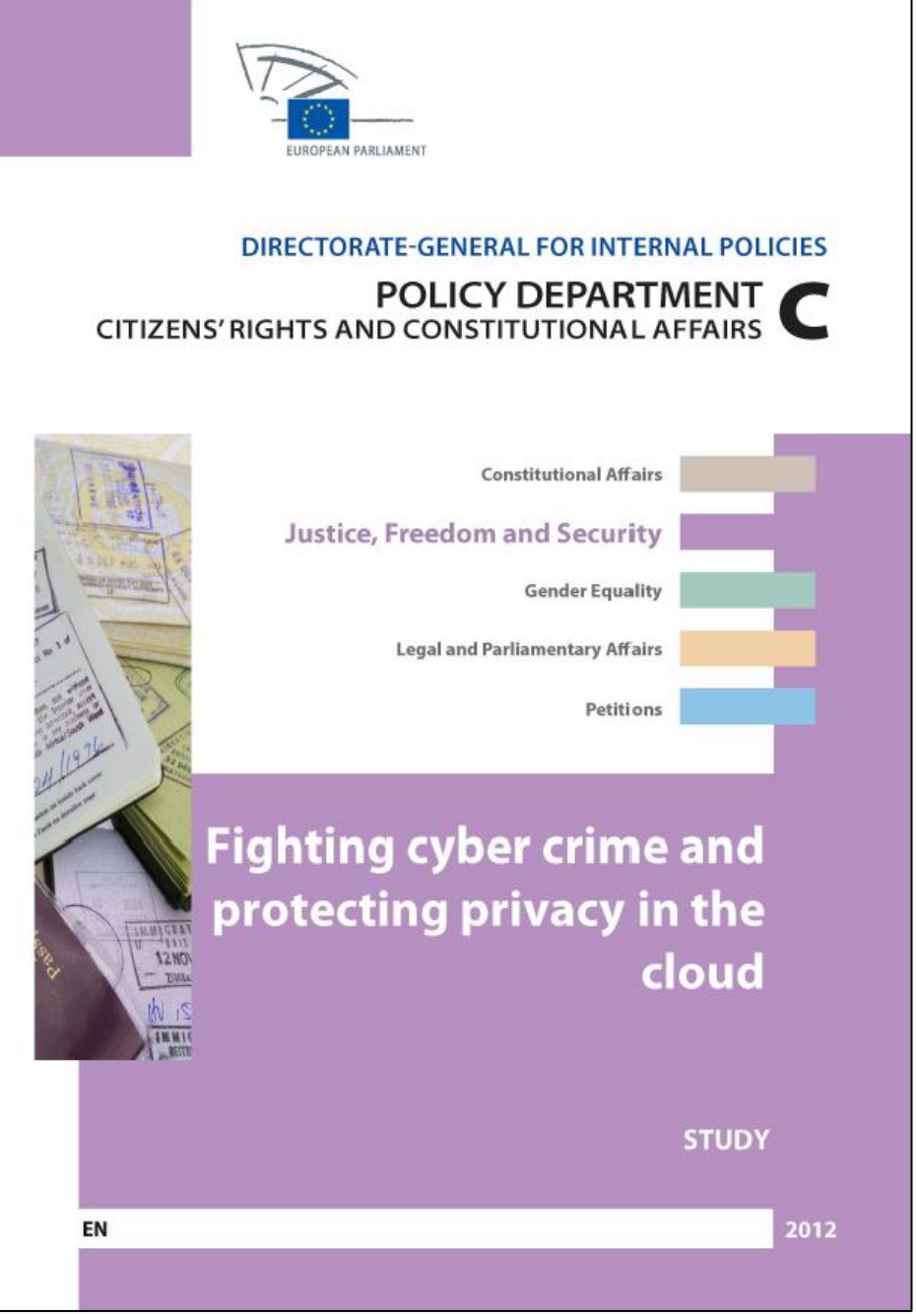
Data Protection

- The Cloud provider usually becomes data processor in terms of DP legislation
- Data processing in datacentres abroad can imply that certain DP requirements cannot be met in the Cloud
- Large differences in DP legislation pose big problems especially in case of processing in non-EU countries

Changes in Jurisdiction

- If a provider's datacentre is located in another country (even within the EU), different legal frameworks apply
- Examples include
  - Seizure of data or disruptions of service for reasons that don't exist in the customer's country
  - Copyright issues when certain content is processed abroad
  - National security interests of the hosting country

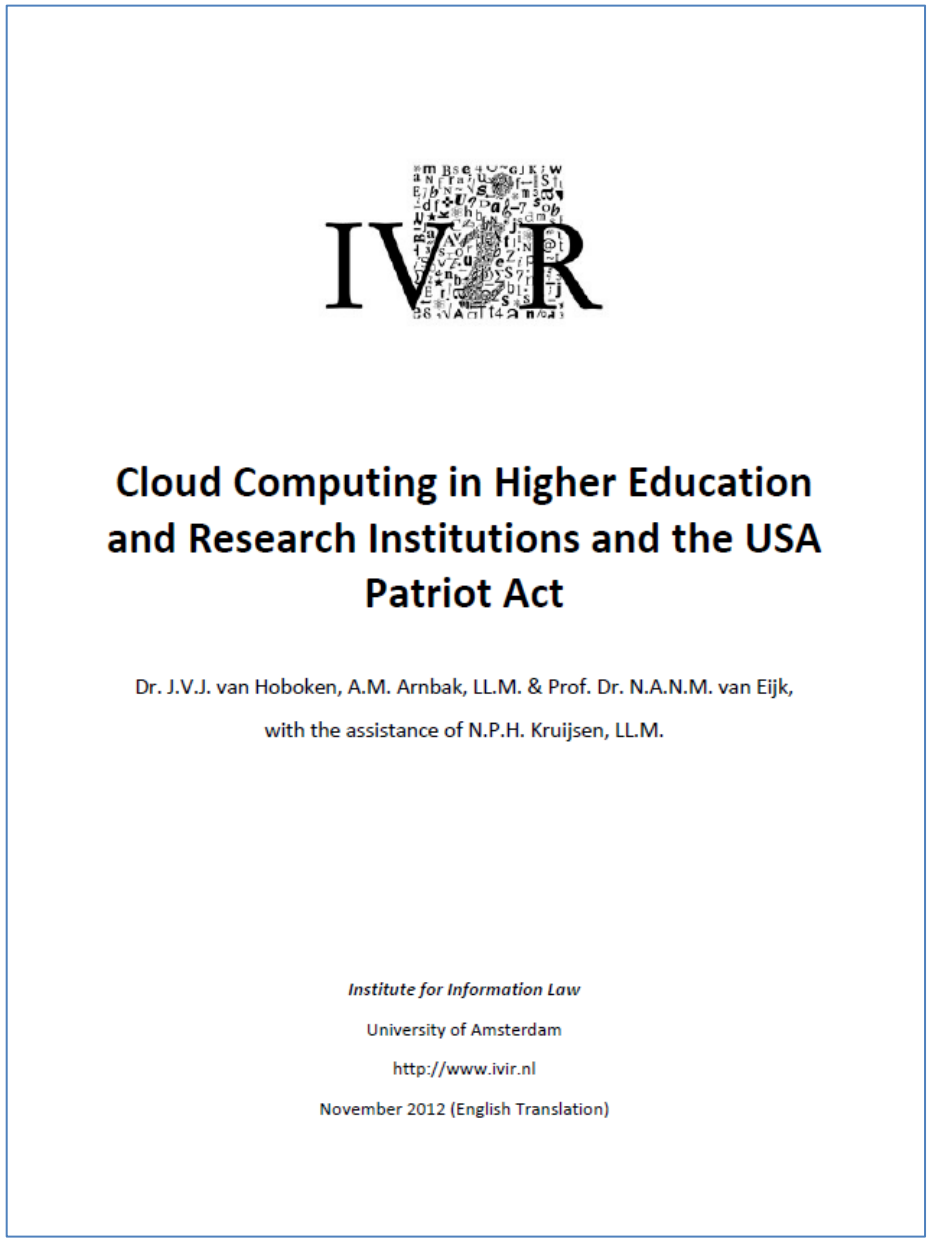
- In some cases, even law enforcement or national security actions from third countries may come into play, e.g. when the provider's business headquarters is based there



From the report:

Lack of legal certainty surrounding the concept of cybercrime and legal frameworks of cloud-based investigations, as well as inadequate tools to safeguard privacy and data protection increase the potential for misuses and abuses by law enforcement actors and agencies. European citizens' data are not sufficiently protected in this regard. This aspect is enhanced by exceptional measures taken in the name of security and the fight against terrorism. The US context is here particularly illuminating, both in the case of the Patriot Act and in the case of the US Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008. In this case, the question of the legal framework of data transfers/processing to third countries is critical.

http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050



From the report:

It is a persistent misconception that U.S. jurisdiction does not apply if the data are not stored on U.S. territory. The key criterion in this respect is whether the cloud provider conducts systematic business in the United States, for example because it is based there or is a subsidiary of a U.S.-based company that controls the data in question.

From the report:

(…) legal protection under specific U.S. laws applies primarily to U.S. citizens and residents.

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534

Differences in Requirements for Governments vs. Companies

- So far, the discussion has been mostly generic
- There are differences in the requirements of public and private sector information processing that also affect the approach to Cloud computing

Legacy Data

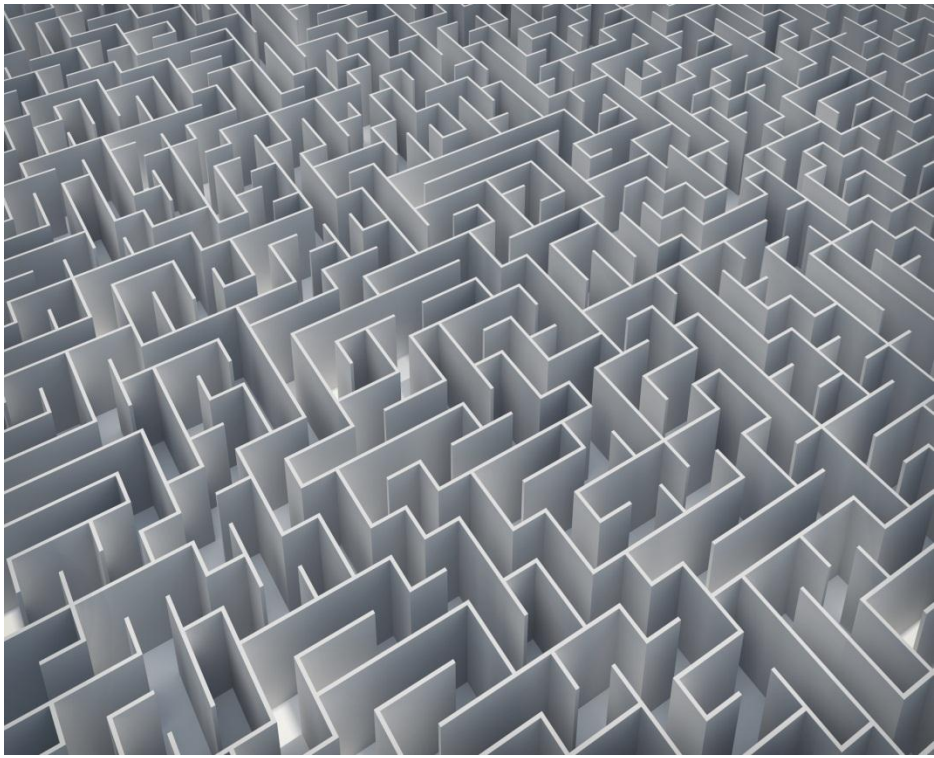
- Public sector IT in many cases has to deal with data that is much more “legacy” than corporate IT
- Examples include
  - Property registers
  - Population registers
  - Public archives
- These also have to remain available and correct for a very long time, compared to corporate data

Legacy applications

- Public sector IT in many cases still uses legacy applications
- Larger re-engineering efforts are required to make these “Cloud-ready”

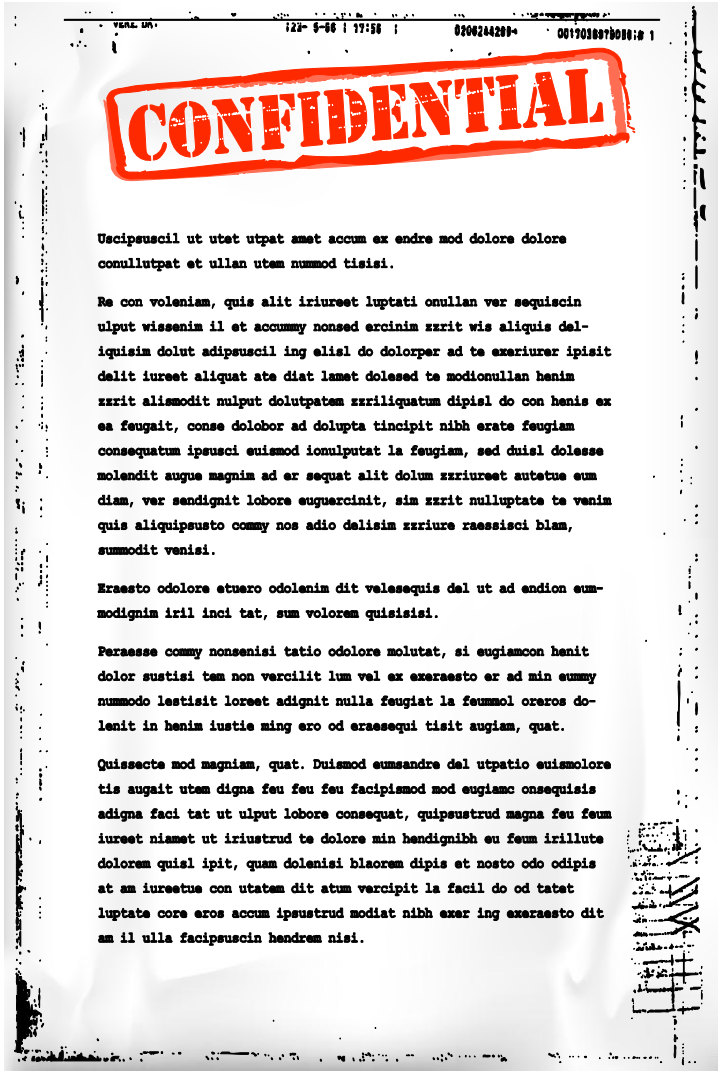
Legacy Processes

- Public sector IT often has to serve much more legacy processes than corporate IT
- Changes in processes are usually more difficult



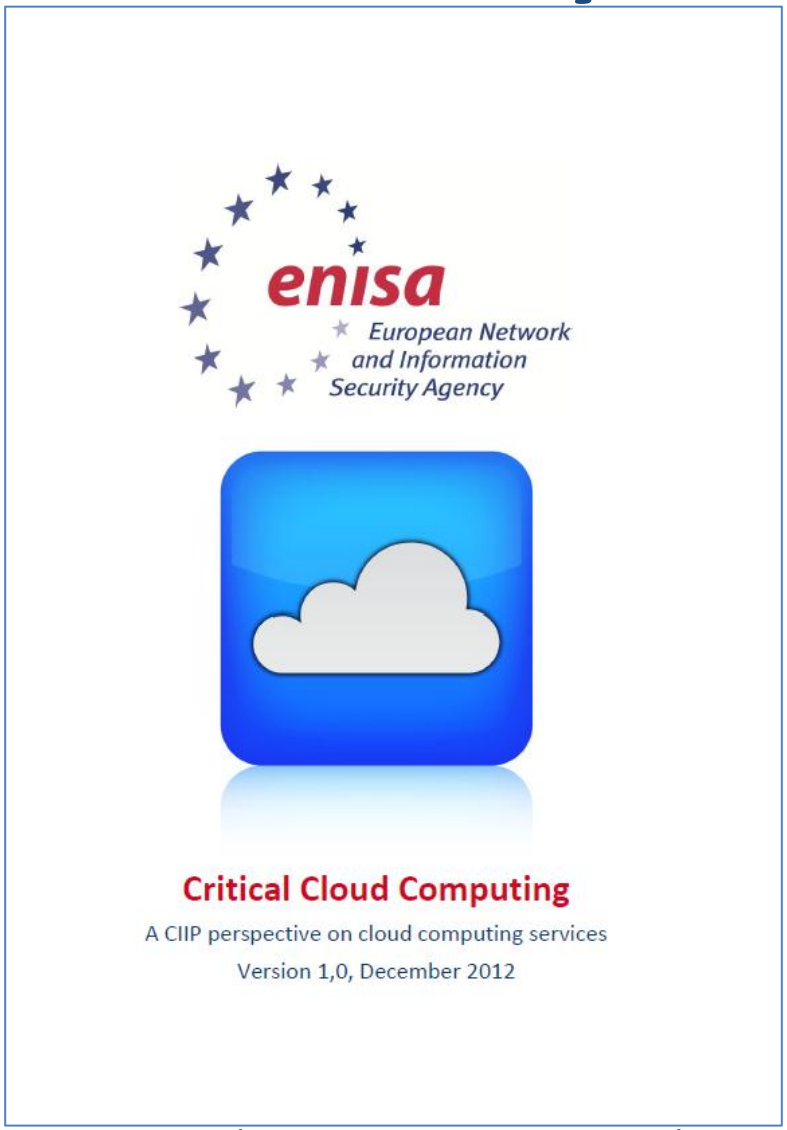
Special Information Assurance Requirements

- Classified information has very special assurance requirements
- Often, it may only be processed on specially accredited IT systems and applications (e.g. in Germany see the VS-ITR)
- Usually, encryption is required, sometimes using proprietary and classified crypto algorithms
- This excludes certain processing models



ENISA's Critical Cloud Study

- First assessment of CIIP aspects of Cloud computing
- Illustrates dependencies and provides examples for failures
- Provides recommendations for Cloud security governance from the CIIP perspective
- Conclusions can be applied to Governmental Cloud usage

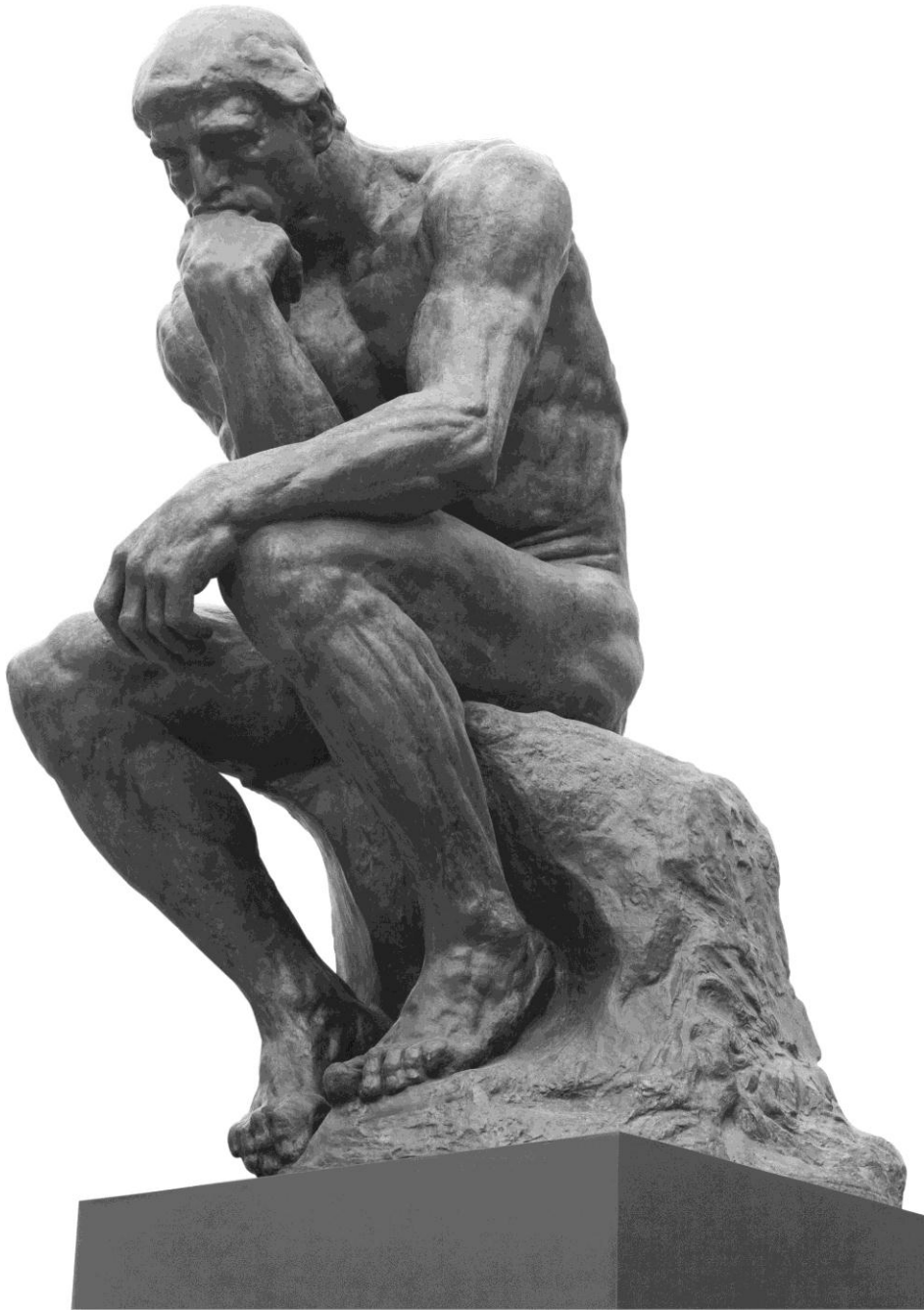


https://resilience.enisa.europa.eu/cloud-security-and-resilience/critical-cloud-computing/view

Critical Cloud Security Governance Model

- Risk Assessment
  - Assess dependencies and make them transparent
  - Prioritize security measures
- Security Measures
  - Best practices to achieve baseline
  - Logical and physical redundancy
  - Audits, tests and excercises
- Incident reporting
  - Mandatory incident reporting
  - Address all basic values of information security (confidentiality / integrity / availability)

Conclusions



Not everything can be shared

- Depending on the asset that has to be protected, sharing resources or even outsourcing is not an option

There is no Free Cheese!

- Cloud computing offers great benefits
  - Efficiency gains
  - Resilience
  - Financial savings
- But there's always a trade-off
- There will be new risks, other risks may change or even increase
- Before adopting the Cloud computing model, the special requirements of Governmental IT have to be considered and taken into account

Risks can be Mitigated

- For Governmental IT, some of the risks we described can be mitigated
- Cloud computing has several “flavours”
- Public cloud is usually the first model that is considered
- However, there are also “Private” and “Community“ clouds
- Private clouds only use the deployment aspect of the Cloud and are not shared with others
- Community clouds only share resources between users with similar requirements

Private and Community Clouds

- Allows much better control, over “where” and “how” of data processing
- Help to mitigate the loss of governance, data protection and jurisdictional risks
- Also allow better security measures to protect against isolation failure and management interface compromise
- The actual operations could still be outsourced to a varying degree

Collected Links to ENISA's Cloud Publications

- 2009 Cloud Computing Risk Assessment
  - http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport
  - Recommendations and key messages in Section 6, pp64-86
- 2009 Cloud Computing Information Assurance Framework
  - http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework
  - Information assurance framework introduced on p6
- 2011 Security and Resilience in Governmental Clouds 2011
  - http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds
  - Conclusions and recommendations pp83-89
- 2011 Security parameters in governmental cloud SLAs
  - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector
  - Key recommendations pp8-9
- 2012 Procure Secure
  - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts
  - Checklist guide to the document pp48-57
- 2012 Revision of the Cloud Computing Risk Assessment
  - https://resilience.enisa.europa.eu/cloud-security-and-resilience/cloud-computing-benefits-risks-and-recommendations-for-information-security
  - Top security risks pp6-8
- 2012 Critical Cloud Computing
  - https://resilience.enisa.europa.eu/cloud-security-and-resilience/critical-cloud-computing
  - Conclusions and recommendations pp22-25

Time for Questions

Contact

European Network and Information Security Agency

Science and Technology Park of Crete

P.O. Box 1309

71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu