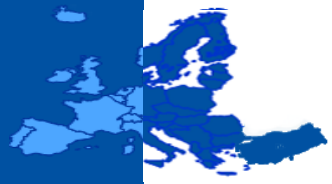


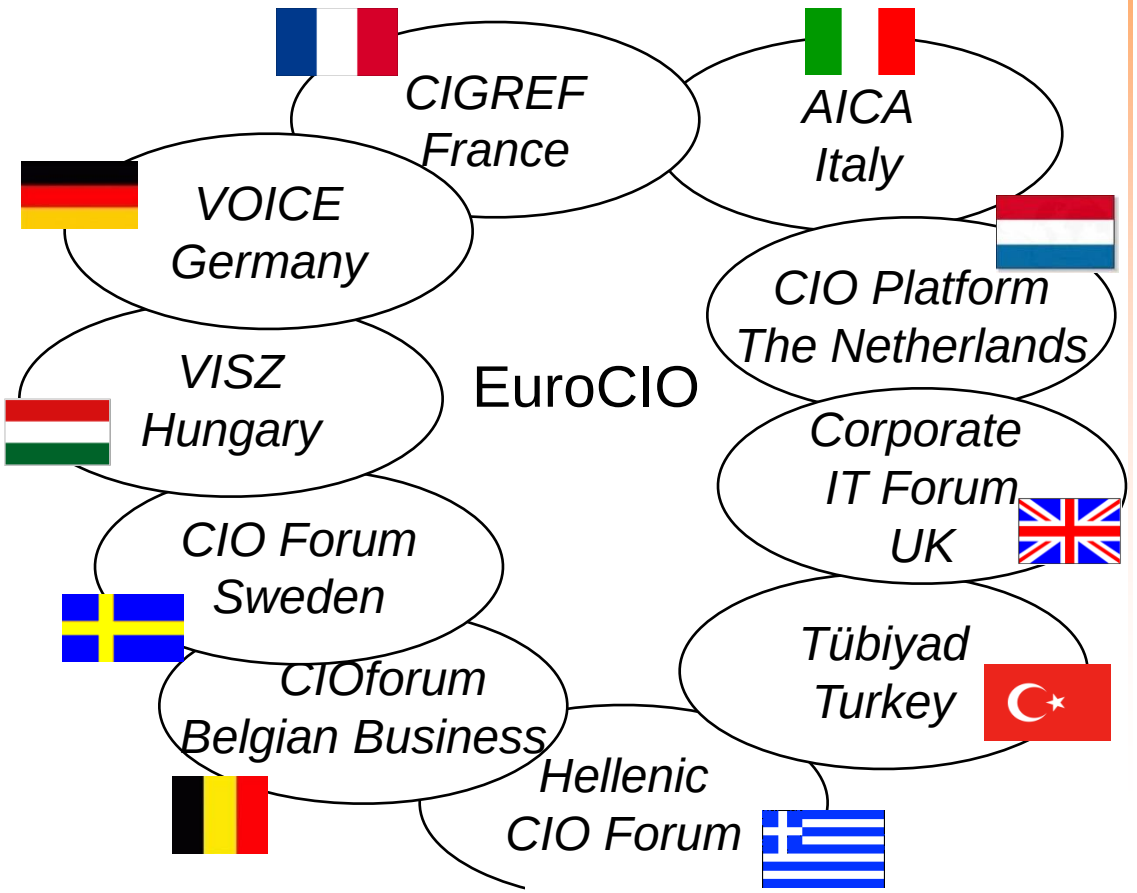
European Users' recommendations for the success of Public Cloud Computing in Europe

Cyril Bartolo
Cloud Computing Council chairman
25-Nov-2014
v1b

The European CIO Association

European CIO Association

- EuroCIO is created ***by CIOs for CIOs*** in 2004
- Since 2011 an international not-for-profit association, registered in Brussels
- 10 National Associations =>
- ca. 700+ consolidated members (private & public)
- in 12 European countries
- Consolidated IT budgets > €150 billion
- Consolidated > 600.000 IT-employees
- Board: Agfa, Eni, Daimler, Shell, Generali, Thyssen-Krupp, OTP Bank, National CIO Bodies
- We represent **the IT-demand side**



Key participations of EuroCIO

- (2010-11) Definition of the European Cloud Strategy
  - (2014) Corresponding Consultation
- (2013-14) European Cloud Partnership (board member)
- Cloud Standards Coordination (DG CONNECT & ETSI)
- SIG Certifications (DG CONNECT)
- SIG SLA (DG CONNECT)
- SIG Data Protection code of conduct (DG CONNECT)
- Safe and Fair Contracts (DG JUST)
- WP214 Consultation (WP29)
- Many other European events (EC or non EC)

- An attention for a governance where Users have equal voice with Providers

Attraction for Cloud

- Cloud is a real new trend of IT (see Adobe), offering elasticity, fast deployment, sometimes good ROI
…but often still not mature enough

Private versus Public Cloud

- Private Cloud is a far more interesting option than Public cloud
  - More control:
    - …on security, data localization, data protection, etc
- This presentation is about Public Cloud

Decision factors

Advantages

- Mobility
- Collaborative
- Less infrastructure
- Less dedicated resources
- Automatic upgrades
- Elasticity/provisioning
- OPEX vs CAPEX
- Etc…

Risks

- Security & DataProtection & Localization
- Liabilities upon User (not Provider)
- Unpredictable public internet SLA
- Reversibility and bandwidth
- Migration cost
- Lock-in and future price increase
- Contract unbalanced in favor of Provider
- Etc…

context of the company, **infra maturity**, users profile, and their use of software, software assets and obsolescence

⇦ ? TCO & ROI ? ⇨

At stake: the failure or success of Cloud Computing in Europe

- A very low adoption rate of public Cloud
  - Gartner anticipated 25% software in SaaS in 2011 but now foreseen to be only 10% in…2018: -60% despite 7 years postponement
- Too many obstacles to uptake Cloud
- Too many risks for the Users
  - More and more understood by Users (awareness increase)

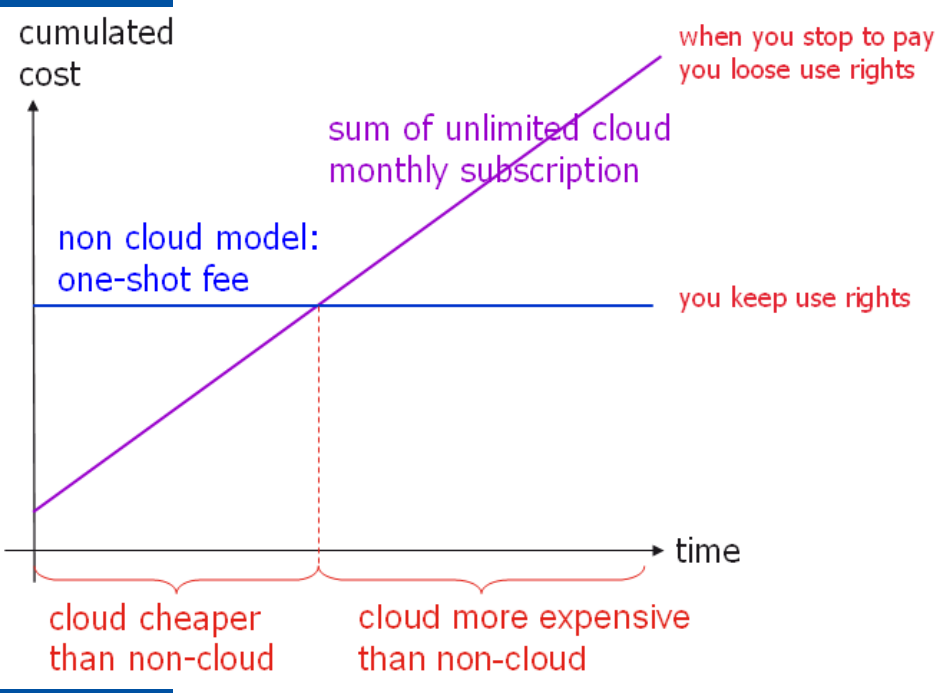
…a path still for failure

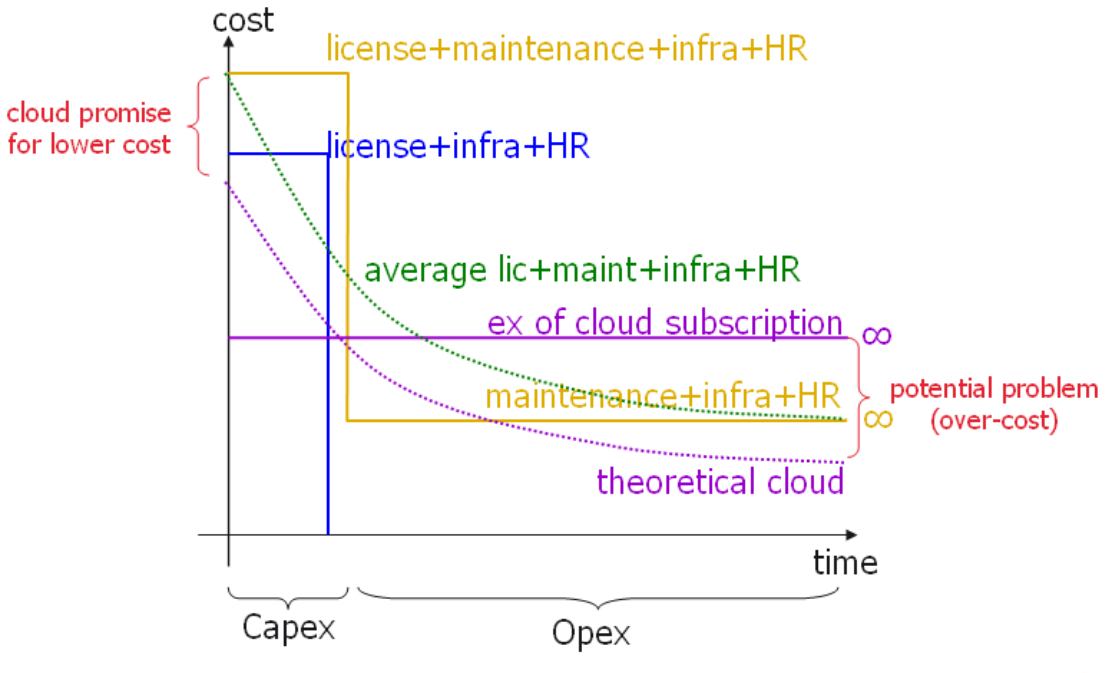
…to be transformed into success by:

- a strong attention and adaptation to Users expectations: the Users decide to adopt Cloud…or not

The European CIO Association

Pricing considerations





The European CIO Association

Cloud contracts

- …are generally unbalanced, not fair, not negotiable. Often their annexes (e.g. security) can be modified unilaterally by the Provider

- Solution:
  - The DG JUST Safe and Fair Contract Terms (SFCT) activity…
  - …to be the minimum basis of future contract negotiation for the Users

Security

- Users are deemed to ensure enough security, but it is often beyond their expertise, and Users have in fact no control on it
  - Users are required by the European legislation to ensure that the security of their Cloud Provider is enough: what does mean 'enough' ? Which definition ?
  - Description of Providers' means for security is sometimes difficult to get and complex
  - Users (especially SMEs) go Cloud because they don't have expertise in security
  - Users are said to define the means of security but in fact Cloud infra is defined by Providers
  - Cloud Providers are the experts in security, they define it, modify it, without Users
  - There is no Standard nor Certification specific to Cloud
- Solution:
  - An European Cloud security certification validated by the WP29, matching the common & minimum* requirements required by the European legislation => simple for Users

this would improve the overall security of European data put into cloud

(*) ex: password should never be stored unencrypted

Liability (the main obstacle?)

- Cloud providers are generally not liable* for service interruption, data loss, data breach of confidentiality
  - But hundreds of millions of user accounts hacked in 2013-14 (lack of incentive?)

- Reversely the Users are civilly and penally liable in case of Provider's security breach on User's data
  - Too risky for many Users

- Solution:
  - The ones making eventual mistakes should be the ones suffering the consequences => joint data controllers

    => (*) no exclusion of liabilities

    => decrease User's liabilities (where User is not the cause)

Future Data Protection regulation

- The basis for the European Users future
- Will determine the success or failure of Cloud
- But particularly difficult for Users to influence it to make Cloud adoptable

- Solution:
  - To involve the Users in the elaboration of the future DP regulation because they are its first stakeholder
  - To adapt the DPreg with the recommendations of this presentation, for e.g.:
    - …fair sharing of Users and Providers liabilities
    - …Cloud specificities,
    - …to include confidential data of enterprises in addition to privacy data,
    - …to avoid to continue surfing on old 1990's principles indirectly but mechanically in disfavor of Cloud Users

  => to reverse things for more balance for the European Users

International transfer of data

- Complex to understand what to do when going Cloud with a Provider transferring data outside the EU
  - About countries, subcontractors, subsequent transfer, etc
  - Is Safe Harbor compliant with EU laws ?
  - Will Safe Harbor be suspended ?
  - What to negotiate in addition to SCC ?

- Solution:
  - Clear information defining which declaration and negotiation is needed for European SCC, and Safe Harbor
  - Providers to be compliant with WP29 (inform about countries and subcontractors, notify any new and wait for approval, subsequent transfers,...)
  - Providers could propose an option to have data stay in Europe
  - Alternative solution to international transfers, government curiosity, Europe GDP, European laws compliancy, etc
    - ⇒ encourage European wide Clouds (where data stay in Europe)
  - Where possible do harmonize European laws

European SCC (model clauses)

- European laws put the Cloud responsibility on Users as data controller, despite Users have no control on the definition and operations of Cloud infrastructure and security
  - Coming from the old outsourcing data controller model (and the 1995 Directive)
  - SCC includes positive and negative things for Users but Providers don't negotiate SCC further (a full negotiation from scratch could have been better)

- Solution (?) (before a final solution in the future DP regulation?):
  - SCC v2004 (joint controllers) for Public Cloud ? (user does not control anything)
  - SCC v2010 (User is data controller) for Private Cloud ? (user control some things)

Requests from supervisory authorities

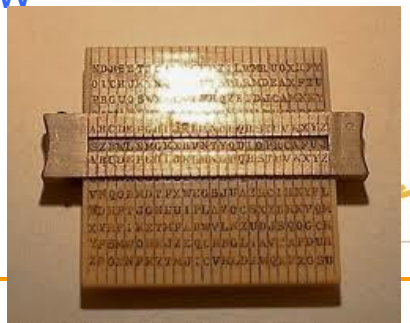
- Users are required things which are in practice often beyond their capacity
  1. Users are required to negotiate the security means, in practice they are not negotiable (and sometimes even difficult to get)
  2. Users are required to get the list of countries/subcontractors where data go (and the subcontractors list) but often Providers say "the list is not available"
  3. Users should have the right to refuse a new subcontractor and/or new country but often Users don't even get informed, or can not refuse (but terminate)

- Solution:
  - European requirements toward the European Users should be adapted to the reality of the practices experienced (1),
  - And adapted to the specificities of the Cloud (3)
  - Providers should follow the WP29 (2,3); or for (3) to adapt obligations

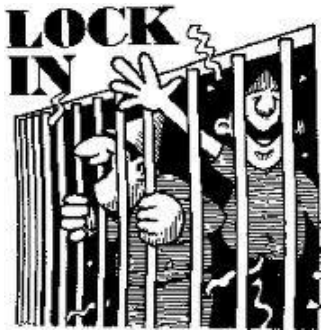
Data ownership and IP rights

- Often it is OK but sometimes the data is utilized by the Provider for other purposes. And who is the owner of the developments made by the User in the Cloud (?)
  - For e.g. advertisement, statistics, etc
  - Including some governments curiosity

- Solution:
  - DP regulation should state that User always keeps ownership
  - Including destruction of data when leaving ('right to be forgotten')
    - Only upon registered letter to avoid misunderstanding (loss of company data!)
  - Laws like PatriotAct/FISAA to be clear and limited to legitimate access only
  - Notify immediately customer in case of confidentiality breach (or suspicious)
  - Data to be encrypted at rest and at flow
  - User should be able to encrypt its data with own private certificates (strong)



Lock-in and reversibility



- Cloud often brings lock-in, which is the worst for Users being forced to accept almost anything
  - User is locked: too difficult to get out of the Cloud for another infrastructure
  - So he is forced to accept for e.g. any new subcontractor/country, or any price increase => danger

- Solution:
  - To cap prices at contract renewal
  - Enough time and means (bandwidth) for reversibility at contract end
  - Reversibility should be available at anytime for the User autonomously
  - Portability and interoperability (open) standards

SLA (performance & continuity of service)

- Sometimes looking like 99,9% guaranteed when in fact there is no SLA after the legal exclusions, or just a few hundred euros compensation

- Solution:
  - SLA should be really guaranteed (with notification, delays, penalties,…)
  - SLA should be controllable and provable by User through supervision console
  - No legal exclusion
  - The Telco possibility to not be dependent on internet (having no SLA)

A User certification or label

- Users (in particular SMEs) are not protected because they can not evaluate a Cloud offer in front of User's interests

- Solution:
  - To factor Users expectations in such User Certification or Label (pass/fail + a total of points)
  - So Cloud will become 'readable' => increasing trust and uptake

Other points

- Providers should contact authorities to ensure their services are compliant with European or national regulations, and such authority should certify such service as compliant (or not),
  - Legal hold and traceability (for e.g. to keep traces of connections or mails headers), encryption of communications
- Providers to bill SaaS not on user but on usage, as it is a Cloud promise
- To ease the difficult integration of Cloud with the enterprise infrastructure
  - for e.g. interfaces, or guaranteeing waterproofness with users directory, private SMTP routing,…

Data in cloud is like money in bank

- Equal mechanisms developed in the financial world to protect customers money are needed for cloud computing:
  - including certification of cloud providers,
  - codes of conducts agreed by demand and supply side,
  - auditing authorities.

- The sooner these mechanisms are in place, the sooner end-users will be willing to use public cloud

Conclusion

- Many European Users believe they are protected when going Public Cloud, when in fact the User is the one who is generally at risk

- For safety of the European Cloud Users and their data, the Users requirements and the Cloud specificities must be included into the future Data Protection regulation, the SCC, the Standard&Certifications, the Contracts, etc

- The European Commission to play a key role: no Cloud success without an European legal framework adapted to Cloud and fair to the Users

- Meanwhile the increasing awareness of the Users must continue

- Easy to go Private Cloud, and possible for Public Cloud but very complex to understand and to adapt in order to limit the risks

euroCIO
The European CIO Association

The European CIO Association

CLOUD POINTS OF ATTENTION for Users

(for a Trusted Cloud Europe) (to allow Cloud adoption)

C.Bartolo
Apr 2014, v1

New Data Protect° regulation + CoC

ensure with Users that below points are included, vote 2014, apply 2015

1. Decrease Users liability (more fair)
2. Harmonize European laws
3. Avoid 'specific limitations' laws
4. Free flow of data within Europe
5. Keep full ownership of data
6. Provider lists countries where data 'is'
7. Option to have data stay in Europe
8. If data outside UE, clarify what to do (SCC?)
9. Protect data against 3rd party curiosity (incl. govs) & inform about requests
10. Cover privacy & business data & cloud
11. Right to be forgotten & destruction policy
12. User informed immediately on breach
13. No liability exclusion if data loss or breach
14. Quick data access if Provider bankrupts
15. Simplify declarations to supervisory authority

SLA & Licensing & Pricing (CoConduct)

30. Telco focus on lower SLA on internet lines
31. No liability exclusion on SLA
32. Supervision console shows real-time SLA
33. Allows read-only after end of subscription
34. Price increase capped (Eur inflation index)
35. Demonstrate ROI; bill on Usage not User
36. Non-Cloud equival. offers don't disappear

Safe and Fair Contracts

for all Users, a minimal balanced contract as a basis for negotiation

37. Any clause applies to sub-contractor
38. Sub-contractors known and accepted
39. Jurisdiction & court at User's country

Security standards & certifications

specific to Cloud are missing & needed (would shield the User from liability)

16. Encryption at rest and at flow
17. Allow encryption with private certificates
18. Provider describes the means for security
19. Risk assessment & Recovery plan
20. Strong authentication
21. Legal hold and traceability required
22. Right to audit

Interoperability & Reversibility (CoC)

decrease lock-in

23. Autonomous reversibility right at ay time to extract data
24. Simple and complex data
25. In a rich & reusable (std) format
26. Contract should give enough time
27. Providers use (e.g. open) standards
28. Ensure interop&portability (incl. 3rd party)
29. Ease business interfaces with User infra

European Trusted Cloud Space bricks and corresponding Codes of Conduct (CoC) or Certifications

Including Sectors oriented developments

40. Designed by USERS

Cloud Users Label

- Providers evaluated in front of the ~40 points
- Accessible to Cloud SME Providers (not a question of money)

=> Cloud becomes readable for all users