Clouds Standards Coordination event
4-5 December 2012

Scope & perimeter of break-out sessions

## BREAKOUT 1: Security and Privacy [Daniele CATTEDU, Marnix DEKKER, Michael FISHER]

*4th December afternoon in parallel with Breakout 2*

**Scope (High-level scope statement covering subject matter).**
The scope covers the creation of a standards landscape and roadmap applicable to electronic information processed or stored in the cloud. The context is information security and privacy/data protection.
Specifically, three main areas are envisaged:

1. governance and compliance
2. risk assessment
3. risk treatment objectives and controls

The security and privacy activity covers standards, codes of practice and frameworks that, when applied in suitable combination, provide methods for assessing and mitigating security and privacy risks.
The term security risk covers risks to the confidentiality, integrity and availability of electronic information.
The term privacy risk covers risks to the appropriate collection, processing and disclosure of electronic personally identifiable information.

## BREAKOUT 2: Interoperability [Emmanuel DARMOIS, Gershon JANSSEN, Keith DICKERSON]

*4th December afternoon in parallel with Breakout 1*

**Scope (High-level scope statement covering subject matter).**
Interoperability within the context of Cloud Computing means enabling the Cloud Computing Ecosystem whereby individuals and organizations are able to widely adopt Cloud Computing technology and related services in such a fashion that multiple Cloud platforms can exchange information in a unified manor and ultimately work together seamlessly.
Examples of such interoperability are e.g. solutions running on multiple disparate Cloud instances and use of resources in other heterogeneous Cloud instances.
To realize this desired Interoperability, standards are required at all levels, e.g. infrastructure, platform, application, service, data and management.

## BREAKOUT 3: Data portability [Petteri ULJAS, Eric HENAULT, Ignacio MAS]

*5th December morning in parallel with Breakout 4 and 5*

### Discussion points and introductions on Data Portability

Regulatory and Legal/Compliance:

1. There is a need for data portability standards and laws for data that exists external to a company. Because of this gap, porting data across geo-political boundaries can be extremely difficult and result in one-off legal agreements and custom developed solutions.

Standards and Security/Protection: Especially as hybrid clouds are beginning to take shape, this will become more important if you want to shift between Public and Private and how to determine which data goes where

2. Portability of user data - cloud consumers use a cloud provider, data is held by that provider and cloud consumers may find that their data is held hostage by the provider.
3. Portability of applications - consumers of cloud services need to ensure they do not get locked into a single cloud provider but have the ability to move their applications from one cloud provider to another cloud provider.
4. Data Security - moving VM's, moving data, being able to cross boundaries of cloud providers is all for naught if providers are unable to keep user's data secure.

Technical considerations : The data could be in a data store embedded within the PaaS application (user, configuration and log data), as a data store that a PaaS applications connects to, or as configuration or log data that external to the application.

5. With today's data rich applications, volume of data can become a technical issue for data portability. Bandwidth, network saturation, QOS impacts on other processes, and latency effects on application behavior all need to be taken into consideration.
6. Applications should be designed to operate in a cloud environment. This design must also take into account the type of data persistence that will be in use (embedded, data as a service, external database/file). One of the application design principles for cloud-based applications is to separate compute from persistence providing deployment and scaling flexibility.

Termination of Service: This is also coming into play more and more and can have a huge impact on the services being delivered. If cloud model is to be as flexible as we all expect it to be, what does that mean to data portability.

7. Data portability applies to various types of data in the cloud; user data, configuration data, service management data, performance management data, monitoring data, alerting and other log data. Not all data is required to move when moving a workload but how to handle that data when a VM is destroyed at the origin?

## BREAKOUT 4: SLA [Jamil CHAWKI, Aileen SMITH, BERND BECKER]

*5th December morning in parallel with Breakout 3 and 5*

**Scope (High-level scope statement covering subject matter**

A Service Level Agreement (SLA) is a documented agreement between the service provider and customer that identifies services and service targets. [ISO/IEC 20000-1:2011].
The scope of this session is to:

a) Catalogue standards organizations and specifications – existing as well as missing - that may be relevant to SLAs that apply to the whole service/supply chain of Cloud.
b) Collect key issues and new ideas relevant to SLAs for Cloud.

Some elements of SLAs will depend on legislation, regulation and other matters outside the scope of standardization.
Potential issues to be addressed by SLA standards/specifications include, but not limited to:

- Issue 1: Stakeholders and their responsibility.
- Issue 2: Handling of e.g. QoS, KPI and KQI in addition to security, privacy aspects relevant for SLA fulfillment.
- Issue 3: Others.

## BREAKOUT 5 REVERSABILITY [Massimo Banzi, Vincent Franceschini, Stefan Tai]

*5th December morning in parallel with Breakout 3 and 4*

**Scope (High-level scope statement covering subject matter**

Scope of the breakout session is the Reversibility within the context of Cloud Computing. Mainly Reversibility addresses the threat of vendor Lock-In.
As a starting point, the following definition for Reversibility may be considered, as the one provided by EuroCIO:
**Reversibility**: "Customers should be able in full autonomy at any time (e.g. through night scheduling) to get back all their data, in a standard format, for a predefined cost and timescale".
In this context, the notion of reversibility implies going back to a previous state of operations: e.g.

- From Cloud back to Non-Cloud
- From Public Cloud back to Private Cloud
- From Cloud B back to Cloud A