



## Cloud Governance

### *Benefits and value from Cloud Service & Security*

Berthing, Hans Henrik

*Publication date:*  
2013

*Document Version*  
Early version, also known as pre-print

[Link to publication from Aalborg University](#)

#### *Citation for published version (APA):*

Berthing, H. H. (2013). *Cloud Governance: Benefits and value from Cloud Service & Security*. Abstract from 7th Annual European grc summit, København, Denmark. <http://www.copenhagencompliance.com/>

#### **General rights**

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

#### **Take down policy**

If you believe that this document breaches copyright please contact us at [vbn@aub.aau.dk](mailto:vbn@aub.aau.dk) providing details, and we will remove access to the work immediately and investigate your claim.



# Cloud Governance

Sep 23-24, 2013

Radisson Blu, Scandinavia Hotel  
Copenhagen, Denmark

Name: Hans Henrik Berthing  
Position: Senior Advisor & Partner  
Company: Aalborg University &  
Verifica

# Agenda

- Benefits and value from Cloud Service
- Cloud Governance
- Maturity of Cloud Services – a study
- Security Perspectives in Cloud



# About me

- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- Service Audit Reports (ISAE 3402)
- Extensive experience with Financial Audit, Internal Audit, Internal Controls, SOX, IT Governance, IT Security and IT Assurance
- Instructor, facilitator and speaker
- Senior Advisor & Associated Professor Aalborg University
- Member of IT Advisory Board FSR-danske revisorer
- Member of ISACA IT Assurance Task force
- ISO Subject Matter Expert





# Business benefits of cloud computing

- Cloud strategies make the enterprise more efficient and agile.
- Cloud computing allows delivered services to be more innovative and more competitive.
- Cloud computing reduces overall operating costs.
- How confident can boards be that management plans will achieve these benefits?

# Value of Cloud Computing

- Shifting funding of IT from large capital investments (legacy IT assets) to operational expenses.
- Reallocating IT resources to core business activities.
- Easier and cheaper applications to implement, use and support.
- Increasing scalability and flexibility, enhancing the ability to respond to changing market conditions.
- Fostering innovation by shifting effort and resources from implementation projects to final product development.

# Governance and Change Issues With Cloud Computing

- Strategic direction of the business and of IT
- Changes to meet performance objectives
- IT is aligned with the business
- Systems are secure
- Risk is managed



# Governance Questions About Cloud

1. Do management teams have a plan for cloud computing?  
Have they weighed value and opportunity costs?
2. How do current cloud plans support the enterprise's mission?
3. Have executive teams systematically evaluated organizational readiness?
4. Have management teams considered what existing investments might be lost in their cloud planning?
5. Do management teams have strategies to measure and track the value of cloud return vs. risk?



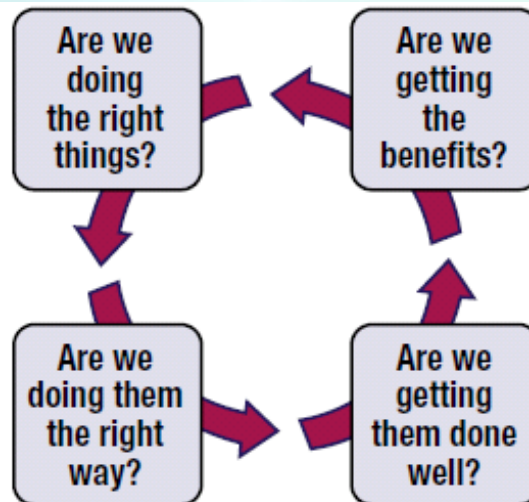
# VAL IT "Four Ares"

The strategic question. Is the investment:

- In line with our vision
- Consistent with our business principles
- Contributing to our strategic objectives
- Providing optimal value, at affordable cost, at an acceptable level of risk

The architecture question. Is the investment:

- In line with our architecture
- Consistent with our architectural principles
- Contributing to the population of our architecture
- In line with other initiatives



The value question. Do we have:

- A clear and shared understanding of the expected benefits
- Clear accountability for realising the benefits
- Relevant metrics
- An effective benefits realisation process over the full economic life cycle of the investment

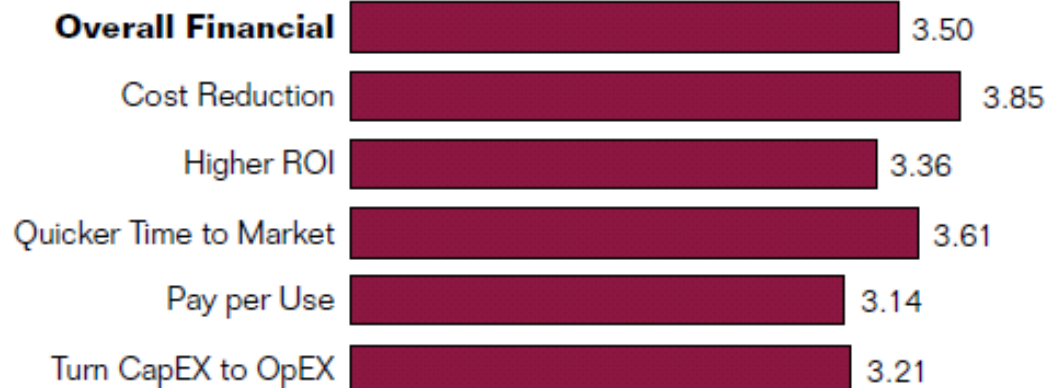
The delivery question. Do we have:

- Effective and disciplined management, delivery and change management processes
- Competent and available technical and business resources to deliver:
  - The required capabilities
  - The organisational changes required to leverage the capabilities

# Cloud Decisions



## Business Enablement



## Financial Performance



## Environment

Source: Cloud Computing Market Maturity Study Results, 2012, ISACA & CSA

# Primary driver for decision to use cloud computing? (n=543)

Frequently cited responses include:

- Cost reduction
- Greater efficiency
- Greater flexibility and access to data
- To keep pace with technology



# Cloud Computing Service Models

Service Model	Definition	To Be Considered
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider	<ul style="list-style-type: none"><li>• Availability</li><li>• Confidentiality</li><li>• Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite)</li><li>• Data ownership</li><li>• Concerns around e-discovery</li></ul>
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail).	<ul style="list-style-type: none"><li>• Who owns the applications?</li><li>• Where do the applications reside?</li></ul>

# Cloud Services Used and Satisfaction With Cloud

• Services	Used	Mean
• Infrastructure as a Service (IaaS)	35,7%	3,39
• Platform as a Service (PaaS)	22,6%	2,98
• Software as a Service (SaaS)	62,3%	3,66
• Scale 0 (Not satisfied) 5 (Highly satisfied)		





# Cloud Computing Deployment Models

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private cloud	<ul style="list-style-type: none"><li>• Operated solely for an organization</li><li>• May be managed by the organization or a third party</li><li>• May exist on-premise or off-premise</li></ul>	<ul style="list-style-type: none"><li>• Cloud services with minimum risk</li><li>• May not provide the scalability and agility of public cloud services</li></ul>
Community cloud	<ul style="list-style-type: none"><li>• Shared by several organizations</li><li>• Supports a specific community that has shared mission or interest.</li><li>• May be managed by the organizations or a third party</li><li>• May reside on-premise or off-premise</li></ul>	<ul style="list-style-type: none"><li>• Same as private cloud, plus:</li><li>• Data may be stored with the data of competitors.</li></ul>
Public cloud	<ul style="list-style-type: none"><li>• Made available to the general public or a large industry group</li><li>• Owned by an organization selling cloud services</li></ul>	<ul style="list-style-type: none"><li>• Same as community cloud, plus:</li><li>• Data may be stored in unknown locations and may not be easily retrievable.</li></ul>
Hybrid cloud	A composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	<ul style="list-style-type: none"><li>• Aggregate risk of merging different deployment models</li><li>• Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.</li></ul>



Source: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, ISACA

# Cloud computing plan? (n=914)

	We do not use it for any IT services.	We use it for low-risk, nonmission-critical services.	We use it for mission-critical services	Unsure
Public cloud	<b>63%</b>	22%	3%	12%
Private cloud	<b>34%</b>	27%	26%	13%
Hybrid cloud	<b>55%</b>	15%	4%	26%



Source: IT Risk/Reward Barometer: Europe, 2012, ISACA (n=980)

# True about private cloud, public cloud and hybrid cloud (n =904)

	The benefit outweighs the risk.	The risk outweighs the benefit.	The risk and benefit are appropriately balanced.
Public cloud	12%	<b>68%</b>	20%
Hybrid cloud	16%	40%	<b>44%</b>
Private cloud	<b>57%</b>	10%	33%



Source: IT Risk/Reward Barometer: Europe, 2012, ISACA (n=980)

# Business Benefits of Cloud Computing

- Cost containment
- Immediacy
- Availability
- Scalability
- Efficiency
- Resiliency



# Tangible Cloud Benefits

Benefit	Description
<b>Tangible</b>	
Cost reduction	Computing cost is shifted from a capital expenditure to an operational cost because the cloud provider supplies the underlying infrastructure as part of the service bundle. In addition, the cloud promises a cost reduction in the following areas: <ul style="list-style-type: none"><li>• Labor—IT system administration hours/headcount</li><li>• Application software (SaaS only)</li><li>• Licensing purchase and maintenance</li><li>• Technical support and user support</li><li>• Maintenance (upgrades, updates, patches, etc.)</li><li>• Hosting (physical building, power, cooling, etc.)</li></ul>
Enhanced productivity	User mobility and ubiquitous access can increase productivity. Collaborative applications increase productivity and reduce rework.
Optimized resource utilization	Enterprises use only the computing resources they need, thus reducing system idle time waste.
Improved security/compliance	Cloud providers may offer robust security controls as a market differentiation.
Access to skills and capabilities	Customers benefit from top-notch skills and capabilities while avoiding employment costs (recruiting, salary, benefits, training, etc.).
Scalability	On-demand provisioning or computing resources eliminate the cost of capacity planning.
Agility	Agility contributes to cost reduction and productivity enhancement due to faster provisioning of systems: <ul style="list-style-type: none"><li>• Faster application deployment (SaaS)</li><li>• Faster application development/testing (PaaS)</li></ul>
Customer satisfaction	Effective utilization of cloud applications can increase collaboration between the enterprise and its customers or reduce response time to customer inquiries.
Reliability	Cloud providers have redundant sites that can address business continuity and disaster recovery in a more efficient manner.
Performance	Better performance and up-time can result from continuous and consistent operations monitoring by the cloud provider.

Source: ISACA Cloud Computing Vision Series White Paper July 2012



# Intangible Cloud Benefits

Benefit	Description
<b>Intangible</b>	
Avoidance of missed business opportunities	A cloud application (SaaS) may be the critical element to land a new business or expand into new markets.
Focus on core business	IT resources can be allocated to support core business functions.
Employee satisfaction/innovation	Mobility and faster performance can improve employee satisfaction and boost innovation.
Collaboration	Real-time collaboration can increase quality and innovation.
Risk transfer	Some risk can be transferred to the CSP (e.g., security breaches, data loss, disaster recovery); this could represent a tangible or intangible benefit.



Source: ISACA Cloud Computing Vision Series White Paper July 2012

# Business Challenges to Consider

Challenge	Description
Incompatibility	Cloud services may not be compatible with the existing IT infrastructure or specific systems that must be integrated.
Uptime	Cloud vendors may not be able to guarantee agreed-on uptime. In addition, uptime may be impacted by other factors, including the customer's Internet service providers.
Performance	Multitenant models can degrade performance over time if capacity is not properly planned. Internet speed can also negatively impact performance.
Security	Cloud computing represents traditional and new risk that must be accounted for and mitigated accordingly (either by the CSP or the customer).
Compliance	The ubiquitous and abstract nature of the cloud can cause an enterprise's transition from compliance to noncompliance without any notice.
Pay-as-you-go	The enterprise must implement controls to avoid overage charges incurred when systems stay connected after a demand spike is over.
Lock-in (hardware or vendor)	Customers may become locked into a specific technology or a specific cloud vendor, which can prevent portability.
Cloud consumerization	Business units may be able to procure cloud services without involving IT. To prevent this situation, the enterprise must adapt its governance framework to control cloud services procurement.
Limited customization (Black Box)	Cloud applications may not be customized every time the business process changes, making the business process a "Black Box" due to costs associated with each modification or application limitations.



Source: ISACA Cloud Computing Vision Series White Paper July 2012

# Risks and Security Concerns With Cloud Computing

- Reputation, history and sustainability of the provider
- Failure to perform to agreed-upon service levels
- Where information actually resides
- Third-party access to sensitive information
- Compliance to regulations and laws in different geographic regions (Public Clouds)
- Information may not be immediately located

# Enterprise's biggest concern about cloud computing? (n=588)

Frequently cited responses include:

- Loss of control of the data
- Data security, privacy and confidentiality concerns
- Availability concerns
- Compliance issues
- Legal issues



# Assurance Considerations

- Transparency
- Privacy
- Compliance
- Trans-border information flow
- Certification





# Cloud Market Maturity Model

**Table 1—Cloud Market Maturity Model**

Stage	Distinguishing Elements of the Cloud Market
Infancy	The market is small with a potential for growth and innovation that has not been realized. The definition of cloud and related roles and responsibilities is not clear. ROI is uncertain. Users and providers can be considered early adopters.
Growth	The market demonstrates significant adoption, rapid growth, and notable innovation in terms of product offerings and use. Definitions of cloud computing and how it can be leveraged are clear. Roles and responsibilities for cloud within the enterprise have evolved to address cloud's unique aspects. Cloud computing is being integrated into core business activities. ROI is clear and examples of successful use are well known. Innovation leads to new product offerings not possible in earlier stages.
Maturity	Market growth has reached its peak. The level of innovation is slowing. New entrants have a difficult time distinguishing themselves from established service providers. Organizational roles and responsibilities are stable, as are relations between users and providers. Cloud computing is business as usual.
Decline	The cloud market is saturated with suppliers. Cloud computing is a commodity. Market leaders are clearly defined. There is little room for new entrants or new product offerings. Users and providers are looking for the next big opportunity.



Source: Cloud Computing Market Maturity *Study Results*, 2012, ISACA & CSA

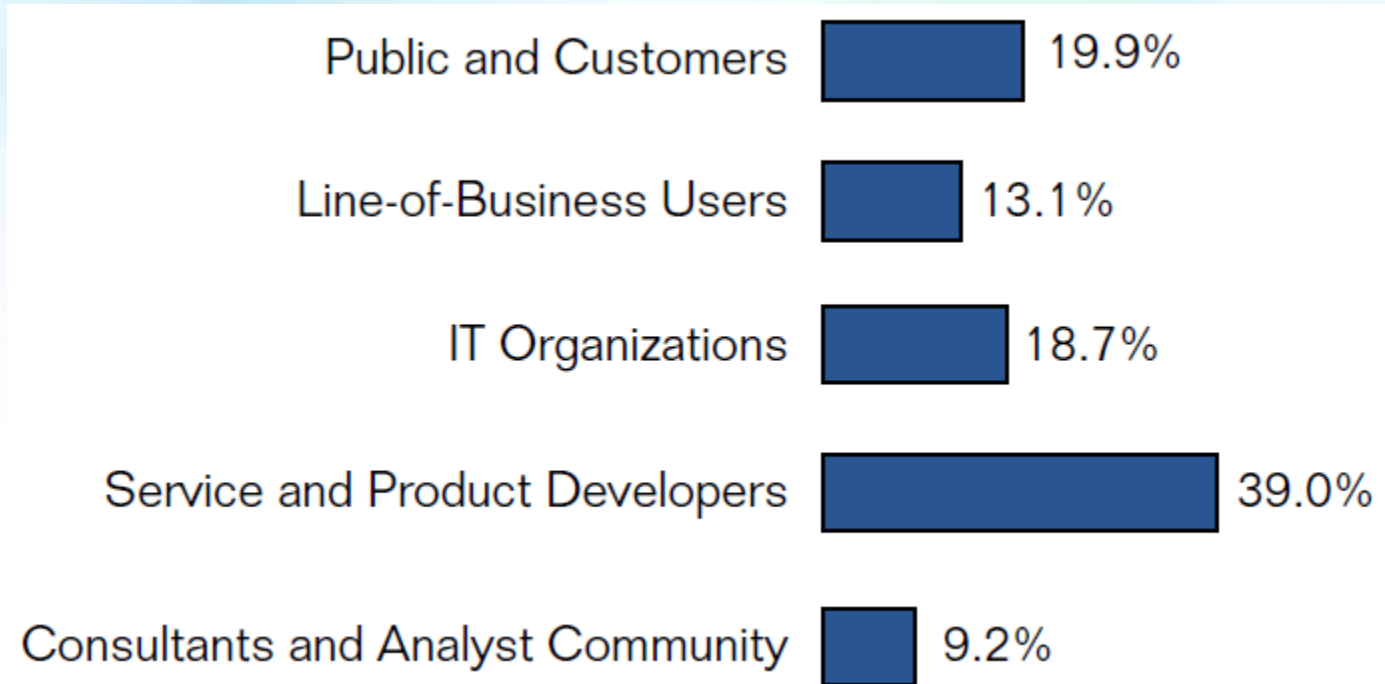
# Cloud Market Maturity

- Time to reach Maturity level



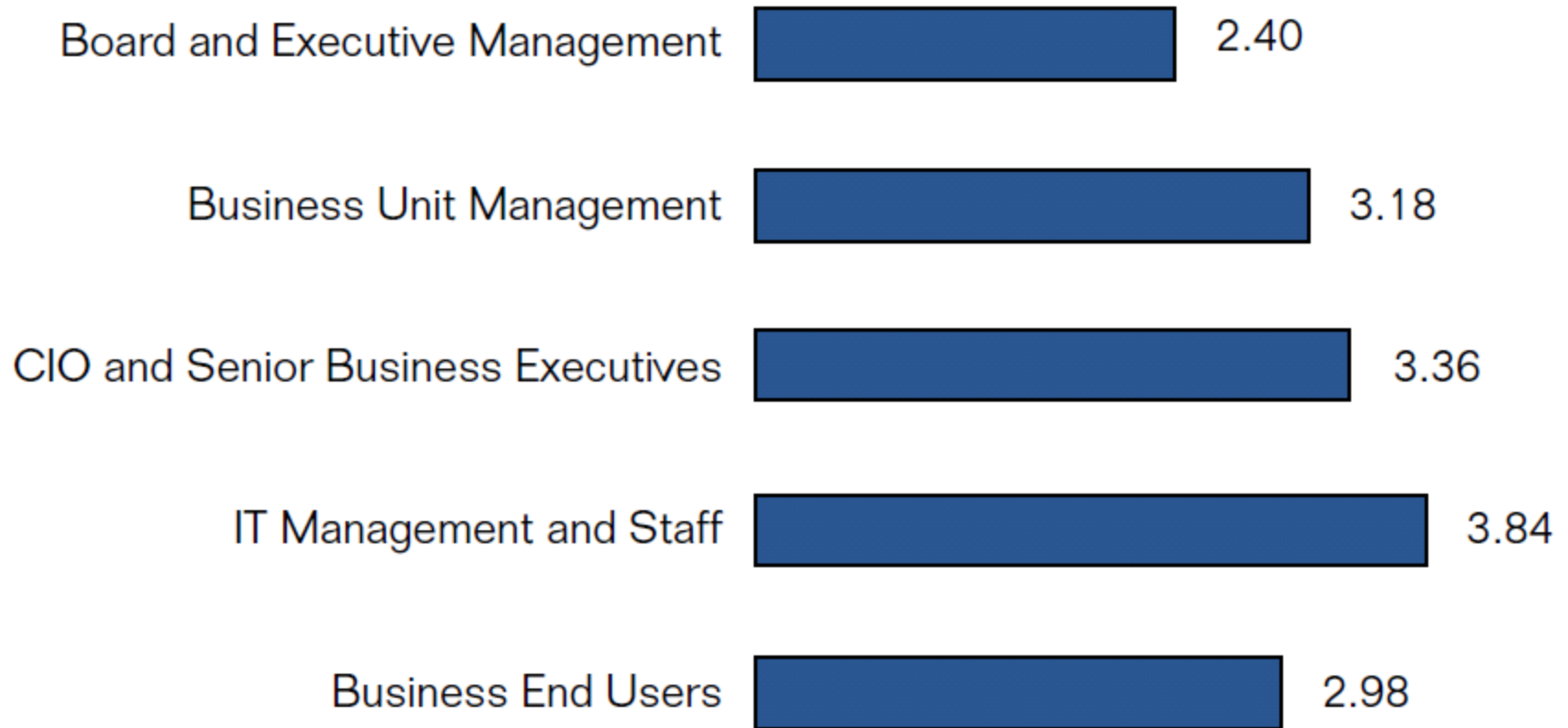
- 23,7-26,5% more than 5 years for maturity level

# Groups Driving Cloud Innovation



Source: Cloud Computing Market Maturity Study Results, 2012, ISACA & CSA


# Mean Scores of Business Group Influence on Cloud Innovation



0 (no influence) to 5 (significant influence).

# Cloud Support for Business Goals

Goal	Rank	Mean Score
Experiment with new technologies	1	 3.58
Provide new services to enhance worker effectiveness and efficiency	1	 3.58
Experiment with new ways of engaging with customers	2	 3.53
Take new ideas to market	3	 3.43
Provide access to best-in-class tools and capabilities	4	 3.25



Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*



# Positive and Negative Influences on Cloud Adoption and Innovation

Positive Influence on Cloud Adoption/Innovation	Mean Score	Rank	Negative Influence on Cloud Adoption/Innovation	Mean Score	Rank
Cost management <b>Proces</b>	3.77	1	Information security	4.22	1
Agility <b>Bus Growth</b>	3.75	2	Data ownership/custodian responsibilities	4.12	2
Time to market <b>Bus Growth</b>	3.73	3	Legal and contractual issues	4.04	3
Efficiency <b>Proces</b>	3.65	4	Regulatory compliance	4.01	4
Productivity <b>Proces</b>	3.61	5	Information assurance	3.77	5
Business unit demand <b>Bus Growth</b>	3.55	6	Longevity of suppliers	3.44	6
Resilience <b>Proces</b>	3.52	7	Contract lock-in	3.42	7
New technology <b>Bus Growth</b>	3.46	8	Performance standards	3.30	8
Customer demand <b>Bus Growth</b>	3.42	9	Disaster recovery/business continuity	3.25	9
Technical resources <b>Proces</b>	3.37	10	Performance monitoring	3.21	10
New markets <b>Bus Growth</b>	3.33	11	Technology stability	3.10	11
Summary Mean	3.56		Summary Mean	3.62	

Source: Cloud Computing Market Maturity Study Results, 2012, ISACA & CSA

# Problem Resolution Components in the Confidence Barometer

Problem Resolution Component	Mean Score	Rank
Continuity/availability	2.89	1
Performance	2.53	2
Problem management	2.42	3
User-supplier relationship	2.35	4
Solution integration	2.31	5
Security/assurance	2.25	6
Contracts	2.07	7
Regulation and legislation	2.06	8
Overall	2.37	



Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*

# Perspectives on Security and Assurance Components

Security and Assurance Component	Overall Rank	User Rank	Provider Rank
Concerns for multitenancy	10	12	11
Information security	12	7	17
Testing and assurance	18	18	18
Data ownership/custodian responsibilities	22	22	23
International data privacy	25	25	26

Security and Assurance Component	Overall Rank	Business Rank	Security Rank	Technology Rank
Concerns for multitenancy	10	13	15	8
Information security	12	11	14	13
Testing and assurance	18	22	10	21
Data ownership/custodian responsibilities	22	23	23	19
International data privacy	25	25	27	25



# Summary

- Ready to articulate the pros and cons.
- Where and how to add value for the business.
- Organization of any scale can go to the cloud.
- Enterprises will use some form of cloud when matured
- BOD's provide guidance to realize the benefits, optimize the risk and control the cost.
- Ask cloud-specific questions.
- Cloud computing are aligned to the enterprise strategy.
- Understand expected benefits and the mechanisms to track and measure them.
- Security and assurance.



# Thank You

- Hans Henrik Berthing,
  - Senior Advisor
- CPA, CRISC, CGEIT, CISA CIA
  - Phone: +45 35 36 33 56
  - Mobile: +45 22 20 28 21
- Mail: [hhberthing@verifica.dk](mailto:hhberthing@verifica.dk)



# Public Cloud

nControl has realized the following benefits from using SaaS solutions:

- A degree of cost savings (US \$2,000 a year) on desktop-based software
- An ability to remain focused on its core competency
- Improved time to market for the organization, dropping to within hours for establishing new accounts, services and/or business partnerships

Other cloud delivery models as well, specifically Platform as a Service (PaaS).

- Requires more involvement from the cloud consumer;
- More flexibility and agility than the traditional software model for delivery of computational resources.

Also challenges with using the cloud,

- Costs associated with using PaaS-based databases
- A backup and/or snapshot of the data on that database cannot be ported over easily to another provider.

The firm relied upon the CSP having relevant certifications and assertions eg. (ISAE3402), (ISO 27001), and the US Department of Commerce (Safe Harbor).





# Community Cloud

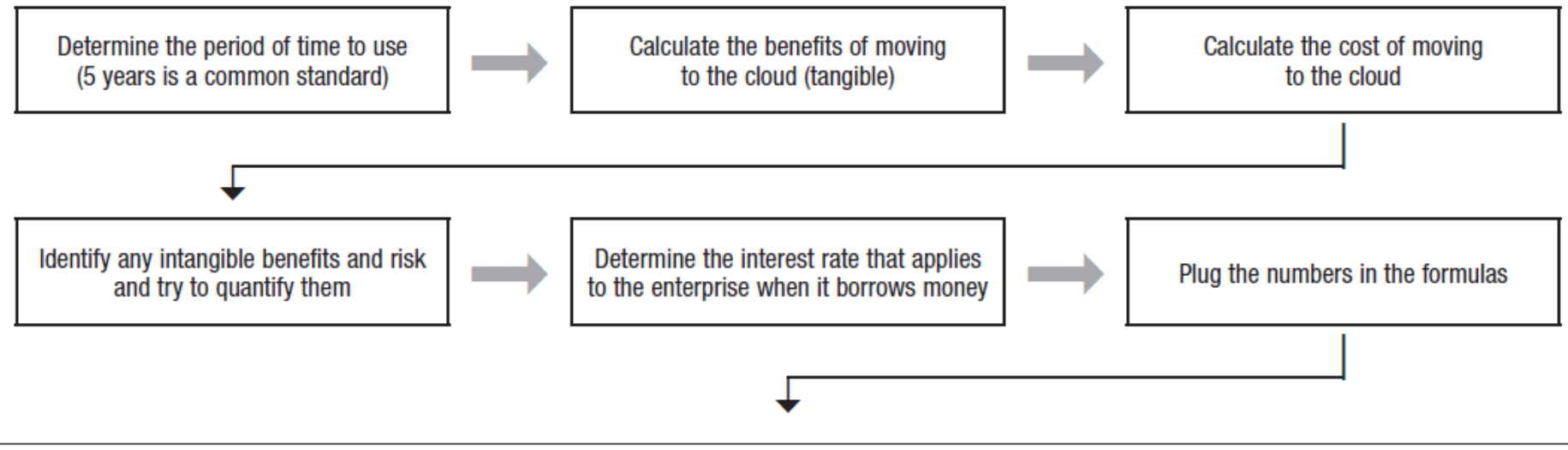
- One's smallest client may be its largest consumer
- A particular service (e.g., videoconferencing) may be a surprise hit
- The delivery of a blended hardware/software solution set may be appropriate in order to receive the maximum return on investment (ROI)
- A service that may have been cost-prohibitive before may be cost-effective in a cloud environment
- Collaboration (with stakeholders) is key to enhanced participation
- Community cloud consumers should not underestimate the economies of scale/cost efficiencies that can be reached by deploying a community cloud
- An organization should focus on its core competency/technical skill set, thus enabling the use of these different skill sets throughout the conglomerate
- An organization can leverage a community cloud for necessities, such as disaster recovery (DR)
- Community clouds leverage a grassroots approach for stakeholder buy-in
- Leverage security and privacy controls to mitigate risk.

# Hybrid Cloud

- Pfizer uses a hybrid cloud for additional computational power during worldwide research and development (WRD) efforts, such as FDA trials and human genome research.
- An external private cloud Infrastructure as a Service (IaaS) delivery model offering—Amazon Web Services' (AWS) Elastic Compute Cloud (EC2) in addition to the Virtual Private Cloud (VPC)—for additional resources when needed.
- The benefit of an external private cloud for additional computing power is the elasticity of the cloud.
- To mitigate the risk and comply with FDA and national and/or statutory jurisdictional data privacy regulations, the organization uses encryption, virtual firewalls/networks, network and system monitoring, and identity and access management (IAM) mechanisms.
- Various controls to ensure the security and privacy of such regulated data, the organization observes a different level of cost savings than other industries.
- FDA trials ebb and flow during the course of business in the pharmaceutical industry year by year, the flexibility and the agility to provision and/or deprovision resources are of paramount importance.
- New technologies such as homomorphic encryption, which allows for computations to be executed on native ciphertext are introduced, the ability of heavily regulated industries to do faster computational processing in the cloud will increase.

# ROI Framework in practise

## ROI Framework in Practice



$$\text{TCO} = \text{Upfront cost} + \text{Recurring cost} + \text{Termination cost}$$

$$\text{ROI} = \frac{(\text{Tangible benefits} + \text{Intangible benefits}) - (\text{Upfront cost} + \text{Recurring cost} + \text{Termination cost})}{(\text{Upfront cost} + \text{Recurring cost} + \text{Termination cost})}$$