Identity Management for the Cloud

New answers to old questions

10. Anwenderkonferenz Softwarequalität, Test und Innovationen

6. und 7. September 2012
Alpen-Adria-Universität Klagenfurt

Dr. Horst Walther, Business Advisor Operational Risk Management
Member of the VCB & Company LLP, London,

agenda

1. Where is the problem?
   Why do we need to talk about IdM in the cloud?
2. The slow move towards the cloud
   The cloud did not come as a surprise
3. Finally the fortress security model fails
   But corporations had a hard time to accept the facts
4. Models, services & actors become standardised
   The NIST Conceptual Reference Model
5. Cloud Computing's deadly sins
   by Mike Small
6. Often IAM is meant when IM is said
   IAM = Identity Management (IM) + Access Management (AM)
7. IAM before & in the Cloud
   What changes for the consumer, when moving into the cloud?
8. OASIS view
   relevant standards & identified gaps
9. SCIM
   Simple Cloud Identity Management by IETF
10. IdMaaS - Identity Management as a Service
    Identity Management Moves into the Cloud
11. Management vs. governance
    A clear cut between hand-on management & governance is essential
12. Conclusion
    What changes, when moving into the cloud?

summary

- Since 10 years+ Identity Management in the cloud is discussed.
- However it offer few new challenges only.
- Neither did the cloud come as a surprise – nor does the requirement for managing identities.
- Rather in the cloud a development culminates that was expected since a long time.
- Quantitative shifts like higher complexity, more outsourced services & mobile and independent devices occur.
- They may well confront corporations with a new aulity – especially those which did not catch up with the steady development.
- There is a backlog of standardisation in various areas – with some gaps currently being filled (e.g. SCIM).
- However access management, audit & compliance have barely been touched so far. – The development just has started.

Where is the problem?

Why do we need to talk about IdM in the cloud?

Since 10 years+ we are discussing Identity Management in the cloud.

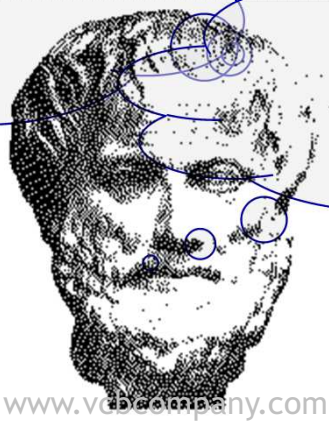
Obviously there seems to be a major issue.

But what makes the difference?

What are old – what are the new challenges?

How do the solutions look like?

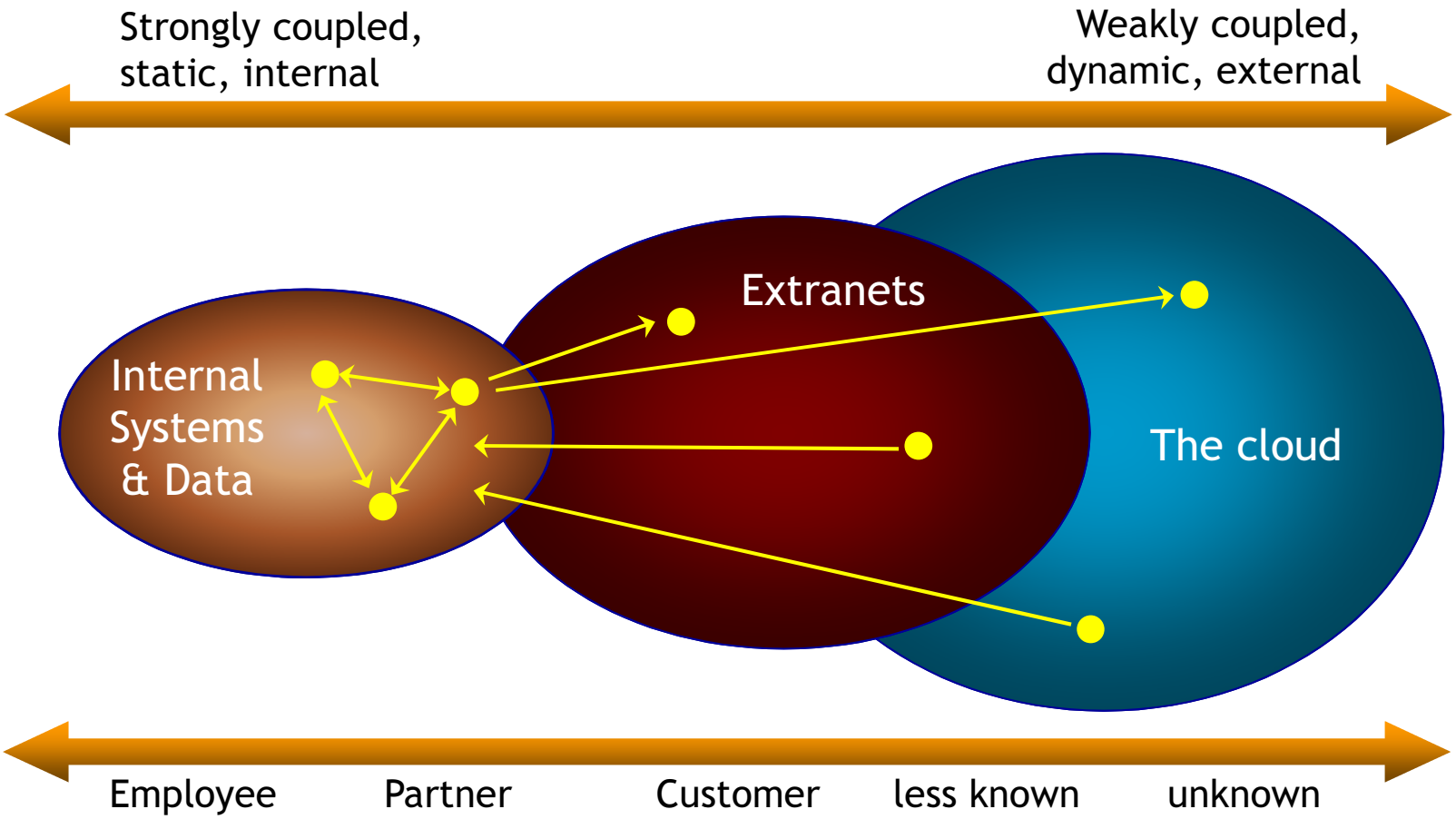
What is going on? What comes next?



The slow move towards the cloud

The cloud did not come as a surprise

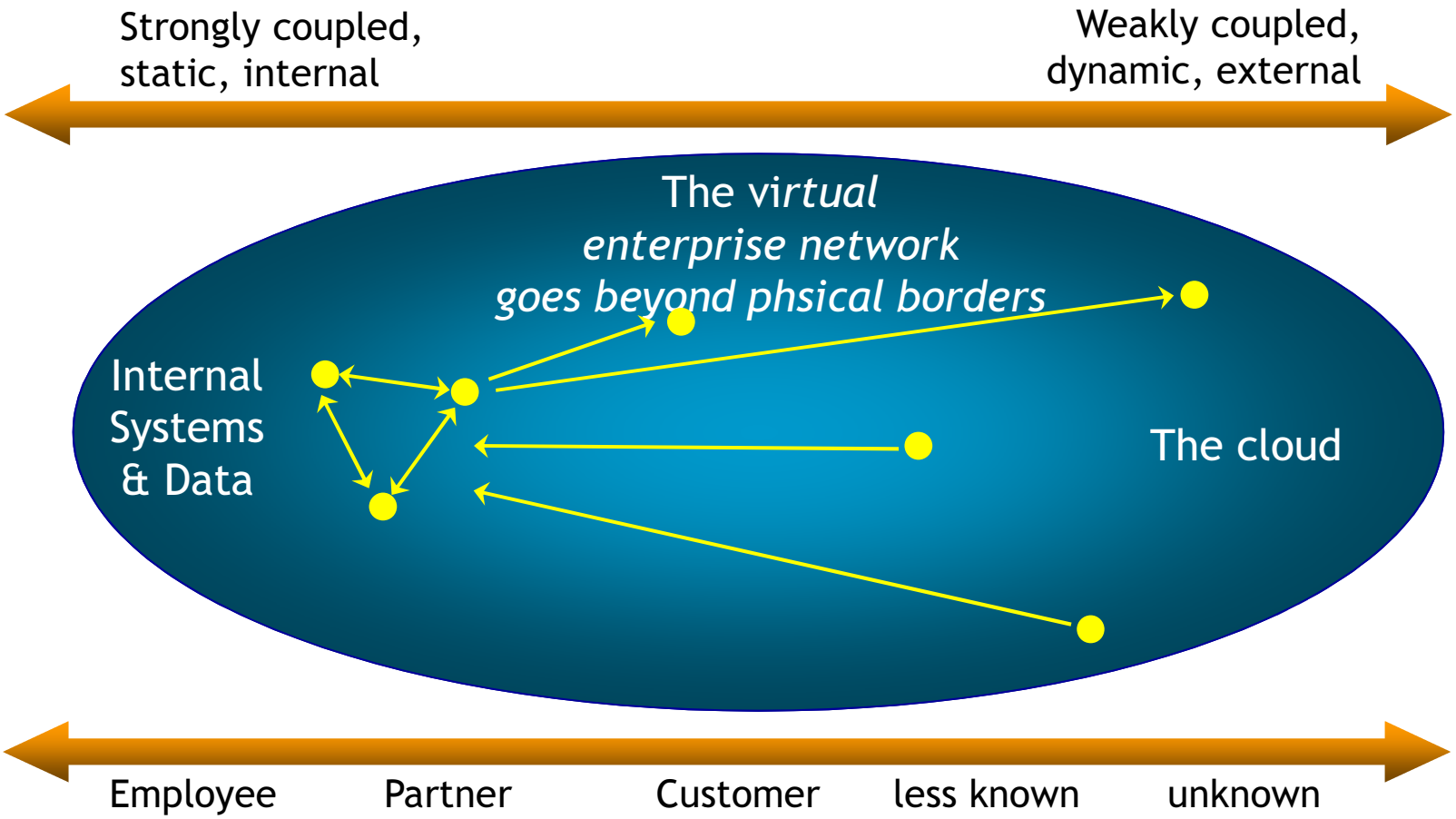
- The closed corporate perimeter is blurring
- There is a long-term move of sourcing internal services out



Finally the fortress security model fails

But corporations had a hard time to accept the facts

- The company perimeter is no longer the line of defence
- A virtual enterprise network requires asset centric security.



Challenges – The CIO's lament

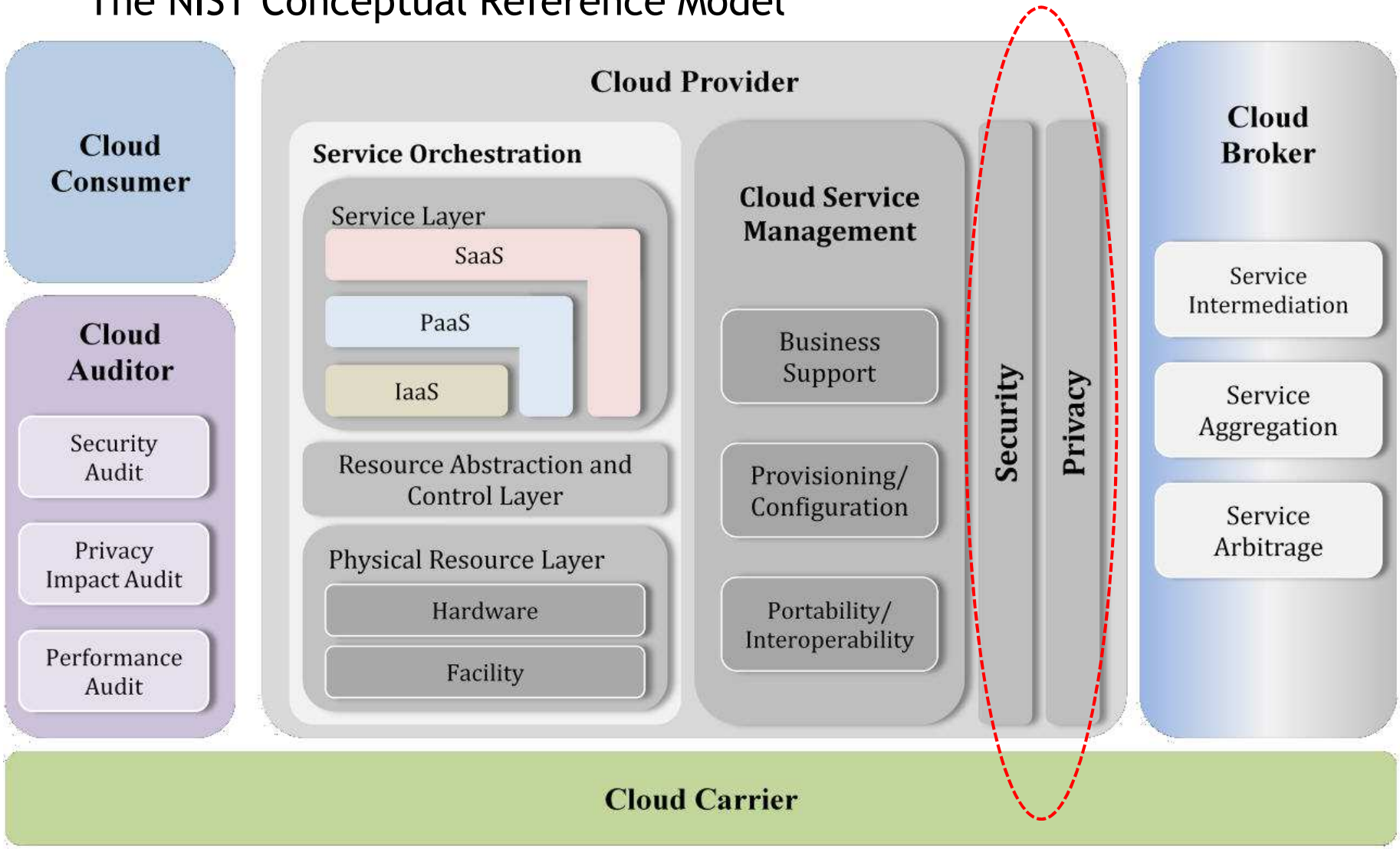
Complexity, cloud & mobile drove the change in the last 5 years.

- Increased **complexity**.
  - There are more things to connect,
  - More people to connect
  - With more data than ever before.
  - It's an end-to-end situation.
- The **role** of IT has changed
  - From being the custodians of IT to being brokers of IT.
  - The all-things cloud lures us.
  - The infrastructure is moving out of the (direct) control.
- The devices too are moving **out of control** the IT.
  - BYOD & mobile devices are incompatible with the perimeter security model
  - We go from managing by our hands on to governing via policies & audits.
  - But generally IT people are not good at governing

➔ *And the outlook is: More of the same.*

Models, services & actors become standardised

The NIST Conceptual Reference Model



NIST: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

The NIST Conceptual Reference Model

Cloud Computing obviously raises the overall complexity

- 5 major participating actors:
  - Cloud Consumer,
  - Cloud Provider,
  - Cloud Broker,
  - Cloud Auditor,
  - Cloud Carrier.
- 4 deployment models:
  - private cloud,
  - community cloud,
  - public cloud, and hybrid cloud.
- 3 service:
  - Cloud software as a service (SaaS),
  - Cloud platform as a service (PaaS),
  - Cloud infrastructure as a service (IaaS).
- 5 service characteristics :
  - on-demand self-service,
  - broad network access,
  - resource pooling,
  - rapid elasticity,
  - measured service.

Cloud Computing's deadly sins

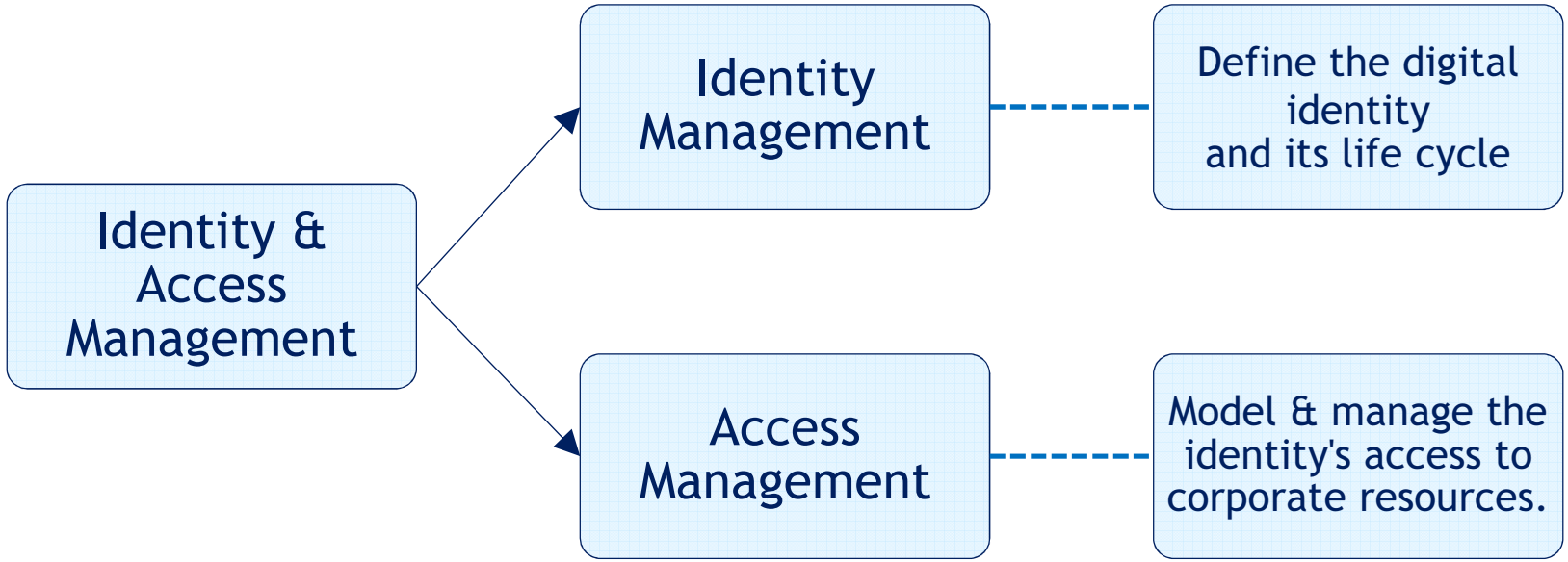
by Mike Small

- Adopting cloud computing can save money.
- But many organizations are sleepwalking into the cloud.
- Outsourcing the provision of the IT service does not outsource the customer's responsibilities.
- The deadly vice of cloud computing of is sloth by inattention to:
  1. Not knowing you are using the Cloud
  2. *Not assuring legal and regulatory compliance*
  3. Not knowing what data is in the cloud
  4. ***Not managing identity and access to the cloud***
  5. *Not managing business continuity and the cloud*
  6. Becoming Locked-in to one provider
  7. Not managing your Cloud provider
- Of these deadly sins of cloud computing #4 directly applies
- Indirectly affected are #2 & # 5

* In medieval times the Christian church created the concept of the seven deadly sins:
1. wrath, 2. greed, 3. sloth, 4. pride, 5. lust, 6. envy and 7. gluttony

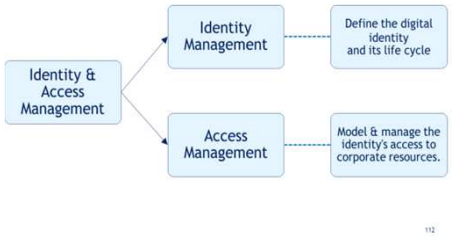
Often IAM is meant when IM is said

IAM = Identity Management (IM) + Access Management (AM)

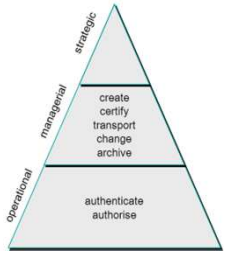


Grouping processes of the Identity- & Access Management

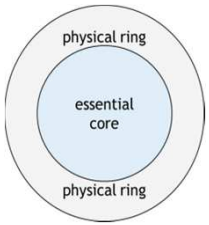
The IAM processes may be viewed from different perspectives*



- into Identity management & Access Management
  - Identity management has a justification sui generis.
  - It is not an appendix of security management
  - Access management can be built on top of Identity management



- into operational and managerial
  - operational: identify, authenticate and authorise
  - managerial: administer digital Identities
  - governance: supervise & direct



- into essential and physical
  - essential: administer and use the essential business functionality
  - physical: integrate, transport, transform and “provision” to deal with the “cruel dirty world” outside.

* www.GenericIAM.org

IAM before & in the Cloud

What changes for the consumer, when moving into the cloud?

Enterprise IAM	Cloud IAM
Mostly partial coverage	Total coverage necessary
Manual & automated processes	Full automation required
Proprietary application interfaces	Standardised interfacing
IAM roles may overlap	Clearly defined IAM roles
Individual, ad-hoc decisions	Policy driven decisions
SSO is a goody	SSO is essential
Hands-on management & governance not clearly separated	Mandatory separation of hands-on management & governance
Low process maturity suffices	High process maturity necessary
➔ *Running an IAM is recommended*	➔ *Running an IAM is mandatory*

Well – not much. But it has to be done now.

OASIS view

relevant standards & identified gaps

Identified relevant standards

- SAML
- OpenID
- OAuth
- SPML
- SCIM
- WS-Federation
- IMI
- (XACML) ?

Identified big / obvious gaps

- Configuration and association with an IdP is not standardized
- No standards or rules for mapping or transforming attributes between different (cloud) domains.
- No profiles or standard roles and related attributes
- No standards for attributes
- No audit standards for IDM systems

Where can the impact of the cloud be felt?

The OASIS 'identity in the cloud' use cases

OASIS formalized 29 cloud use cases out of (35 received)

- Infrastructure Identity Establishment
- Identity Management (IM)
  - General Identity Management
  - Infrastructure Identity Management (IIM)
  - Federated Identity Management (FIM)
- Authentication
  - General Authentication
  - Single Sign-On (SSO)
  - Multi-factor
- Authorization
- Account and Attribute Management
  - Account and Attribute Provisioning
- Security Tokens
- Governance
- Audit and Compliance

Impact on the Identity Management

OASIS: More emphasis on provisioning and configuration

- Speed - Rapid provisioning:
  - Automatically deploying cloud systems based on the requested service/resources/capabilities.
- Robustness - Resource changing:
  - Adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.
- Compliance - Monitoring and Reporting:
  - Discovering and monitoring virtual resources, monitoring cloud operations and events and generating performance reports.
- Transparency - Metering:
  - Providing a metering capability at some level of abstraction appropriate to the type of service.
  - e.g., storage, processing, bandwidth, and active user accounts.
- SLA management:
  - Encompassing the SLA contract definition
  - SLA monitoring and SLA enforcement according to defined policies.

SCIM

Simple Cloud Identity Management by IETF

- For provisioning user identity to cloud-based service providers.
- The SCIM protocol …
  - exposes a common user schema and extension model
  - is expressed in JSON (JavaScript Object Notation) or XML over HTTP
  - uses a RESTful (Representational State Transfer)-API.
  - maps to SCIM LDAP inetOrgPerson
  - binds to SAML
  - Is supported by several security software & cloud vendors
    - Cisco, Courion, Ping Identity, UnboundID and SailPoint; Salesforce, Google and VMware.
- Version 1.0 of the specification was approved in Dec. 2011.
- Proposed milestones …
  - mid. 2012: the SCIM core schema
  - mid. 2012: RESTful interface definition,
  - mid. 2012: use cases as a living document by the end of summer
  - mid. 2013: formalized SAML bindings
  - mid. 2013: LDAP mappings.

SCIM - Modes & Flows

CSP → CSP

Cloud Service Provider to Cloud Service Provider Flows

- Create Identity (Push)
- Update Identity (Push)
- Delete Identity (Push)
- Sync Identity (Push & Pull)
- SSO Trigger (Push)
- SSO Trigger (Pull)
- Password Reset (Push)

ECS → CSP

Enterprise Cloud Subscriber to Cloud Service Provider Flows

- Create Identity (Push)
- Update Identity (Push)
- Delete Identity (Push)
- SSO Pull

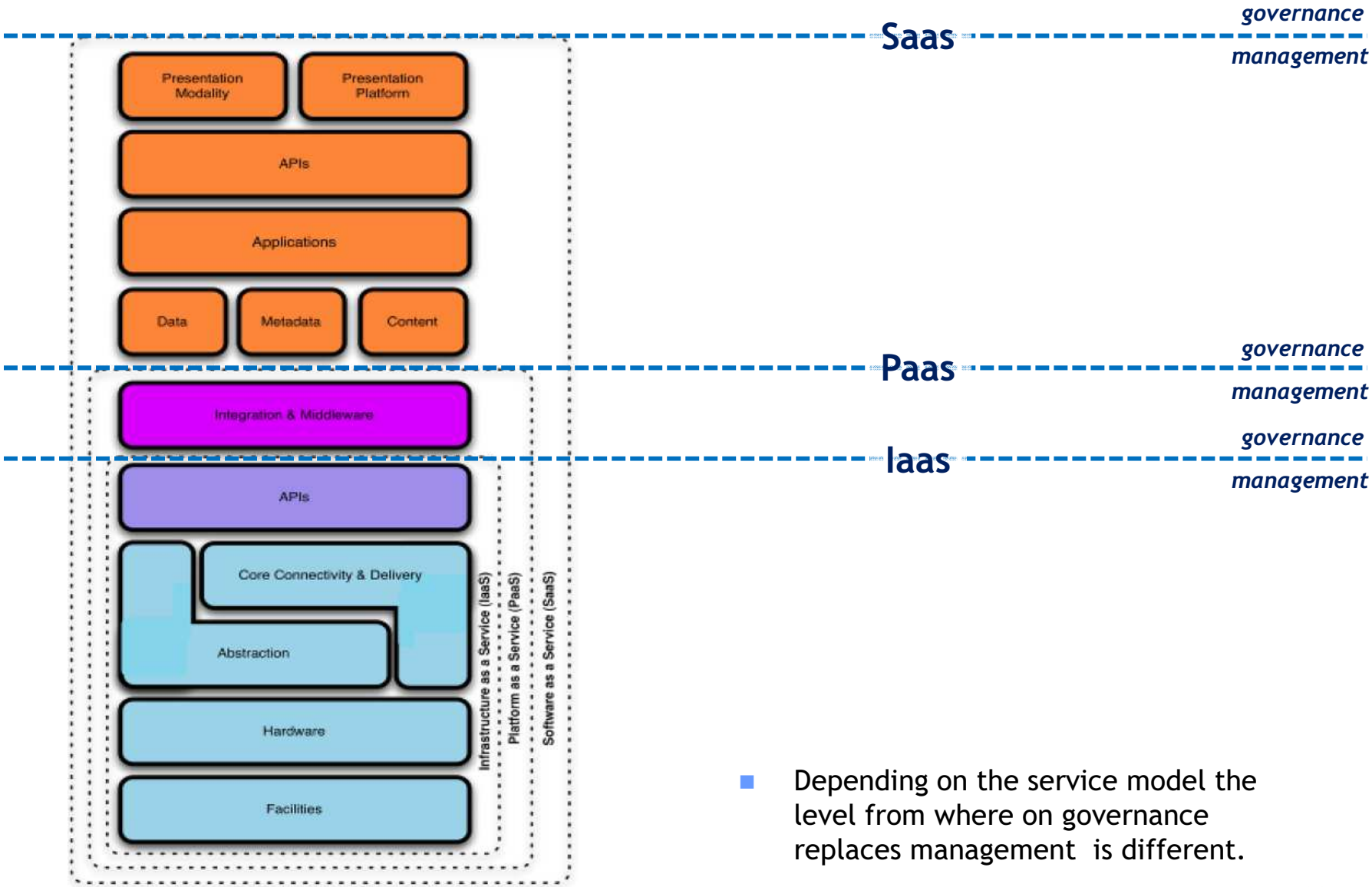
IdMaaS - Identity Management as a Service

Identity Management Moves into the Cloud

- IDMaaS = IdM + SaaS
- 10 key criteria to be considered:
  1. Be sure about the **service level agreements** (SLAs).
  2. Explore the **compliance** / liability ramifications
  3. Define how **control** will be shared?
  4. Plan and define the **interface** with the service provider.
  5. Consider the **applications** to integrate into the solution.
  6. Align your **security model** with the service provider.
  7. Understand the **business disruption** caused by the move.
  8. Explore the effort of **changing** back / to another provider
  9. Make sure your **provider** is the **right** one for IDMaaS as well.
  10. Consider the whole life **cycle costs** under different scenarios.
- If you confidently cover all 10 points you may move to IdMaaS

Management vs. governance

A clear cut between hand-on management & governance is essential



- Depending on the service model the level from where on governance replaces management is different.

Big Picture: the Context is
the Industrialisation of Service

Compliance

- Compliance enforces the use of infrastructure standards.
- ITIL is just the beginning – CoBIT, ValIT and others will follow.
- The cloud offers a framework for the implementation.
- ITIL, SOA, compliance frameworks are details of a bigger picture.

2 global forces change the environment.

enterprises

Standardisation
Automation
Modularisation
continuous improvement
core competences

Globalisation

- Market forces enforce the concentration on core competencies.
- Non-competitive activities will be standardised.
- They will be sourced globally at low prices,
- outsourced / cloud-sourced / off-shored

… or performed according to *best practice* reference models.

Conclusion

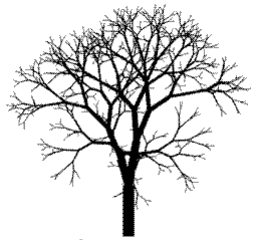
What changes, when moving into the cloud?

Well, not much!

- Moving to the cloud doesn‘t offer fundamentally new challenges.
- Full coverage, automation, single-sign-on, user-self-service, … should have been IAM feature before as well.
- Out-sourced & off-site running applications were in use since years.
- Cost pressure & increased complexity are the real differentiators
- They enforce one more step towards the industrialisation of services.

It‘s about …

Quantity → Quality



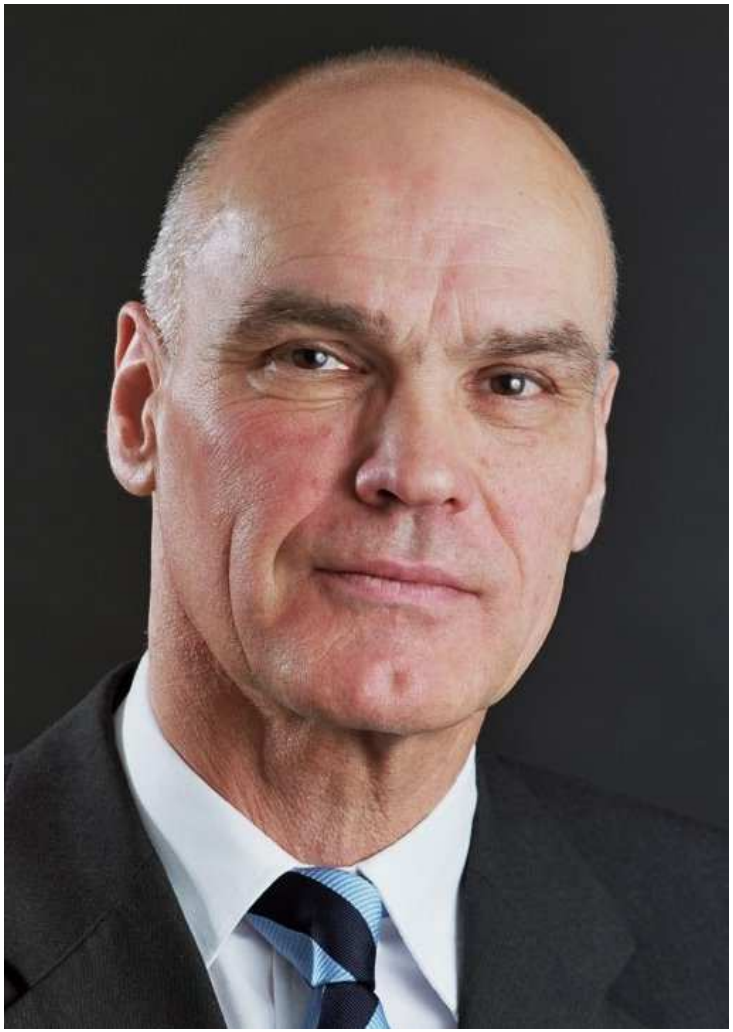
questions - acknowledgements – suggestions?

Attention
Backup slides

Standards

- SAML
  - Most mature, detailed, and widely adopted specifications family for browser-based federated sign-on for cloud users
  - Enables delegation (SSO)
  - Multifactor authentication
  - Support strong authentication and web SSO, avoid duplication of identity, and share only selected attributes to protect user privacy
  - Platform neutrality. SAML abstracts the security framework away from platform architectures and particular vendor implementations.
  - Business-to-business and employee-facing use cases
- Shibboleth
  - Led by Internet2 to provide peer-to-peer collaboration using a federated identity infrastructure based on SAML.
  - Huge adoption rate in university and research communities
- Liberty Alliance
  - An organization of vendors and enterprises that is largely perceived as having formed in response to Microsoft's Passport efforts.
  - Identity federation framework (ID-FF) and identity Web services framework (ID-WSF). Their ID-FF work, which has now been incorporated into SAML 2.0.
  - Provides testing services for SAML 2.0 as well as their own protocols.
- SPML
  - Emerging
  - Xml-based framework being developed by oasis for exchanging user, resource, and service provisioning information among cooperating organizations.
- XACML
  - XACML is an oasis-ratified, general-purpose, xml-based access control language for policy management and access decisions.
  - Xml schema for a general policy language, processing environment model to manage the policies and to conclude the access decisions.
  - A standard way to express authorization policies across a diverse set of cloud services and externalize authorization and enforcement from the application
- OAUTH
  - OAUTH is an emerging authentication standard that allows consumers to share their private resources (e.g., photos, videos, contact lists, bank accounts) stored on one csp with another csp without having to disclose the authentication information
  - Supported via an API by service providers including GOOGLE, TWITTER, FACEBOOK, and PLAXO
- OPENID
  - OPENID an open, decentralized standard for user authentication and access control, users can log on to many services with the same digital.
  - However trust issues remain
- WS-*
  - Driven by a collaborative effort between Microsoft, IBM, VeriSign, RSA Security, Ping Identity and others.
  - Composable suite of specifications for enabling secure Web services.
  - WS-Trust, WS-Federation, and WS-Policy are evolving mechanisms for layering authentication, authorization & policy across multiple security domains.

Dr. Horst Walther is a business advisor



- Horst Walther is member of the *VCB & Company, LLP.* in London.
  - +44 208 1237381
  - horst.walther@vcbcompany.com
- He focuses on…
  - due diligence, audits and potential analysis of the corporate IT,
  - The development and verification of IT-Strategies and
  - Change Management in the area of information technology.
- He studied chemistry, computer science, oriental studies and economics.
- He worked in various companies in the software development and IT management & advisory.