DRAFT V1.0

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Exploring the Future of Cloud Computing

* Phase II *

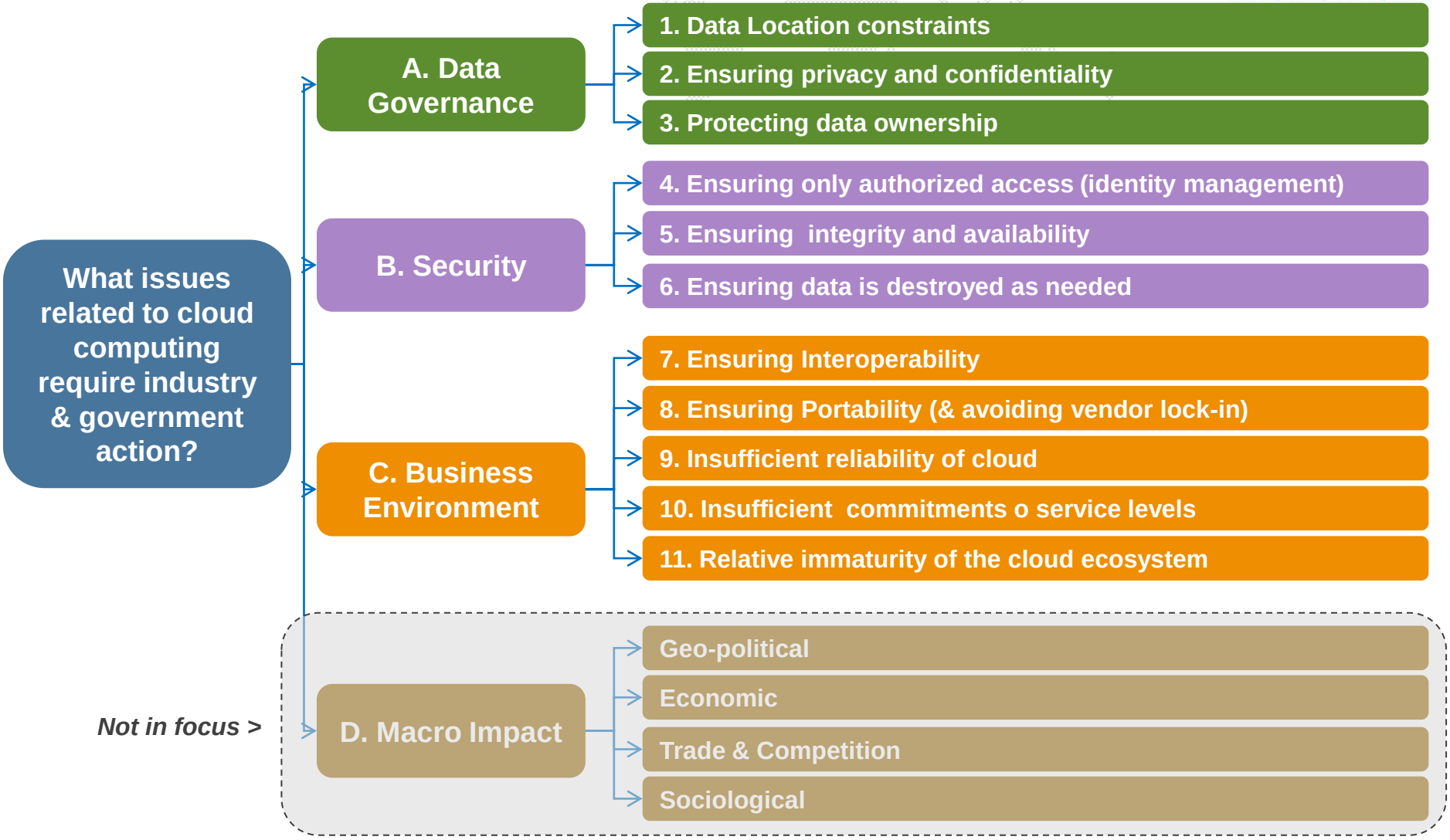
Stakeholder consultation: key issues for discussion

November 2010

Cloud Issue Tree

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE



Source: Davos 2010, Forum Workshops, Working Group calls

List of KEY issues to address

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

A. Data Governance

1. **Data location** constraints
2. Ensuring **privacy and confidentiality**
3. Protecting **data ownership**

B. Security

4. Ensuring only authorized **access** (identity management)
5. Ensuring **integrity and availability**
6. Ensuring data is **destroyed** as needed

C. Business Environment

7. Ensuring **Interoperability**
8. Ensuring **Portability**
9. Insufficient **reliability** of cloud
10. Insufficient commitments to **service levels**
11. Relative **immaturity** of the cloud ecosystem

Note: more issues may be added during the workshop and leading to Davos

Data Governance

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #1: Data location* constraints

Issue description

Conflicting and unclear constraints on where public cloud data can be located or stored

Why it's important:

- *Data location can create trans-border jurisdictional complications*
- *Protectionism might limit providers' freedom and increase their costs*
- *Customers are concerned about political risk when the data is stored in a foreign country*
- *Data in the cloud may have more than one legal location at the same time*

Key Considerations

Industry & Customers

1. Industry needs more clarity around the **different jurisdictions** and legal obligations in each country
2. As cloud opens up collaboration across multiple organizations in multiple locations (or jurisdictions) it is not clear **which data location requirements prevail**
3. When limits are imposed on data location, costs increase comes into consideration with the risk of **losing economies of scale** and being prevented from having data centers in low cost locations
4. Some believe that data location constraints (keeping data within national boundaries) are really a form of **protectionism**
5. Industry is concerned that the government is entering an "arms race" where different political constituencies will want to **develop their own rules**
6. Data restriction creates **obstacles to** internal and external **collaboration**

Government

1. The actual issue is which **jurisdictional law** applies: depending on where the data is, different security obligations will be enforced
   - EU needs to establish who controls the data (who is responsible and liable), where they are established and which equipments are used
   - US takes sectoral (e.g. Healthcare) approach with overarching consumer protection law
2. Some gov't reps view the risk of losing control over **IP** (intellectual property), **trade secrets**, etc. as a concern that prevents companies from transferring data to the Cloud.
3. Politicians are focused on data location and some are reluctant to move to the Cloud because of the potential **job-cuts in IT**
4. Government feels the need to **protect** their (not always knowledgeable) **citizens**

** Data location is both the physical/geographical location of the data as well as the jurisdictional and legal pertinence of the data.*

Data Governance

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #1: Data location constraints (cont'd)

Potential recommendations

i. Voluntary adoption of **best practices** (e.g. EU endorsement of binding corporate rules and model contracts; APEC model to facilitate free flow of information; Canadian accountability model)

ii. International agreements

- **International treaty** to govern where data is stored and how it is protected (e.g. Bretton Woods type convention to orchestrate data movements) via a series of bi-lateral or multi-lateral agreements and free trade talks
- Creation of a cloud **economic zone** (data haven) where accountability is clear
- Independent '**safe harbor'** in a neutral third country (stated in ICT 2010 Brussels conference)
- Expansion of the **'safe harbor '**agreement

iii. Agreement around **what should be in contracts and agreements** vs. policy

iv. Universal agreement around the **categorization of sensitive data**

v. Industry to agree to **voluntary safeguards** or commit to keep data within a **small number of jurisdictions**

vi. Implement **"privacy by design"**, provide trust marks, enforce visibility and data disclosure (such as where the data is located)

Questions and next steps

1. How can monetary, privacy, customer protection, jurisdictional, philosophical, political differences be overcome in creating an international treaty?
2. Would a small non-controversial country work to act as a "data haven" or are we discussing a "virtual" zone?
3. Can we quantify the impact of the problem?
4. How safe harbor best practices be applied to the cloud?
5. Where is the best research on these topics?

Data Governance

Issue #2: Ensuring privacy* and confidentiality*

Issue description

Lack of clarity on requirements and approaches for ensuring privacy and confidentiality when data is stored in the cloud

Why it's important:

- *The use, storage and disclosure of personal, business or government information is perceived to be riskier in the cloud*
- *Users' privacy and confidentiality risks may depend on the providers' architecture and privacy policies*
- *Government and laws could force a cloud provider to share user data*

Key Considerations

Industry & Customers

1. Defining, addressing and isolating ***sensitive* data** are important though extreme data segregation might not be efficient from a cost perspective
2. There are additional privacy & confidentiality risks when the data (even non-sensitive data) is **linked and connected** out of context
3. Some service providers are concerned that placing usage limitations on customer data (including usage patterns) might **hinder innovation**, new features, and improved services.
4. The **data controller** has different responsibilities from the data processor and in many cloud implementations it's not clear who is a processor and who is a controller *(Note: the provider/controller concepts are not universal nor fully mature)*
5. The definition of what constitutes **"sensitive" data** varies by country

Government

1. There is a need to **differentiate personal and non-personal** data to clarify which law applies
2. **An International treaty** on data protection is very **unlikely** due to the range of issues such as tax collection and privacy rules and fundamental philosophical and political differences are so high
3. With varying degrees of standards and levels of protection, **providers cannot be trusted** uniformly to protect data in the Cloud (however the market will sort out un-trusty providers)
4. Government is pressed to mitigate uncertainty and create more **user awareness** of privacy protection. They are sometimes concerned about providers **offloading liability** to 3rd parties.
5. Information stored on computers is, in most cases, entitled to certain **protection** (*e.g. US: 4th amendment & Electronic Communications Privacy Act*) however, it is debatable whether information stored remotely/virtually is entitled to the same protections or not.
6. Because of these concerns, some governments **recommend to only use private cloud** services, stating that public clouds can only be used safely with non-essential data.

**Privacy is the condition of being free and protected from unauthorized intrusion*
**Confidentiality is ensuring the privacy of others and ensuring only authorized people have access it*

Data Governance

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #2: Ensuring privacy and confidentiality (cont'd)

Potential recommendations

i. **Awareness & Transparency**
   - **Clearer, transparent provider policies and practices** to better assess the privacy and confidentiality risks users face; explicit internal accountability programs by cloud providers could go a long way at creating trust and avoid increased regulatory action
   - Encourage **users to be more aware** and vigilant

ii. Implement the **"privacy by design" approach**, provide trust marks, enforce visibility and data disclosure (such as where the data is located)

iii. A **mechanism** for Cloud service providers to disclose certain **levels** of cloud security and confidentiality (e.g. level 0 to level 10)

iv. **Harmonizing and consolidating** the approach of the **various bodies** that are working on privacy & confidentiality

v. Provide **clarity** around which **private records** should be protected contractually versus regulation (refer to existing examples: Health Insurance Portability and Accountability Act ("HIPAA") and Gramm-Leach-Bliley Act ("GLB") with respect to service terms for health records and personal financial information)

vi. **New architectural models**, such as remote managed cloud appliances

vii. Industry to take a more **proactive stance on self-regulation** (e.g. via accountability models). In essence companies could create global data protection laws generating **de-facto standards**

viii. Appointing **data protection officers** within companies

Questions and next steps

1. There are many organizations focusing on privacy & confidentiality in the cloud (OECD: Organization for Economic Cooperation and Development, data protection commissioners around the world, the US department of commerce, ISO, Cloud Security Alliance, etc.). Which ones are creating applicable recommendations?
2. How can the EU-US "safe harbor principles" be made more relevant to the cloud by going beyond the EU-US limitation?
3. Maybe the informing principle can be "privacy by default"? How do we approach a revision of the data protection directives?
4. In terms of making liability disclosure more visible to the user, can we use a layered approach (essential information first, then full document later)?

Data Governance

Issue #3: Protecting data ownership

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue description

Governments and customers are concerned that data may be stolen or lost; industry is concerned about the government's lack of policy clarity.

Why it's important:

- *Data ownership might be affected by the cloud. It s not clear who owns the data (client, service provider, etc.)*
- *Law enforcement and gov't access can, in some cases, by-pass data ownership*
- *Ensuring proper access and monitoring access (who, how, when) are fundamental requirements by customers*
- *In the current economy data is seen as an economic good that can be exchanged (data as currency) , which hinders considerations around privacy and ownership*

Key Considerations

Industry & Customers

1. Inherently data ownership is also tied to data location and data privacy, however, data ownership can also refer to **meta-data and time of use** of data
2. Industry is very concerned about how and under what circumstances will **government and law enforcement access data** (government access; law enforcement; litigation; trans-border regulations)
3. Industry is unsure how to address potential **conflict of laws** issue regarding **law enforcement access** (different laws in different jurisdictions)
4. The cloud may affect **licensing and IP models** due to the uncertainty in data ownership

Government

1. Difficulty to **differentiate types of data** and what is personal data or not
2. Lack of agreement of **what makes data valuable**, how to account for changes in value as data changes hands and how to deal with data that can infer information on other data
3. Cloud computing obfuscates the EU data protection directive of data owner, controller and processor especially when the end users are uploading data; there are cases where a **legal limbo** (in EU law) could be created.
4. Governments are concerned about **how to manage the risk** in the cloud environment due to the lack of clarity on who is responsible as data changes hands.
5. Government feels that there is a lack **adequate consumer protection** deriving from consumer widespread law unawareness, lack of data and identity control, and the uncertainty about what might happen in the case of provider failure
6. Currently there is a lack of clarity on **requirements to notify** users and regulators **about malicious access, breaches** and procedures for incident management
7. Striking the **right balance** between protecting confidentiality and the need to access data is difficult

Data Governance

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #3: Protecting data ownership (cont'd)

Potential recommendations

i. Provide clarity around data ownership

- Policy around **specific use cases** can help industry address questions around data ownership

ii. Ensure data access controls

- Law enforcement requires computer **forensic protocols**; there needs to be a procedure for law enforcement access to digital evidence
- Limit the extent of useable data accumulation in the cloud, e.g. through encryption and purpose limitation schemes
- Providing users with a **unique digital identity** (digital ID cards) might help regulate access
- **Revisiting cyber-security laws** might help provide clarity around malicious access to data

iii. Increase user awareness

- Reach out to **consumer association** and interest groups to increase user awareness and better understand virtualization

iv. Creating a **mutual aid agreement** among cloud providers or an **oversight mechanism** similar to those designed to address bank failures

Questions and next steps

1. What could be some of the key use cases to be addressed by policy?
2. What successful example of digital identities are there in specific geographies and what lessons can we learn from them?
3. What are the existing bodies doing research around cyber-security? What are the existing regulations and where are they out-dated when it comes to cloud computing?

Security*

Issue #4: Ensuring only authorized access

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue description

Aggregated and co-located (cloud) data attracts criminals. Losses may be magnified. Breaches are visible and trust has not been yet established.

Why it's important:

- *Ensuring proper access and monitoring access (who, how, when) can be very onerous for the provider*
- *There are jurisdictional concerns around data access (depending on where the data is different security obligations will apply)*
- *There is lack of clarity around who (as wells as when and how) accesses the data*
- *Government and users may naturally demand further controls and require additional security layers than the providers*
- *There is heightened fear of cyber-attacks*

*Brookings defines **security** composed of 6 pillars: confidentiality, integrity, availability, accountability, assurance, and resilience*

Key Considerations

Industry & Customers

1. Cloud should be seen as **critical infrastructure**, with associated rights and obligations (e.g. encryption and identity)
2. Industry is concerned about ensuring proper **overall identity management** (not just user identification), which encompasses access rights, access controls, access logging, etc.
3. **Encryption** can be expensive (an added performance overhead not faced in on-premise applications) and might need to be limited to more sensitive data
4. The **overall crypto infrastructure** is relevant (not just encryption per-se) and that includes: key management, the size of the keys, the algorithms, etc.
5. Industry is **not motivated** to act because it believes that in some cases its security is superior to that of private data centers.
6. Using **hypervisors** for virtualization and isolation can leave vulnerabilities

Government

1. The cloud is **shifting responsibilities**: giving up physical control of data shifts security responsibilities. Monitoring providers is crucial, trust by itself is not sufficient.
1. Government talks about a "**unique identity** dream in the cloud" where it is possible to assign a unique identity to users
2. **Encryption** might provide a false sense of security
3. Government wants to see more **clarity about liability in contracts** as well as more clarity in **reporting incidents**

Both

1. Industry, government and users are concerned about verifying **who has rights** to enter the system and the credentials of who accesses the system on a consistent basis
2. Social engineering and **user manipulation** are harder to detect and prevent as opposed to infrastructure invasion
3. It is not realistic to base security on lock-out model; need to work on assumption of malicious **insider or compromised data** already in place

Security

Issue #4: Ensuring only authorized access (cont'd)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Potential recommendations

i. **Clarity around identity**
   - **Smart cards and digital identities** can reduce cyber attacks . It needs to be possible to identify people: currently it is difficult to identify who was involved. Ideally there would be a certificate to authenticate
   - A **global identity framework**

ii. **Policy clarification around data encryption** requirements for sensitive (versus non sensitive data) may alleviate the burden for providers

iii. **Criminalizing and prosecuting** malicious hacking of cloud services may provide deterrence to malicious attackers, increase consumer confidence in the cloud, and enable law enforcement

iv. Moving from a reactive model to a **predictive model** will further decrease unauthorized access

v. **Harmonization of**
   - The various government security **certifications** (FISMA in the US, CESG assurance model in the UK, "ISO" 27000-series, etc.)
   - The various national strategies (e.g. US White House 'National Strategy for Trusted Identities in Cyberspace' document)

vi. Identifying ways to **demonstrate** that **security measures** that were promised were actually put in place

vii. **RIM** challenged the question of jurisdiction because of very high protection - possibly a **test case**

viii. Authority to **remove infected machines**

ix. Additional **research** into end-to-end security

x. **Less reliance** on the public internet

Questions and next steps

1. What lessons can we learn from the US department of defense CAC (common access card) , from the German identity card, and from the e-government initiative in Belgium that uses identity cards for authentication?
2. What are the best practices around identity management?
3. What can we learn from the hacking of the internet?
4. What is the best research on this topic?
5. What other governments have created security certifications, beyond the US and the UK?
6. How can we leverage the work that ENISA (European Network and Information Security Agency) is doing around cloud security?
7. What regulatory references can be used when looking at criminalizing attacks in the cloud (e.g. Computer Fraud and Abuse Act ("CFAA"))?

Security

Issue #5: Ensuring integrity and availability (& addressing data loss)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue description

Continuous breaches have created an environment of distrust in the safety of cloud

Why it's important:

- *Users and businesses rely on being able to access data at any moment and they want it to be intact.*
- *Losing data creates cost and liability issues*
- *There might not be one single point of accountability in the cloud*
- *Customers are not only worried about data integrity but they are also concerned about the degradation of data quality*
- *Likely, much stronger disaster recovery procedures and certifications are needed.*

Key Considerations

Industry & customers

1. Industry is concerned about **data segregation** and logical separation of the data
2. Often cloud computing embraces **multi-tenancy**, so tenant isolation is not possible
3. Industry is seeking greater **clarity** about what they should be doing to comply with **government standards**
4. Some companies think they are being already **sufficiently transparent**

Government

1. Cloud computing **shifts responsibilities**: infrastructure in the cloud is no longer under user control.
2. In the US, government agrees that it is **not appropriate to dictate** certain security standards from governments
3. Government is concerned about **insufficient measures** to protect cloud systems from ***DDoS*** (distributed denial-of-service attack)
4. Governments would like to see stronger **collaboration and liability sharing** between cloud stakeholders
5. Government wonders if companies are willing to **guarantee resilience** (*the ability to work in a degraded mode and continue proving services even in the presence of failures)* in their contracts
6. Governments suggest that they should **collect data on incidents** since no other party is independent enough to provide an independent information (they believe companies have a disincentive to report incidents)

Both

1. More clarity is needed around **liability and accountability responsibilities**
2. For fixed line networks and mobile networks it is difficult to guarantee **full service**

Security

Issue #5: Ensuring integrity and availability (cont'd)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Potential recommendations

i. **Standards**
   - Creation of standardized comparative **availability models** for cloud
   - **Defining availability** (e.g. to be able to execute access x% of time)

ii. **Contracts** demonstrating adequate controls around data protection

iii. **Audits**
   - Compelling providers to undertake **SAS 70 style audits** of their security procedures
   - Creation of cloud based security **auditing standards**
   - Improve logging

iv. **Additional research** into security

v. Create **insurance protection** for breaches

vi. **New architectural models**, such as remote managed cloud appliances

Questions and next steps

1. What are the elements of an availability model? Are there existing examples and best practices that can be leveraged?
2. What kind of case studies are available in terms of governments subsidizing cloud systems to be more resilient (see J-SAS) and 'European Network and Information Security Agency' - ENISA - studies around it) and what can we learn from them?

Security

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #6: Ensuring data is destroyed as needed

Issue description

Data destruction relates to making sure data is un-retrievable forever once deleted

Why it's important:

- *Users want to be assured that once the data is deleted no one can ever access it again*
- There is no clarity around what constitutes data deletion
- Given that cloud providers are the only ones with access to the physical infrastructure, the only thing customers can do is trust the provider

Key Considerations

Industry & customers

1. Data deletion can be both a technical and a policy issue. Once the **policy is stated** there are many technical ways to address the policy.
2. **Persistence of digital data** or retrievability of data from 'erased' systems is difficult to avoid
3. Industry is concerned about "what is the **appropriate role for government** regarding data destruction or data deletion?" and the answer should be use-case driven
4. There is a **cost associated with data deletion** (including furthering R&D)

Government

1. Governments are concerned with **secondary use / accumulation of data** collected for specific purpose and used/accessed for another purpose (such as advertising)
2. Some believe that everything on the cloud should be **encrypted**. Customers need to also be assured that there is no more unencrypted data. This can't be done with services (only at the infrastructure level)
3. Governments believe that **encryption is only a temporary solution** (there is no way for the customers to verify deletion of data) as what can be encrypted today will be broken tomorrow
4. Government is particularly worried about **health records**, which are particularly sensitive
5. Because of **data mirroring**, data deletion could be very difficult to guarantee (SWIFT case)

Both

1. Everyone is concerned about **proper data deletion**

Security

Issue #6: Ensuring data is destroyed as needed (cont'd)

Potential recommendations

i. Having a **clear policy** on data destruction can help industry better address what technical requirements and capabilities are needed to delete data

ii. **Generally accepted data deletion practices** might be adequate if they are properly defined

iii. **Furthering R&D** around data deletion can provide reassurance to users

iv. **Different laws to require** different levels of security depending on the **sensitivity of data** (e.g. more stringent for health records)

Questions and next steps

1. What are the costs associated with furthering R&D around data deletion?
2. What are some of the strongest best practices around data deletion?

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #7: Ensuring Interoperability*

Issue description

Governments, customers and business are concerned about insufficient interoperability between public clouds

Why it's important:

- *Interoperability can be critical to ensure the availability of certain data and services*
- *There are many cost and competition considerations around interoperability*
- *Interoperability can be especially valuable within PaaS and SaaS*
- *There is tension around interoperability: cloud vendors aim for independence while governments and users want more interoperability for the sake of innovation, competition, resiliency*

Key Considerations

Industry & customers

1. There is lack of agreement on **what interoperability means** and it conflicts with company's desire to **differentiate themselves**
2. Industry fears that **excessive standardization** might be **restrictive** to the growth of cloud and stifle innovation
3. Industry is supportive of the work around **standardization** of identity management systems (technical & policy driven), e.g. Distributed Management Task Force's (DMTF: Distributed Management Task Force) work.

Government

1. Government points out that there is a **lack of common development environments**
2. Governments see a role to **provide guidance** around interoperability as the industry may not move fast enough
3. Government believes that interoperability reduces lock-in

Both

1. Stakeholders need to look **beyond just technical** interoperability: systems interoperability, accountability, and liability structure, application interoperability, etc.
2. Stakeholders feel very strongly about the need to **differentiate** how interoperability is addressed with **each cloud model**: Infrastructure is very different than application as a service.
3. There is a lack of clarity around **accountability** while transacting data in an interoperable scenario
4. Many believe that we are years away from application portability

Interoperability is the ability of systems (data, software, services, applications, policies, etc.) to seamlessly **communicate with each other (e.g. a common development language) even if in different cloud providers or platforms*

Business Environment

Issue #7: Ensuring Interoperability (cont'd)

Potential recommendations

i. Creating **clearer understanding** around the meaning of interoperability and the key priorities around interoperability, from a business stand-point, should be done before getting into technical solutions

ii. **Harmonizing different standards** of the organizations that are discussing interoperability

iii. Create widely and globally accepted **interoperability standards**

iv. Creating a voluntary **cloud bill of rights**

Questions and next steps

1. What does interoperability mean? If interoperability is about building distributed applications across different clouds, is there anything more that the implementation of standard web protocols required? Or should their be vertical specific application data interoperability standards?
2. In terms of the various academic grids out there (open science grid, NSF: National Science Foundation, open cloud manifesto) what does everyone subscribe to?

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #8: Ensuring Portability*

Issue description

Governments and customers are concerned about their ability to move data and applications across clouds and back behind the firewall

Why it's important:

- *Moving from on-premise to cloud and vice-versa, and between cloud environments can be inefficient, time-consuming and expensive*
- *Customers and governments are more inclined to "open portability"*
- *However, open portability might undermine vendor differentiation and the incentive to innovate (cloud as a commodity)*
- *Portability and data ownership are intrinsically tied*

Key Considerations

Industry & customers

1. Industry fears that open portability might **limit the free competition** and growth of proprietary innovation.
2. There are concerns around what the **switch over costs** would be with open portability
3. Industry is also concerned about the **impact of portability regulation** (e.g. anti-trust) on the business

Government

1. Government is concerned about **customers becoming dependent** (locked-in, unable to switch over) on certain vendors
2. Governments sees a role to **provide guidance** around portability as currently there is lack of self-regulation schemes to avoid vendor lock-in
3. **Portability of informed consent** is a concern for governments and relates to ownership of the data (once you upload data, who owns it?)
4. Governments suspect that industry is reluctant to move to open portability because that might affect a **change in the cloud business model** and the associated revenue stream.

Both

1. Data portability is tied to **data ownership** (who owns the data), **data protection**, law **enforcement access**, and **liability**
2. **Differentiating between models** that intentionally constrain users and models that simply want to differentiate offerings is relevant to the discussion

Portability is the ability for customers to **move data and applications across public clouds and from public to private and vice-versa.*

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #8: Ensuring Portability (cont'd)

Potential recommendations

i. Establishing portability standards . Industry would like some **harmonization** around the various **standards bodies** that are doing work around portability (e.g. DMTF: Distributed Management Task Force)

ii. Revisiting existing **anti-trust regulations** and configuring them to apply in the cloud environment

iii. **Explore other models** (e.g. telecom industry) to regulate portability that may be applicable to the cloud

iv. Addressing **liability** in portability scenarios

v. Invest in **additional research** around the needs, desires and technical options of portability

Questions and next steps

1. Is it too early in the cloud maturity model to discuss portability?
2. Should the standards be at the level of defining the types of data that can be exported, the basic mechanisms that should be supported, and the effort/responsibilities associated with exporting data from the cloud? Or should the standards go to the level of defining specific data formats as well as the mechanisms?
3. What would be the key elements of a portability standards document ?
4. What lessons around portability can be learned from other industries *(e.g. vertical separation has been one of the ways to address cartels in telecom*)?
5. What role do new virtualization approaches play?

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #9: Insufficient reliability* of cloud

Issue description

Customers perceive that reliability today is not sufficient for mission critical needs, and there is no clear path to improvement.

Why it's important:

- *There have been several recent examples in which cloud services have been compromised because of technology failures.*
- *Customers perceive cloud differently depending on how vendors address planned and unplanned downtime, what kind of backup strategies they have in place, and how they react during a crisis.*
- *Understanding how providers are ready to address extraordinary circumstances (failure of the service, bankruptcy , etc.) is a pain point for customers*

Key Considerations

Industry & customers

1. Industry believes that the increased use of cloud will generate **new models** for assessing reliability and reputation
2. Users are concerned about what might happen when a provider goes **out of business**
3. Users are concerned about **resource exhaustion** when one or few tenants are using up all the providers resources

Government

1. Governments have showed concerns around reliability and continuity particularly for **smaller cloud providers** who do not have large data center capacity and back-up capabilities

Both

1. Users associate cloud reliability with the providers' reliability. However sub-contractors and **other layers of service** might present varying levels of reliability.

**Reliability is the ability of cloud and cloud providers to consistently perform their intended or required functions, on demand and without delay, degradation or failure.*

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #9: Insufficient reliability of cloud (cont'd)

Potential recommendations

i. Encouraging **crowd capabilities** to monitor and evaluate reliability can increase user access to information (hence increase transparency)

ii. Harmonizing the different standards (e.g. OASIS open reputation management systems technical committee, etc.)

iii. Compelling providers to undertake a **SAS 70** (Statement on Auditing Standards) **style audit** of their reliability may increase customer confidence

iv. A possible solution to accountability is clarifying the roles of the **data controller's responsibility and liability** around what happens in the cloud (this may or may not coincide with service provider)

v. Creating **Metrics and Monitoring tools**

- Compelling and encouraging cloud providers to offer **standardized reliability metrics** (backups, remote processing, etc.)
- Provide **alarm systems** to alert when the system goes down or is compromised; need to treat the public cloud system as a complex interconnected system (analogy to the financial system)
- Creating **rating agencies** to evaluate the comparative quality or scope of a Cloud Provider

vi. Funding **more research** into root causes of failures, new fault-tolerant architectures, fault-tolerant systems

vii. Creating **mutual agreements** among providers

Questions and next steps

1. What key elements would reliability standards metrics have to include? What steps are needed to create a harmonized body of standards?
2. What are the most accepted reliability standards? What key elements would an acceptable reliability standards document have to include (downtime, uptime, back-up strategies, data center capacity, etc.)

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #10: Insufficient commitments to service levels

Issue description

Industry has not provided clear or sufficient service levels around availability, reliability, response time, etc.

Why it's important:

- *Clear service level commitments from providers to customers are key to ensuring high quality and comparability of cloud services*
- *Availability of the service (uptime), performance of the service (response times, bandwidth) , service suspension and other considerations are critical challenges between provider and customer if not clearly addressed*

Key Considerations

Industry & customers

1. Service commitment **can't be very standardized** since they depend on different circumstances: the model, the platform, the customer needs
2. Industry is interested in **policy service level agreements,** including how to manage a particular policy against particular personally identifiable information.
3. Industry is interested in further understanding the **different aspects of SLAs** (uptime, security, etc.) that are relevant to their customers (governments, businesses, users) because that impacts the quality of the service
4. Some industry players believe they are **transparent** enough, and that it is too early for strong SLAs

Government

1. Governments want to see vendors provide **clearer service level agreement** with **standardized metrics** to evaluate their services
2. The discrepancy and lack of standards in **contractual setting** between different parties makes the comparison of service capabilities difficult

Both

1. Providers, users and governments are all interested in understanding how SLAs can me measured . Users especially are interested in understanding how service commitments will be **met, monitored, measured and penalized** if not met
2. There is **not enough competition** yet to ensure SLAs evolve
3. While SLAs could help address many of the data issues, currently there s not enough **consistency**.

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #10: Insufficient commitments to service levels (cont'd)

Potential recommendations

i. Proposing a **scale or a gradient** (compliance at "X" level) might allow to map SLAs across different cloud providers

ii. Further reinforcing **transparency** will increase visibility into the actual quality of the service

iii. Making sure that **policy controls** are in place in the cloud around the data (as opposed to policy around things like uptime or infrastructure service level) will further help with transparency

iv. Establishing **audit certificates** and a validation process will allow for a more consistent measurement and comparison of cloud services

v. Making **escrow terms** available may ensure business continuity in case of a Cloud Provider going bankrupt or defunct

vi. Harmonizing the different standards being created by various bodies (DMTF, OASIS, etc.)

Questions and next steps

1. Do we need a new certification body or how do we leverage existing bodies?
2. How do we exhaustively list and revisit all the existing service level standards (DMTF*, OASIS*, FedRAMP*, etc.)? What are some of the criteria for creation and acceptable and comprehensive standard document?

** DMTF: Distributed Management Task Force*

OASIS: Organization for the Advancement of Structured Information Standards

FedRAMP: Federal Risk and Authorization Management Pilot program

Business Environment

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Issue #11: Relative maturity of the cloud ecosystem

Issue description

Symptoms of immaturity of the cloud ecosystem (business models, enabling technologies such as access, architecture, market concentration, competition, training capabilities, regulatory, and taxation issues) slow down adoption and create concerns among users and gov'ts, though many agree we are making rapid progress

Why it's important:

- *Cloud is dependent on the availability, access & maturity of enabling technologies*
- *Because of the high barriers to entry there are concerns around the high level of cloud market concentration*
- *Cloud may be "disrupting the value chain" and changing the way traditional solutions are being built*
- *Uploading large data over network is an infrastructure challenge*

Key Considerations

Industry & customers

1. Industry believes that we will experience a **natural evolution** of the key issues as cloud evolves, including the evolution of enabling technologies, the emergence of new business models, and new uses of business data
2. As the use of cloud increases, so will the **dependence on the network** . Network centricity will require addressing broadband issues and cyber-security issues.
3. Industry is concerned about whether current **IP systems** will evolve and be able to address cloud needs. Similar concerns are around patent, license models and copyright infringement.

Government

1. Governments are asking themselves if the **cloud system is imbalanced**, if the dominance of large (U.S.) players (especially infrastructure) will hinder the growth of smaller players (especially application and service)
2. Government is concerned that potential surge in **small cloud start-ups** might repeat issues from the web-hosting crash (e.g. domino effect bankruptcy, lack of escrow protection, etc.).

Both

1. There still isn't enough understanding around cloud and an **education process**
2. There is a need for new type of **technical skills**. It's a new opportunity but there aren't enough people who know how to architect cloud solutions (NSF –National Science Foundation- is helping raise the number of students studying cloud)
3. The marketplace does **not yet have sufficient competition** due to the high cost of entry and is primarily dominated by American companies
4. There is insufficient access in **emerging markets**
5. There is **insufficient Venture Capital** activity
6. The Enterprise IT industry is **consolidating**, reducing focus on innovation and slowing disruption by cloud technologies

Business Environment

Issue #11: Relative maturity of the cloud ecosystem (cont'd)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Potential recommendations

i. **Reviewing existing IP laws** and adapting them to cloud environments
ii. Stimulating **further investment** in cloud services and broadband
iii. Provide greater access to the internet and subsequently cloud computing for developing nations
iv. **Furthering research** around the **economic impact** of cloud
v. Cloud service providers making **it easier to build applications** on top of their environments
vi. **More research** on the barriers; into TCO (is cloud really cheaper?); into the need for access bandwidth
vii. More specific **focus on critical clouds** (e.g. healthcare, collaborative healthcare)
viii. **More competition** by forcing openness and interoperability
ix. Adoption of **open source models**, other open models
x. **More collaboration** with carriers
xi. More engagement by **universities**
xii. **New architectural models**, such as remote managed cloud appliances
xiii. More focus on **government cloud use** to provide role model
xiv. More encouragement of **small business**
xv. More **Venture Capital** investment
xvi. Some countries taking the lead to create a **GNP-boosting cloud**
xvii. **Leverage approaches** used for broadband to encourage the building of cloud infrastructure (e.g. Japan)
xviii. Governments to provide **subsidy to public cloud** to accelerate the growth of the economy (*e.g. Japan's Ministry of Economy, Trade and Industry invests in J-SAS, a cloud platform that aggregates different business applications for SMEs*)

Questions and next steps

1. Are existing IP laws outdated? How can they be updated or modified to apply to cloud?
2. Should governments update copyright and other IP laws (to encourage the online dissemination of cloud services and content) to appropriately limit the liability of cloud providers in situations where hosted content or software infringes third party intellectual property rights?
3. Should governments promote improved broadband access by creating a framework and incentives to encourage private-sector investments in next-generation broadband networks (fiber and wireless)?
4. Is there enough R&D being done to assess the long term evolution and growth of the cloud market?
5. What lessons can we learn from other technologies that needed to mature?

APPENDIX

Cloud computing > context/scope

Base Definition

"Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services." *[source: the University of California at Berkeley]*

Footnotes: a) Access to the cloud can be provided via multiple technologies (Internet or other b) "services" can be multiple (data, etc.)

Potential Attributes

- ❑ On-demand self-service
- ❑ Broad network access
- ❑ Resource pooling
- ❑ Rapid elasticity
- ❑ Measured Service
- ❑ Massive scale
- ❑ Virtualization
- ❑ Resilient computing
- ❑ Low cost software
- ❑ Geographic distribution (multiple jurisdictions)
- ❑Multiple accountability
- ❑Service orientation
- ❑ Advanced security technologies
- ❑ Multi-tenancy

Relevant Deployment Models

Public cloud – sold to the public, mega-scale infrastructure (e.g. Amazon, Google, Salesforce, Azure, etc.)

Hybrid cloud – composition of two or more clouds where you might where you can abstract applications or services through a combination of in house infrastructure or reach out to multiple Clouds.

Community cloud – a shared infrastructure for specific community (e.g. health care)

Note: Private clouds (ones that an enterprise owns , does not share and are typically behind a firewall) are NOT included in phase II scope

Sources: University of California at Berkley, NIST, EU Information Society and Media, IDC, Harvard

A possible hierarchy of cloud-based offerings

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD