FAQs to the report “Cloud Computing: Benefits, risks and recommendations for information security”

What is the background to this report?
Cloud computing was identified as one of the emerging applications, which is likely to have a very big impact on European businesses and governments and therefore it was included in the context of ENISA’s emerging and future risk assessment programme. IDC forecasts a growth of European cloud services from €971m in 2008 to €6,005m in 2013.

Some of the key conclusions of this paper show the cloud’s economies of scale and flexibility are both a friend and a foe from a security point of view. This paper allows an informed assessment of the security risks and benefits of using cloud computing - providing security guidance for potential and existing users of cloud computing.

This paper was produced by ENISA editors using input and comments from a group selected for their expertise in the area, including industry, academic and government experts.

What is included in the report?
The report covers the technical, policy and legal implications for information security and most importantly, makes concrete recommendations for how to address the risks and maximise the benefits for users.

This paper explains, based on concrete scenarios, what cloud computing means for network and information security, data protection and privacy. We look at the security benefits of cloud computing and its risks. Most importantly, we make concrete recommendations for how to address the risks and maximise the benefits.

What is cloud computing and how new is this technology?
Cloud computing is not a new technology, rather a new way of delivering computing resources. Computing services ranging from data storage and processing, to software, such as email handling, are now available instantly, commitment-free and on-demand.

Since we are in a time of belt-tightening, this new economic model for computing has found fertile ground and is seeing massive global investment.

Cloud Computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Are there any benefits of cloud computing for information security?
Cloud computing has significant potential to improve security and resilience and the report lists and describes some of the main benefits, which include
- **Security and the benefits of scale**: put simply, all kinds of security measures are cheaper when implemented at larger scale.
- **Security as a market differentiator**: Security is a priority concern for many cloud customers; many of them will make buying choices on the basis of the reputation for confidentiality, integrity and resilience and the security services
offered by a provider. This is a strong driver for cloud providers to improve security practices.

- **Standardised interfaces for managed security services**: Large cloud providers can offer a standardised, open interface to MSS providers. This creates a more open and readily available market for security services.

- **Rapid, smart scaling of resources**: The ability of the cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption etc to defensive measures has obvious advantages for resilience.

- **Audit and evidence-gathering**: Cloud computing (when using virtualisation) can provide dedicated, pay-per-use forensic images of virtual machines which are accessible without taking infrastructure off-line, leading to less down-time for forensic analysis. It can also provide more cost-effective storage for logs allowing more comprehensive logging without compromising performance.

- **More timely effective and efficient updates and defaults**: Default 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.

- **Benefits of resource concentration**: Although the concentration of resources undoubtedly has disadvantages for security, it has the obvious advantage of cheaper physical perimeterisation 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, maintenance processes. The extent to which those savings are passed on to customers will obviously vary.

What is the security assessment in the report based on?

For the purposes of this Cloud Computing risk assessment we analyzed three scenarios:

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

The SME use case scenario is published as ANNEX II in the report and a summary of the Resilience and eHealth ones is found as ANNEX III.

The level of risk in the risk assessment 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 certain likelihood.

What are the risks identified in the assessment?

ENISA’s report outlines some of the information security benefits of cloud computing, mentioned above. The report lists 35 key risks, classified in three categories:

- Policy and Organizational
- Technical
- Legal
Some of the risks that ENISA would like to highlight are:

- **Lock-in** (policy and organizational) is one of the main risks due to the limited amount of tools, procedures or standard data formats or services interfaces that could guarantee data and service portability. This makes it extremely difficult for customer to migrate from one provider to another, or 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.

- **Loss of governance** (policy and organizational). In using cloud infrastructures, the client necessarily cedes control to the cloud provider on a number of issues, which may affect security. 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 defences.

- **Isolation failure** (technical) concerns the computing capacity, storage, and network that are shared between multiple users and the risks includes the failure of mechanisms separating storage, memory, routing and even reputation between different tenants of the shared infrastructure.

- **Data protection** (legal). Cloud Computing poses several data protection risks for cloud customers and providers.

**Is it safe for companies and governments to trust the cloud providers with their data, which in some cases might include the entire business infrastructure?**

This is one of the key questions for potential cloud costumers and the most important part of the report is a detailed checklist of criteria that can be used to identify the cloud providers’ security-consciousness.

It is important to note that Cloud Computing can refer to several different service types, including Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The risk and benefits associated with each model will differ and so will the key considerations in contracting for this type of service.

**What are ENISA’s recommendations and key messages around cloud computing?**

One of the most important recommendations of this report is a set of assurance criteria that includes

- To assess the risk of adopting cloud services
- To compare different Cloud Provider offers
- To obtain assurance from the selected cloud providers.
- To reduce the assurance burden on cloud providers.

In addition to this the report also gives legal recommendations. The following is a list of areas the customer should pay attention to when assessing agreements of cloud services:

- Data Protection
- Data Security
- Transfer
- Law Enforcement Access
- Confidentiality and Non-disclosure
The report also includes legal recommendations to the European Commission and a section on research Recommendations. ENISA recommends the following as priority areas of research in order to improve the security of cloud computing technologies:

- Building trust in the cloud
- Data protection in large scale cross-organizational systems
- Large scale computer systems engineering (systems)

For full report:

For press release:

Additional material:
SME Survey on Cloud Computing
Cloud Computing Information Assurance Framework

For further details, contact:
Daniele Catteddu, Risk Analysis & Management Expert ENISA
daniele.catteddu@enisa.europa.eu
Giles Hogben, Network Security Policy Expert, ENISA
Ulf Bergstrom, Press & Communications Officer ENISA
press@enisa.europa.eu, Mobile: +30 6948 460143