

# Toward Risk Assessment as a Service in Cloud Environments

Burton S. Kaliski Jr. and Wayne Pauley  
EMC Corporation  
**HotCloud '10**  
June 22, 2010

# Risk Assessment: Definition

- Quantitative and/or qualitative **valuation of risk** in a **specific context** against a **given threat** with a **probability of occurrence**
- Includes **system characterization, threat assessment, vulnerability analysis, impact analysis, and risk determination**
- Many well-established standards for assessing security; some for privacy as well

OCTAVE  
NIST Assessments  
DOJ/DHS Shared  
27002:2005 COBIT  
PIA SP800-53  
ISO/IEC 22307:2008

[www.tagxedo.com](http://www.tagxedo.com)

# Risk Assessment in the Cloud: Challenges

Cloud Characteristic (per NIST)	Challenge
On-Demand Self-Service	<ul style="list-style-type: none"><li>• Human interaction is replaced with <b>automated controls</b> – which now must be “trained” to pass security audits</li></ul>
Broad Network Access	<ul style="list-style-type: none"><li>• <b>Endpoints</b> can be any type, location, not just a pre-approved set</li></ul>
Resource Pooling	<ul style="list-style-type: none"><li>• <b>Dynamic allocation, virtualization</b> mean that resources are not known in advance</li><li>• <b>Multi-tenancy</b> brings threats “in house”</li><li>• <b>Location independence</b> introduces significant diversity in applicable laws</li></ul>

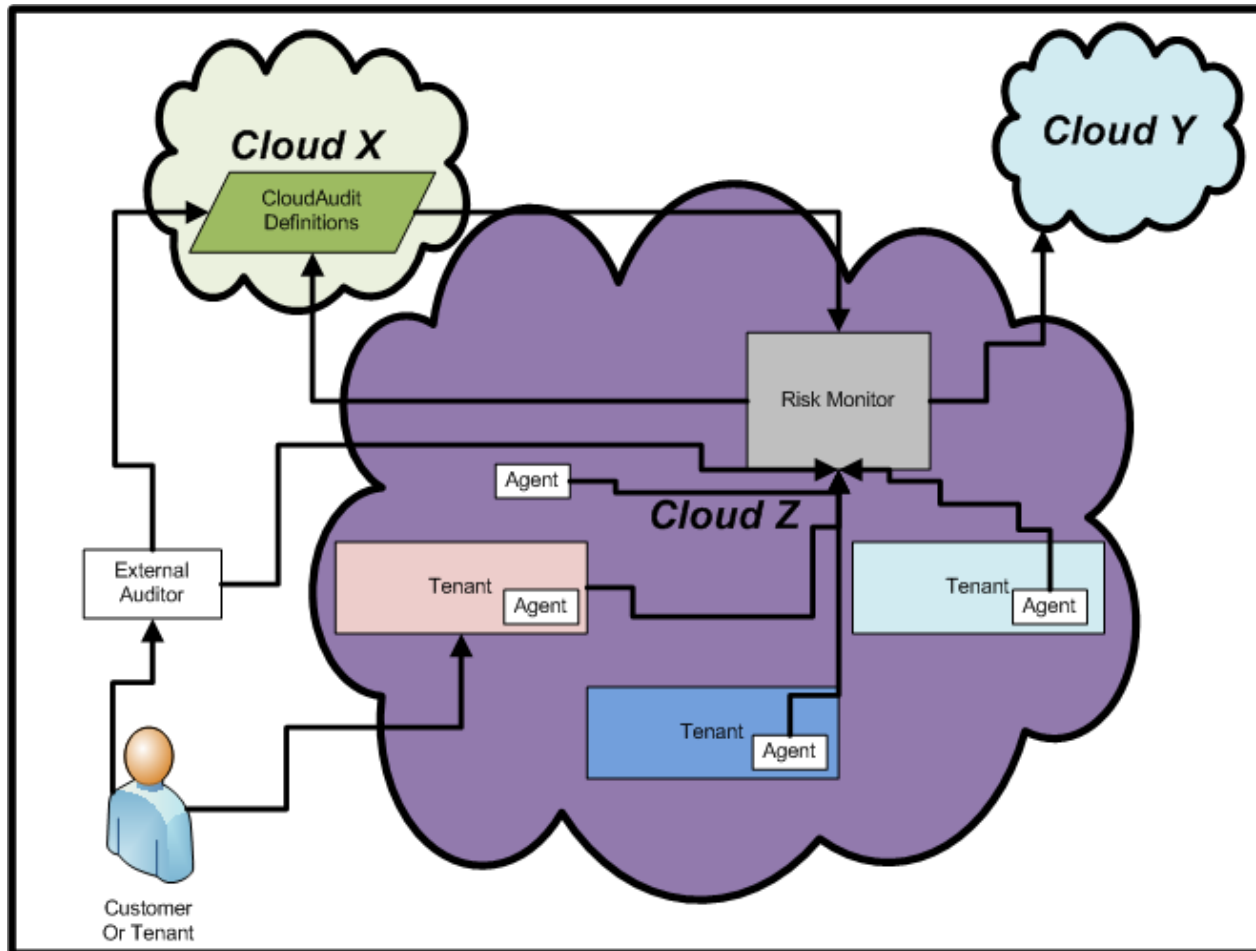
# Risk Assessment in the Cloud: Challenges

Cloud Characteristic (per NIST)	Challenge
Rapid Elasticity	<ul style="list-style-type: none"><li>• <b>Cloud bursting</b> engages multiple levels of sub-providers, who must also be assessed</li></ul>
Measured Service	<ul style="list-style-type: none"><li>• <b>Metering information</b> has more detail about multiple tenants – a higher-value target</li></ul>
	<ul style="list-style-type: none"><li>• <b>Economics</b> of the cloud also complicate assessments:<ul style="list-style-type: none"><li>• <b>cloud infrastructures will be constantly changing</b> due to market growth, M&amp;A – risk assessments will rapidly become stale</li><li>• <b>cost competition may discourage investment</b> in risk assessments while <b>increasing risk-taking</b></li></ul></li></ul>

# Proposal: Risk Assessment as a Service

- Approach: an **automated “risk score”** (e.g. like “credit score”)
  - for a given tenant or application – or for general use
  - pre-assessment and on-demand
- Modes: **provider self-assessment, third-party audit, consumer assessment** (non-privileged)
  - internal and external agents involved
- **Policy-based IT management** translates assessment of underlying dynamic resources into overall score

# Architecture



# Topics for Further Research

- **Automated measurement and analysis** for risk assessment
  - What sensors are needed? What language to use?
    - E.g., CloudAudit defines a dictionary based on common standards
- **Automated *adjustment*** based on the assessment
- **Trust assurances** for measurements
  - “Who guards the guards?”
- **Effectiveness of automated assessment vs. traditional approaches**

# Contact Information

- **Burt Kaliski**

Director, EMC Innovation Network  
Founding Scientist, RSA Laboratories

[kaliski\\_burt@emc.com](mailto:kaliski_burt@emc.com)

[community.emc.com/people/kalisb](http://community.emc.com/people/kalisb)

- **Wayne Pauley**

Director, Global Product Sales

[wayne.pauley@emc.com](mailto:wayne.pauley@emc.com)



**EMC<sup>2</sup>**<sup>®</sup>

**where information lives<sup>®</sup>**