Reference Model
of Cloud Computing
Public Carrier’s View

Vladimir Belenkovich

April, 14, 2010
SG-17 meeting
Sources

- Open Cloud Manifesto, Spring 2009
  http://www.opencloudmanifesto.org/

- Cloud Computing definition
  NIST, version 15

- Cloud Standards Summit, July 2009, OMG
  http://cloud-standards.org
Security Guidance
for
Critical Areas of Focus
in
Cloud Computing V2.1

Prepared by the
Cloud Security Alliance
December 2009
What Comprises Cloud Computing?

The earlier version of the Cloud Security Alliance’s guidance featured definitions that were written prior to the published work of the scientists at the U.S. National Institute of Standards and Technology (NIST) and their efforts around defining cloud computing. NIST’s publication is generally well accepted, and we have chosen to align with the NIST Working Definition of cloud computing (version 15 as of this writing) to bring coherence and consensus around a common language so we can focus on use cases rather than semantic nuance.

It is important to note that this guide is intended to be broadly usable and applicable to organizations globally. While NIST is a U.S. government organization, the selection of this reference model should not be interpreted to suggest the exclusion of other points of view or geographies.

NIST defines cloud computing by describing five essential characteristics, three cloud service models, and four cloud deployment models. They are summarized in visual form in figure 1 and explained in detail below.

Figure 1 - NIST Visual Model of Cloud Computing Definition

- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service

Resource Pooling

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Public
Private
Hybrid
Community

Essential Characteristics
Service Models
Deployment Models
Cloud computing is about gracefully losing control while maintaining accountability even if the operational responsibility falls upon one or more third parties. It is important to note that the use of cloud computing as an operational model does not inherently provide for or prevent achieving compliance. For an excellent overview of control frameworks which provides good illustrations of the generic risk assessment framework; this, in turn, helps to determine how the gaps and ultimately risk mandates, it becomes much easier to determine what needs to be done in order to feed back into a security architecture patterns documentation, control framework alluded to above, see the Open Security Architecture Group.
Let’s get rid of hierarchy

Let’s get rid of hierarchy

SaaS

PaaS

IaaS

Integration and Middleware

APIs

Presentation Modality

Presentation Platform

Applications

APIs

Data

Metadata

Content

Hardware

Facilities

Abstraction

Core connectivity
Let’s move it around
Let’s remove some details
Methodology needed

- Trusted service cloud
- Service methodology merged with security methodology
- Standards reuse
NGOSS Methodology

- M.3050.0-4 eTOM
- M.3190 Shared Information and Data (SID)
- Role models, stakeholders
- TNA - Technology Neutral Architecture
- Business view ➔ System view ➔ Implementation view ➔ Performance view
Simple rule of thumb

Standards reusability is the only way to cope with the complexity spell.
Thank you!

vbelenkovich@gmail.com

Skype: vbelenkovich