# Cloud Standards

**Arlindo Dias**
**IT Architect**
**IBM Global Technology Services**

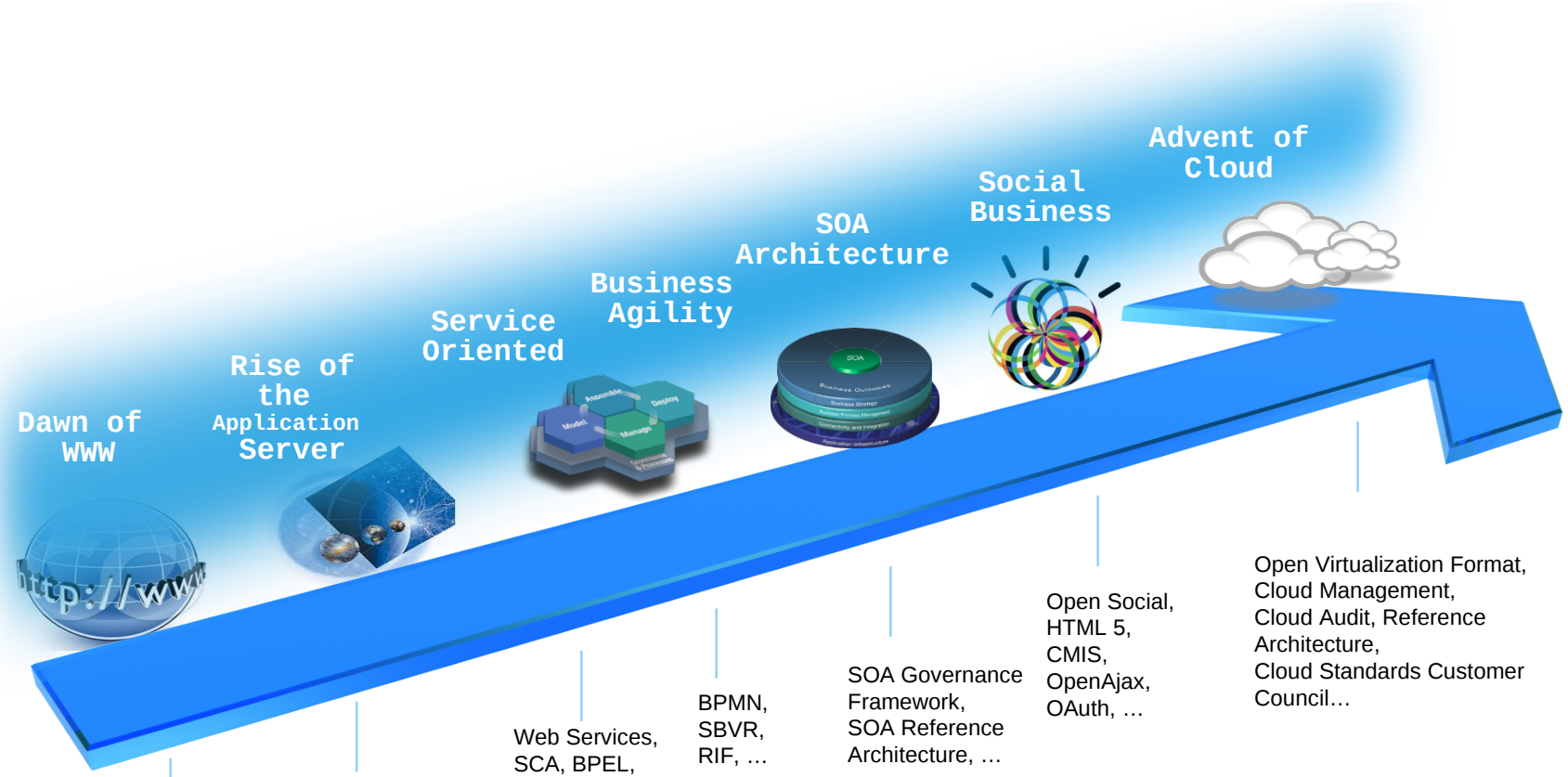
**CLOSER 2102**

# Agenda

- Overview on Cloud Standards
- Identity and Access Management
- Discussion

# Overview on Cloud Standards

# Why “an open Cloud” is important?




Cloud builds on and leverages the standards which preceded this market cycle

# Context

Cloud computing is a model for ***enabling cost effective business outcomes through the use of shared application and computing services***. The value …. if possible …. is better economics in the execution of business processes.

Hype around cloud has created a flurry of standards and open source activity leading to market confusion.

As important as current standards development efforts are, they are not enough.

There is a lack of a customer driven prioritization and focus within the cloud standards development process.

# The landscape

| | DMTF | The Open Group | OASIS Standard | ETSI | CSA cloud security alliance | OpenGridForum | tmforum | SNIA |
|---|---|---|---|---|---|---|---|---|
| Architecture | | ✓ | ✓ | ✓ | | | ✓ | |
| API | ✓ | | | ✓ | | ✓ | | ✓ |
| Virtualization | ✓ | | | | | | | |
| Management | ✓ | ✓ | ✓ | | | ✓ | | ✓ |
| Storage | | | | | | ✓ | | ✓ |
| SLA | | ✓ | ✓ | | | | ✓ | |
| Network | ✓ | | | | | | | |
| Security | ✓ | ✓ | ✓ | | ✓ | | | |

ETSI · Open Cloud Consortium · ISO International Organization for Standardization · simple cloud · GICTF · Apache · NIST · δ·CLOUD · ncoic · ITU International Telecommunication Union · libcloud · RESERVOIR

Dozens of new communities and organizations have formed around cloud standards including industries and governments (e.g. INCITS in US and CESI)

# Cloud Standards Customer Council


On April 7, 2011 industry leaders from across the world formed the ***first customer led consortium*** designed to shape the face of open standards based cloud computing.

- Drive user requirements into standards development process.
- Establish the criteria for open standards based cloud computing.
- Deliver content in the form of best practices, case studies, use cases, requirements, gap analysis and recommendations for cloud standards.

## Structure

- Participation –. Primarily C-Level executive, VP of Development, IT management, Enterprise architects, cloud strategy
- Meetings– Monthly virtual meetings. Quarterly face-to-face co-located at OMG events. Participation through forums and subgroups.
- Oversight – Managed by OMG
- Leadership – Founding members form steering committee
- Standards Development – This group will not produce standards but will provide guidance to existing standards development organizations

## Deliverables

- Web Presence- Community, Webcasts, Case studies, blog, vendor showcase, whitepapers, case studies awards.
- Candidate Deliverables – ready to use content in the form of use cases, case studies, requirements, gap analysis and recommendations for cloud standards, and training.
- Awareness – Drumbeat of awareness utilizing events, press, books, analysts partnerships and media.

*http://www.cloud-council.org/application*

# Identity and Access Management

# Agenda

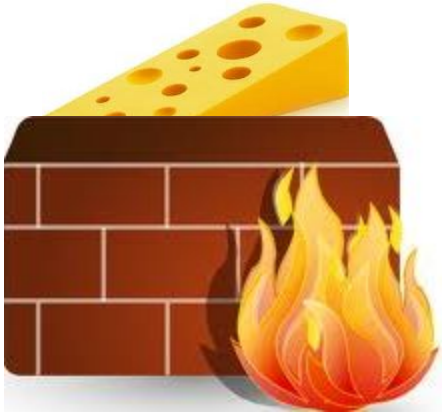
- How to think about IAM from Cloud perspectives
- Industry Standards and Working Groups
- Scenarios
- Wrap-up

# Trends affecting Cloud and IAM


User and data mobility ↑


API Calls ↑

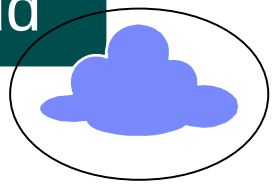
Perimeter security ↓



Browser Access ↓

# Individuals will consider Cloud IAM from one or more of these perspectives

**FOR** the Cloud



- What IAM capabilities are required in the cloud infrastructure and management platform?

**WITH** the Cloud

- How can IAM be used to integrate on-premise and cloud based IT services?
- How can IAM enable cloud adoption?

**FROM** the Cloud

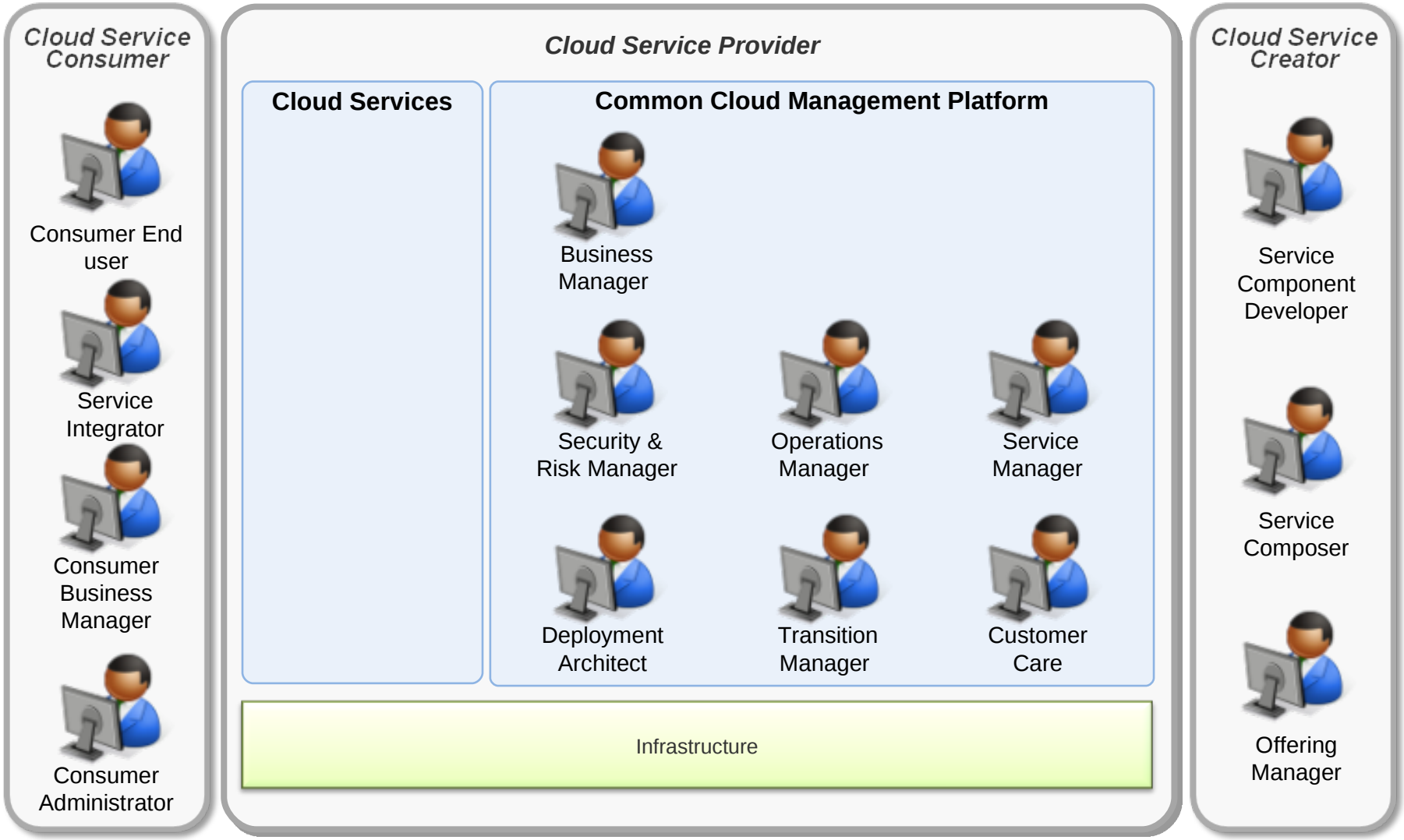
- How can IAM services delivered via a cloud based model benefit on-premise or cloud based IT?
- How can IAM in the cloud be compared to equivalent on-premise solutions?

# What is different about IAM in a Cloud Context?

| Consideration | What makes it different? |
|---|---|
| Data Locality | Identity information may no longer be protected by the same laws and regulations as if it was in your on-premise environments. |
| Multi-tenancy | Cloud management interfaces are used by multiple tenants to manage their own use of the cloud. |
| Cloud Provider Administration | Cloud provider's administrators are not necessarily subject to the same controls as in the on-premise case. |

IAM can be an enabler for cloud adoption – not just a security control motivated by risk management.

# Identity/access model for a multi-tenant cloud must support a variety of roles and their entitlements



# Agenda

- How to think about IAM from Cloud perspectives
- Industry Standards and Working Groups
- Scenarios
- Wrap-up

## Security Assertion Markup Language (SAML)


- Initially developed in 2001
- Reasonable adoption among enterprises and cloud services
- Requires trust between identity provider and relying party partners
- http://www.oasis-open.org/committees/security/

## OpenID

- User-centric SSO
- Initially developed in 2005
- Wide adoption in web
- Lower adoption in enterprise context
- http://openid.net/

## OAuth


- *"An open protocol to allow secure API authorization in a simple and standard method from desktop and web applications."*
- Initially developed in 2007
- Adopted by Google, Twitter, Facebook, ...
- Eliminates need for password based credentials to be used in API calls
- http://oauth.net/

## OpenID Connect


- Announced earlier in 2011
- Based on OpenID 2.0 protocol
- Intended to achieve the same outcomes as OpenID but with RESTful APIs to simplify ubiquitous use.
- Designed to integrate with OAuth
- http://openid.net/connect/

## Service Provisioning Markup Language (SPML)

- XML based framework for identity provisioning
- Initially developed in 2001
- Low adoption among enterprise application vendors
- http://www.oasis-open.org/committees/provision/

## Simple Cloud Identity Management (SCIM)

- Formed in late 2010
- *"designed to make managing user identity in cloud based applications and services easier"*
- *"make it fast, cheap, and easy to move users in to, out of, and around the cloud"*
- http://www.simplecloud.info/

## OASIS Identity in the Cloud TC


- TC initially formed in 2010
- *"Developing profiles of open standards for identity deployment, provisioning and management in cloud computing"*
- http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud

## Cloud Standards Customer Council


- Formed in 2011
- Broader than just identity, security
- Intends to influence existing standards efforts, not create new standards
- http://cloudstandardscustomercouncil.org/

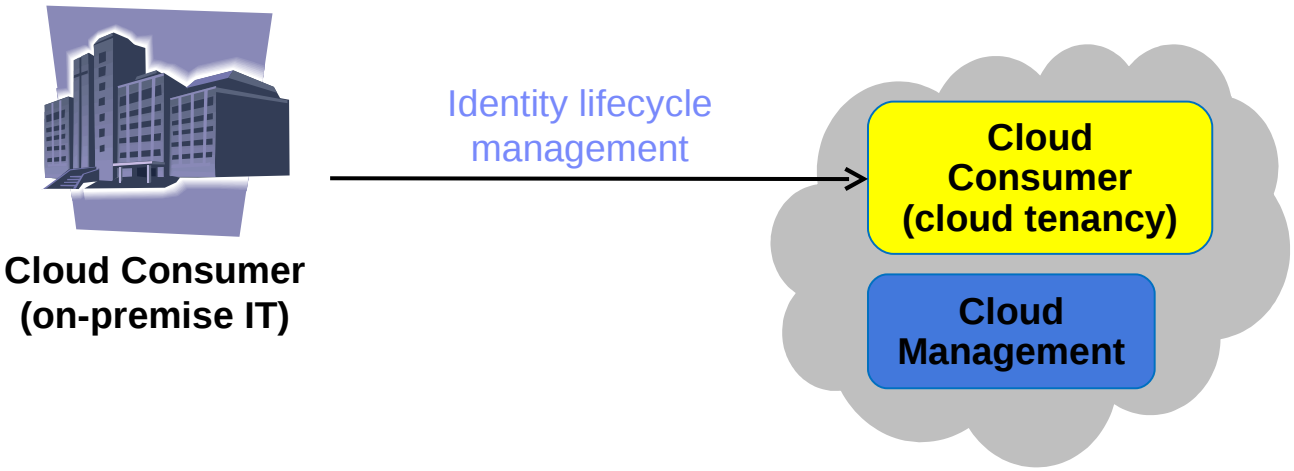
# Cloud Security Alliance

- Formed in 2009
- *"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."*
- Not intended to be a standards body
- https://cloudsecurityalliance.org/
- Australian chapter: http://www.linkedin.com/groups?gid=3966724

# Agenda

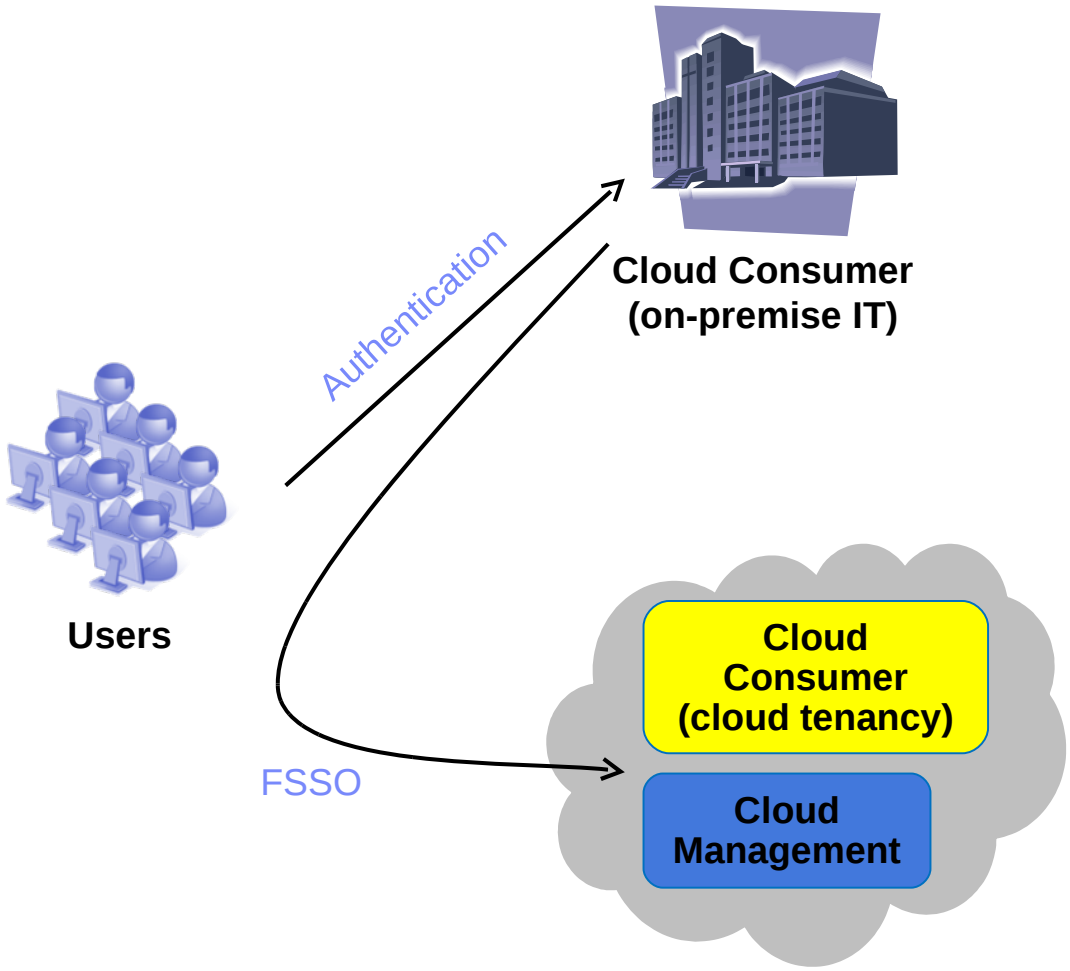
- How to think about IAM from Cloud perspectives
- Industry Standards and Working Groups
- Scenarios
- Wrap-up

# Integrate on-premise identity governance with the Cloud



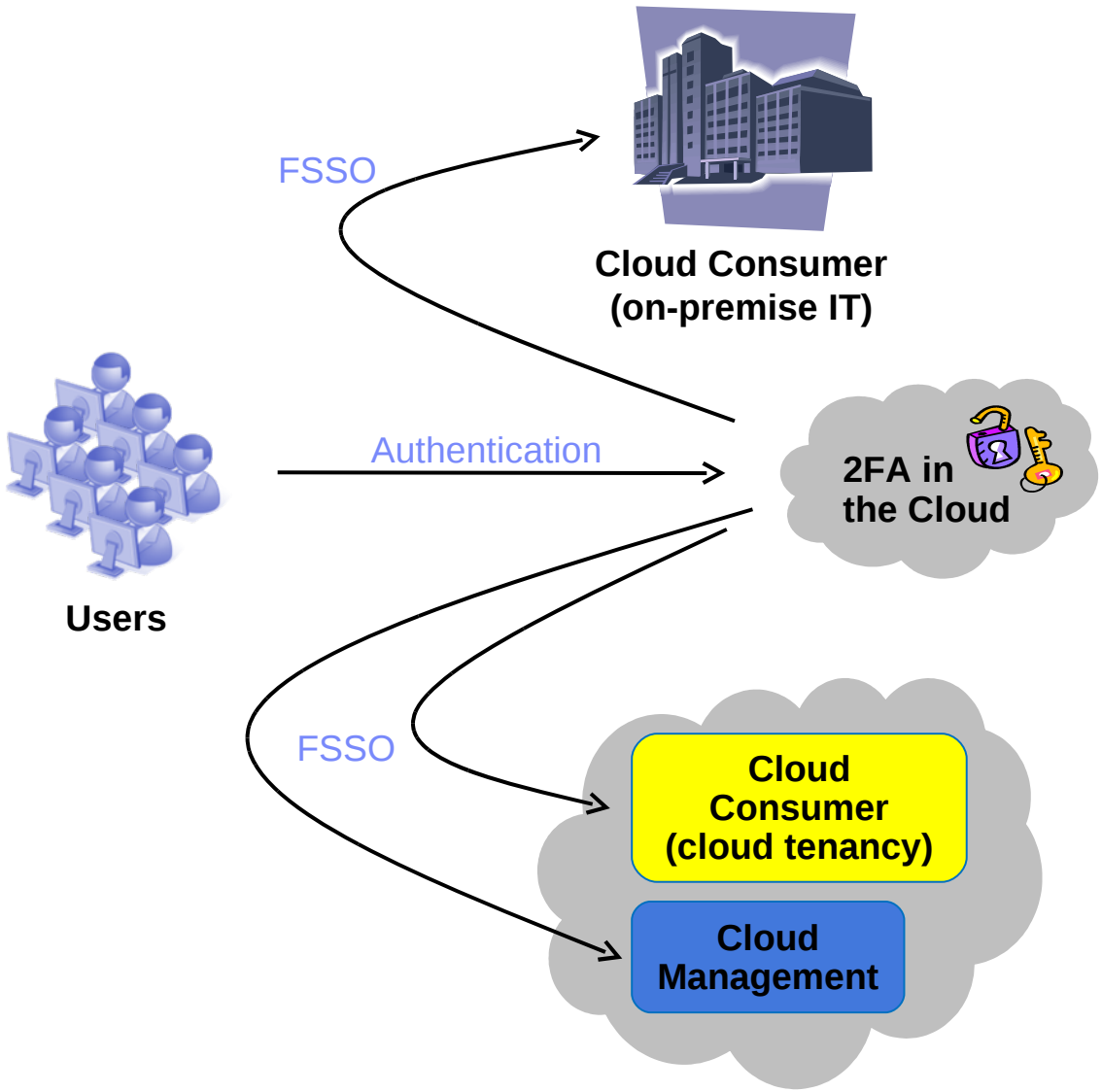

- Extend on-premise identity governance capabilities to IT services hosted in the Cloud
- Standards are not widely adopted at this time
  - SPML is one potential standard
- Examples:
  - Manage users and groups within a GoogleApps domain from on-premise identity lifecycle management
  - Run adapters from traditional identity provisioning solutions on cloud based instances.

# Integrate on-premise authentication with the Cloud



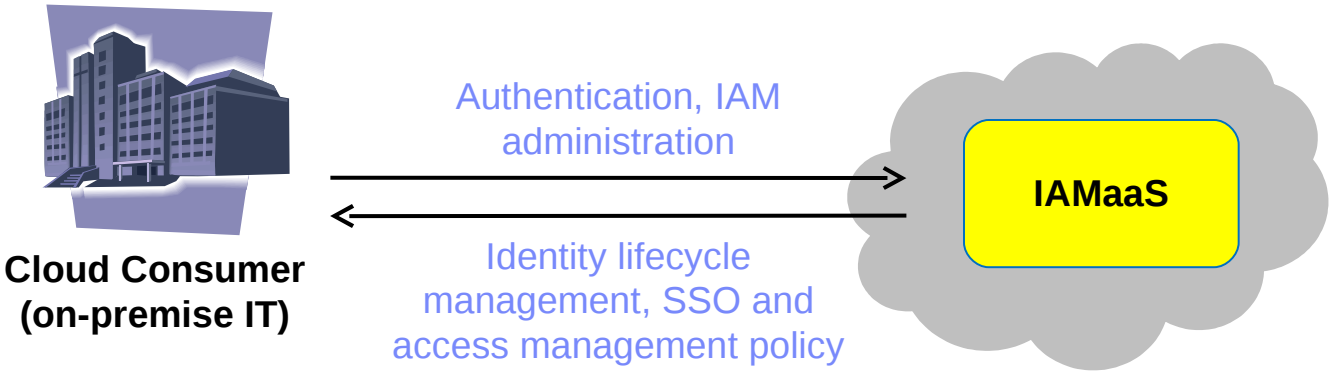

- Reuse existing on-premise identity and credential stores
- Federated Single Sign-on (FSSO) may be the integration approach
  - FSSO standards include SAML, OpenID
- Example: Use SAML to integrate with Salesforce.com

# Strong authentication from the Cloud



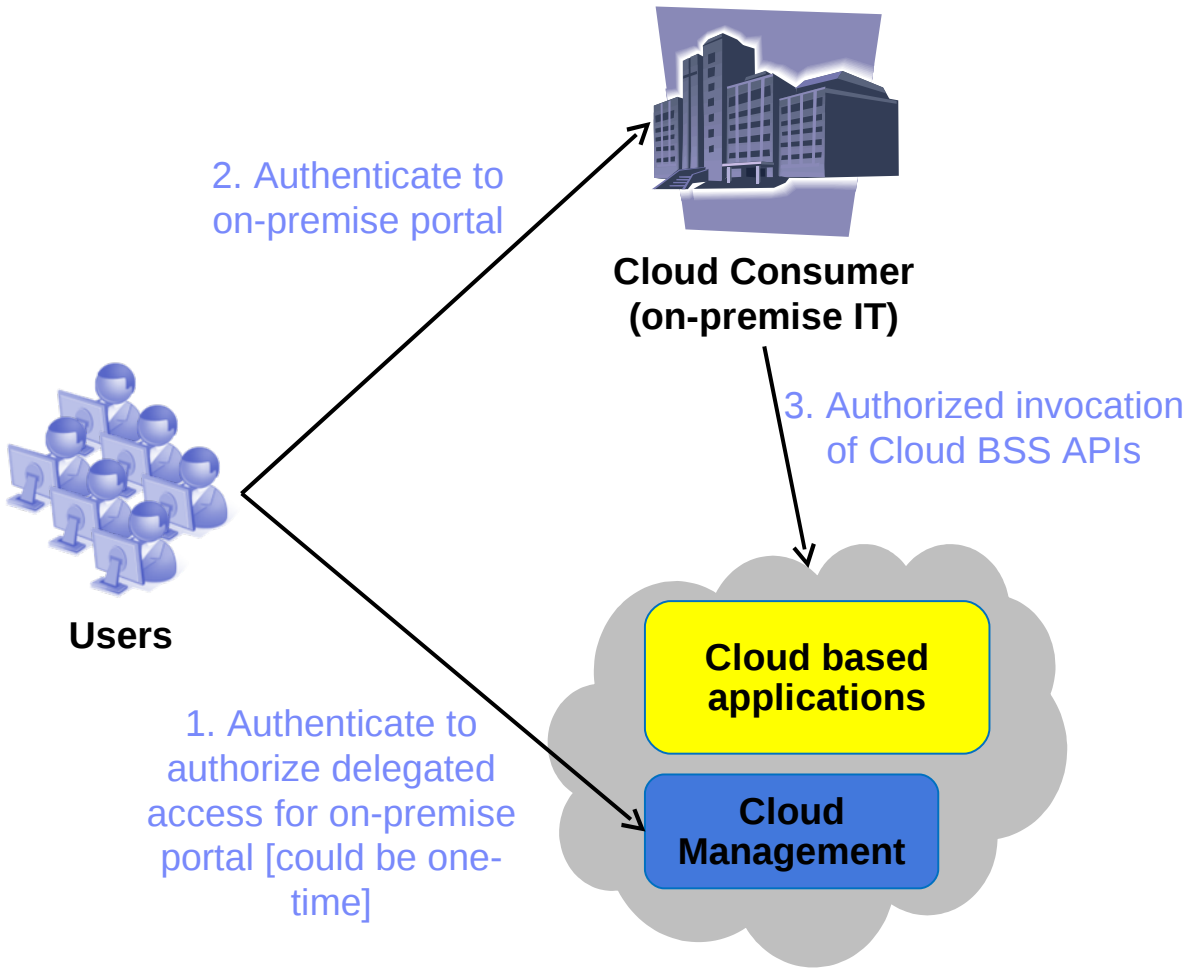

- Potential integration with on-premise or cloud IT
- Federated Single Sign-on (FSSO) may be the integration approach
  - FSSO standards include SAML, OpenID
- Example: authentication based on possession of a mobile device

# Identity and access management from the Cloud



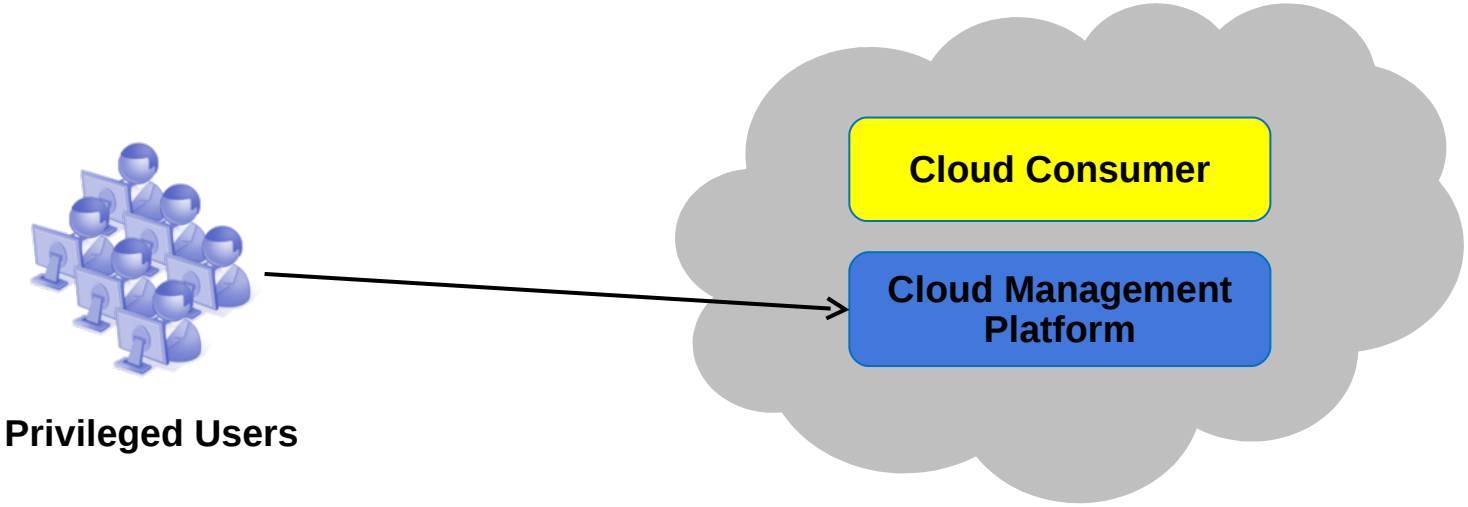

- An alternative model for delivery of IAM services, while retaining the rich capabilities of on-premise systems
- Suitable for many, but not all customers
- Example: IAMaaS delivered by traditional IAM vendors or their partners (e.g. Lighthouse Gateway)

# Integrate access management of on-premise portal with Cloud management platform



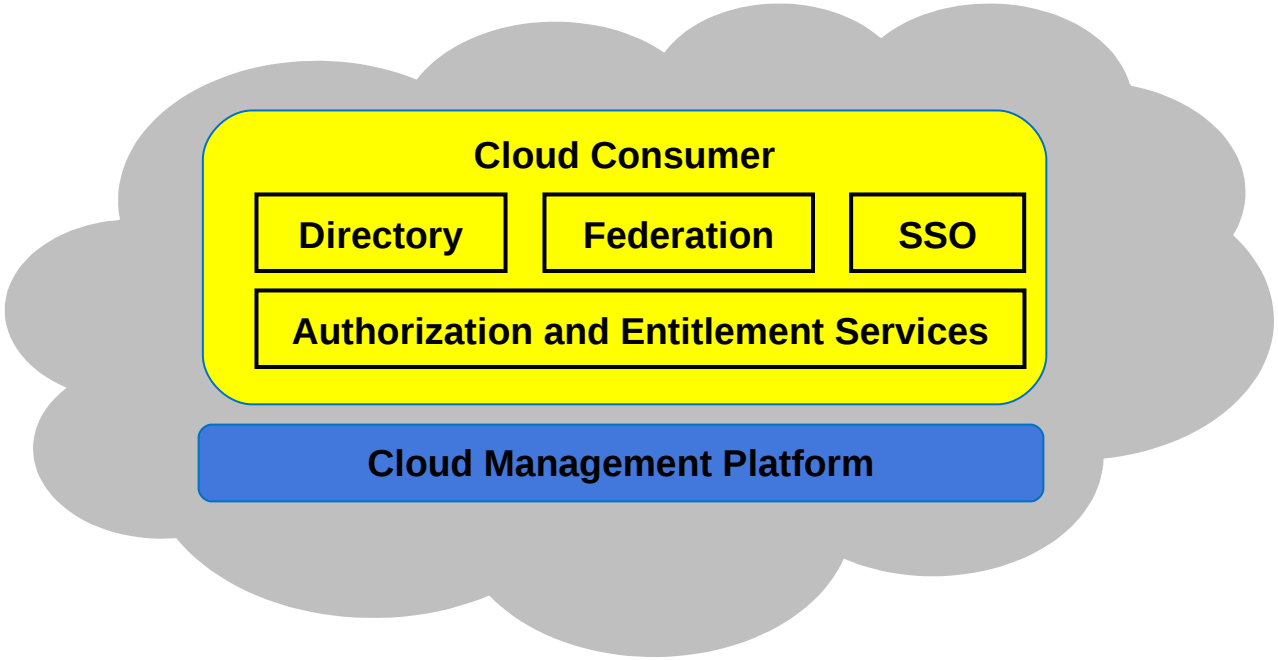

- On-premise portal aggregates across multiple cloud providers
- Use of Cloud APIs is authorized based on user identity, not just the enterprise's
- Example: Use OAuth for scoped, delegated authorization of Cloud BSS APIs

# Monitoring the cloud service provider's privileged users



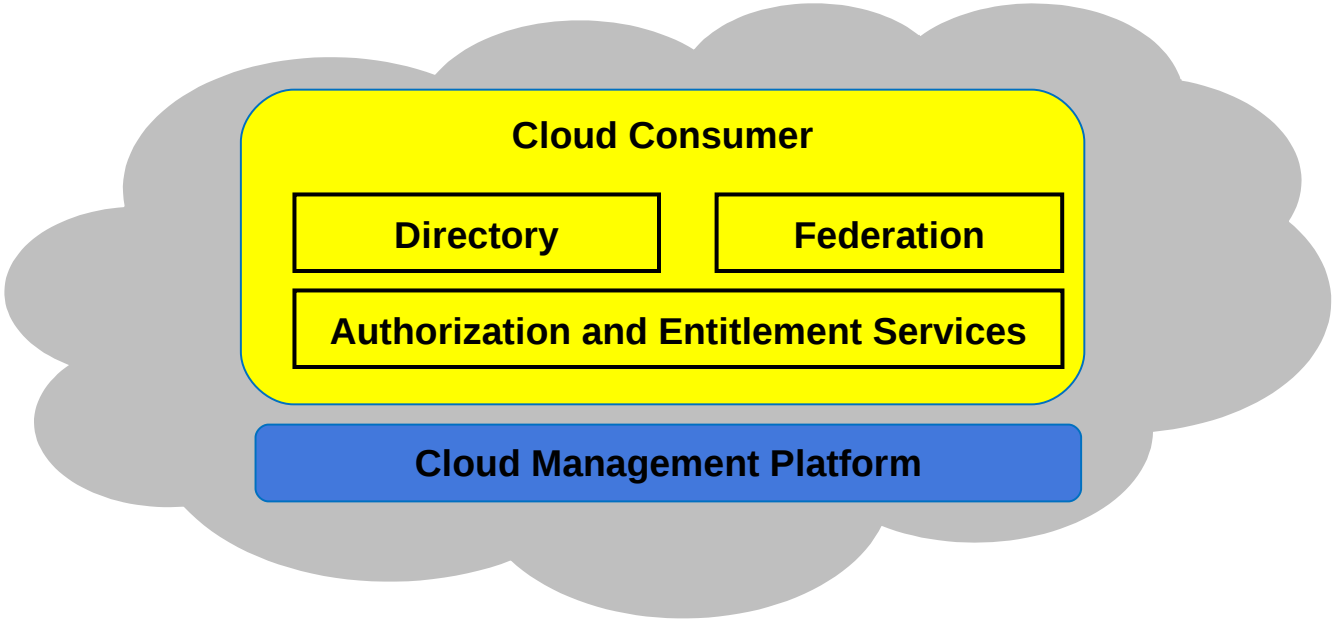

- Important part of securing the cloud infrastructure
- Example: Management, monitoring and auditing of privileged users operating the cloud infrastructure

# Identity-enabled Infrastructure as a Service




- Images enabled with common authentication services
- Examples:
  - Windows Desktop as a Service with Active Directory
  - SSO, user switching for end users in Desktop as a Service
  - Linux VMs with LDAP enabled SSH

# Identity-enabled Platform as a Service

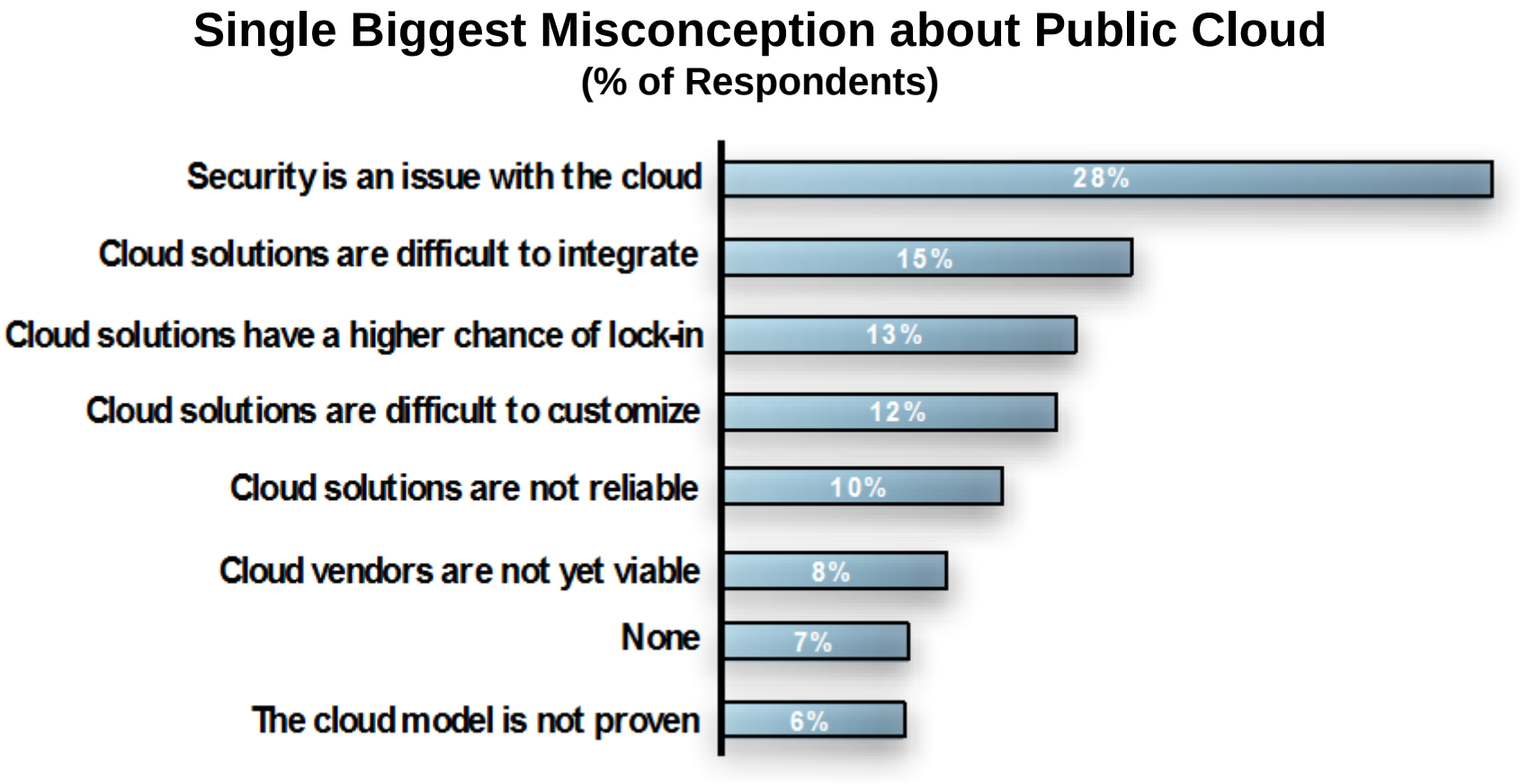



- Application environments pre-configured with IAM technology and best practices
- Examples:
  - Authentication via LDAP server component
  - Federation infrastructure

# Agenda

- How to think about IAM from Cloud perspectives
- Industry Standards and Working Groups
- Scenarios
- Wrap-up

# What can we learn from companies who have already adopted public cloud solutions?




Appirio, State of the Public Cloud: The Cloud Adopters' Perspective, October 2010
http://thecloud.appirio.com/StateofthePublicCloudWhitepaper1.html

# Conclusion

- Identity and access management is a **logical starting point** for integrating on-premise and cloud security services
- There is **a lot of standards** activity for identity, access and cloud currently underway
- Mature, pre-cloud standards are suitable for applying **to some** cloud scenarios now
- Identity and access can be demonstrated as an enabler for cloud adoption, **not just a 'control'** driven by risk and compliance.

# Cloud IAM's Can of Worms

- What types of new identity management methods and tools are needed to support your cloud deployments?
- Are new standards mandatory for integrating your on-premise and cloud identities?
  - What would those standards need to address?
- Do you consider identity providers such as Google and Facebook suitable for supporting your cloud deployments?
  - If so, why?
  - If not, why not?
- How does IAM affect the economics of moving to the cloud?

# References

# References

- Cloud Computing Security Considerations, Australian Department of Defence
  - http://www.dsd.gov.au/infosec/cloudsecurity.htm
- Cloud Computing - Benefits, risks and recommendations for information security, European Network and Information Security Agency
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
- Cloud Controls Matrix, Cloud Security Alliance
  - http://www.cloudsecurityalliance.org/cm.html
- Guidelines on Security and Privacy in Public Cloud Computing (SP 800-144), NIST
  - http://www.nist.gov/itl/csd/cloud-020111.cfm

# IBM Cloud Security Guidance

Based on cross-IBM research and customer interaction on cloud security

Highlights a series of best practice controls that should be implemented

Broken into 7 critical infrastructure components:

- Building a Security Program
- Confidential Data Protection
- Implementing Strong Access and Identity
- Application Provisioning and De-provisioning
- Governance Audit Management
- Vulnerability Management
- Testing and Validation

IBM

Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

## Cloud Security Guidance

### IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

### Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

**Note:** As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.





http://www.redbooks.ibm.com/abstracts/redp4614.html?Open

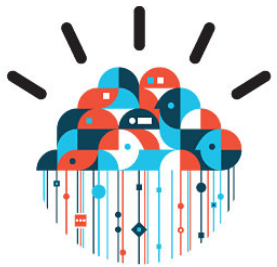
# Discussion

# Backup (Roles example)

# Thanks!

*Computing Clouds are like cats, they only obey to who feed them!*

arlindodias@pt.ibm.com




38