White paper

enabling trusted European Cloud

Your business technologists. Powering progress

Contents

Introduction

Cloud has been the flavour of IT for a good while now.

As the world moves on to new fashions in technology – Big Data and the Internet of Everything, for example – should we assume that all the important decisions around cloud are settled? The answer is no.

Atos has been involved in many of the initiatives aimed at designing the cloud landscape, and we believe we can offer a useful analysis of the issues we must address for today and tomorrow.

Atos is a leader in cloud solutions and services, and because of that we have been invited to work closely with legislators and other companies in developing strategic cloud strategies for Europe. Our CEO, Thierry Breton, was a member of the Steering Board of the European Cloud Partnership (ECP), for example. It was the ECP that in 2014 produced a document entitled "Establishing a Trusted Cloud Europe" , establishing the rationale for cloud adoption in Europe.

Atos Research and Innovation (ARI) – the group which supports Atos clients needing solutions that go beyond what current products provide – has strongly supported that EU initiative, running a number of projects that contribute to the concept of Trusted European Cloud.

Our leadership has been enhanced by creating our own cloud solution company, Canopy , the end-to-end cloud services provider that acts as a change agent in delivering on a global scale. Canopy is more than just a cloud solution provider: it enables customers to drive truly transformational IT via the cloud, by leveraging Atos' world-class datacenter and consulting services.

Atos' experience as an EU partner, and as a leader in digital services, teaches us that new trends in IT such as cloud are not always as readily adopted in Europe as they are in the US. New trends need balancing against other European beliefs in fundamental rights and values: deep concerns about security and the right to privacy, for example. There are of course business and employment consequences as a result.

Does this position represent innate conservatism in Europe, or a greater sense of ethical responsibility? Either way, our cautious European attitude to adopting new delivery models needs to be properly understood in order to address those concerns.

One of the major issues for cloud adoption is trust. Like 'peace', you only really know what trust is when you have got it. It is also a fragile concept: slow to gain, and much easier and faster to lose. From Atos' experience with our customers, potential cloud users are looking for a number of factors above and beyond their technical needs when seeking services they can trust, including:

- Compliance: adherence to laws, regulations and standards
- Security: of data confidentiality, integrity and availability
- Transparency or visibility: of where things are and what is going on
- Privacy: to ensure that personal data is safe and not misused (a particular concern in Europe)
- Auditability: assurance that checks and balances are applied by independent trusted parties
- Portability: avoiding vendor lock-in, by ensuring easy movement between providers.

Atos is rigorous in ensuring that our cloud service services are trustworthy. We believe that a trusted delivery environment can be established, verified, and deployed by users, at a real, practical and operational level.

On the supply side, this could result in cloud services which, although assembled from components from all over the world, are supplied by European organisations and are branded "Made in Europe", with some sort of quality and compliance assurance associated with that brand.

Our Steering Board membership of the European Cloud Partnership makes us confident that a "Trusted European Cloud" brand is possible. Such a brand should convey confidence that our fundamental rights are not betrayed for commercial purposes.

We also strongly believe that we need one clear European Cloud Standard to which the industry should adhere. Atos and its partners are working closely with the European Commission (EC) to clarify what the relevant components are for that Standard, and it is becoming clear what is likely to be included.

In parallel, an EU-wide General Data Protection Regulation (GDPR) is about to emerge, which will have significant effects on data privacy.

In this document, Atos aims to clarify these fundamental issues affecting cloud developments in Europe, and reassure potential cloud customers that there are ways of steering through them. We propose a roadmap in which all parties, including customers, need to be involved to achieve a vibrant and successful cloud environment that is fit for our European purpose.

Neelie Kroes, then Vice President of the European Commission.

"Europe should aim to be the world's leading 'trusted cloud region'."

Memo, 15 October 2013

1 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935

2 See: http://canopy-cloud.com/

Cloud

This document is not a full introduction to cloud services. A separate companion document by the same author aims to provide that[3], based on recognised NIST[4] standard definitions. This document instead concentrates on the key aspects relevant to the development of the cloud services landscape today and tomorrow. However, it is important to establish some basic reasons why cloud is gaining such importance.

Many potential cloud customers are drawn by: potential cost reductions; the attractive move from fixed capital investments (capex) to variable operating expenses (opex); and the appeal of services that are highly flexible and adaptable.

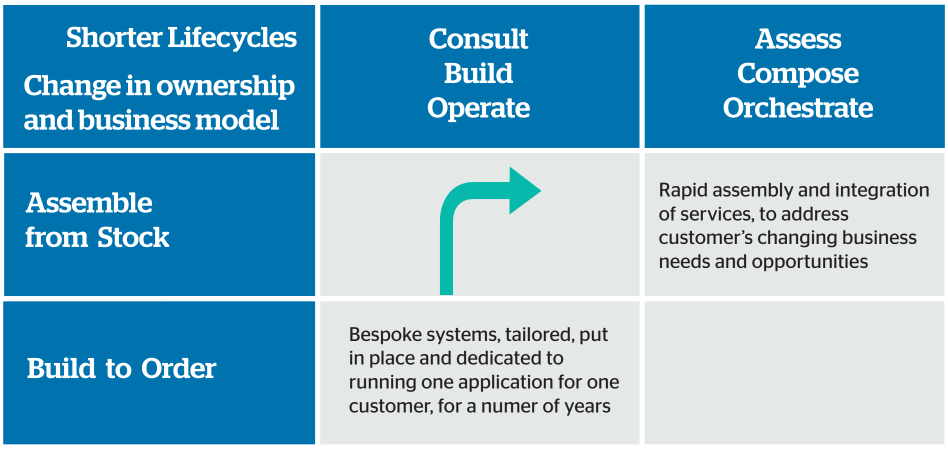
Cloud is also attractive as a comprehensive set of services – epitomised by *"anything as a cloud service"*. This can include infrastructure, software, or an ever-increasing range of business tools. *"As a service"* is important: with cloud, customers no longer need to own or even manage resources to make use of them.

The concept is familiar. In recent years, most large enterprises have introduced some form of outsourcing, so a move to cloud support is incremental[5]. Many organisations now understand committed service levels and quality standards from their outsourced arrangements, and expect similar standards with cloud services. For some organisations, though, the move to cloud is more of a leap, and absorbing the lessons from others is important.

The move towards cloud is in fact closely entwined with two major, simultaneous movements within IT services:

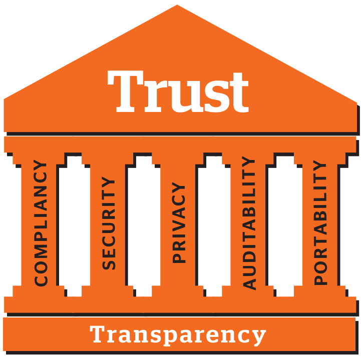
From Build to Order (BTO) to Assemble from Stock (AFS)
This is the change from using infrastructure and systems that are commissioned and deployed specifically to run one application for one customer, to a situation where standard infrastructure pre-exists and is selectively assembled for a particular purpose. It implies both a large degree of standardisation and a change in the ownership model.

From Consult, Build, Operate (CBO) to Assess, Compose, Orchestrate (ACO)
In the past, most systems would be built in a lifecycle of months or even years. They would be characterised by a "waterfall" process, where lengthy sequential processes would be used to analyse requirements, develop a solution, and then operate it (largely unchanged) for many years. Now we see an almost continuous build process, using rapid development and "devops"[6] where new software changes can be deployed even on a daily basis.



Shorter Lifecycles Change in ownership and business model	Consult Build Operate	Assess Compose Orchestrate
Assemble from Stock		Rapid assembly and integration of services, to address customer's changing business needs and opportunities
Build to Order	Bespoke systems, tailored, put in place and dedicated to running one application for one customer, for a numer of years	

The House of Trust in Cloud
- anchored in the EU



Trusted European Cloud

Atos, creating a quality secure cloud environment in Europe with clear and open compliance standards.

[3] Shaping the cloud: why and how you should develop a cloud strategy now, Atos, November 2011, https://atos.net/content/dam/global/we-do/atos-shaping-the-cloud-white-paper.pdf

[4] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[5] Indeed, many, including Gartner and De Nederlandsche Bank define and treat cloud as a form of outsourcing.

[6] See https://en.wikipedia.org/wiki/DevOps

When combined, these changes can have a profound effect on how systems are deployed and used. This is when cloud services become particularly attractive, provided there are well-defined processes with built-in checks and assurances to ensure an acceptable quality of service, especially for business-critical services.

One point that sometimes causes contention is the idea that services only need to be "good enough". For many customers, "good enough is not good enough for our business". Organisations may be used to BTO services designed specifically to fulfil their stated needs, but in an AFS model, components are selected from the range available, which need to be combined to meet requirements. The criterion for that selection is that the component or level chosen is indeed good enough, but many people react irrationally to that suggestion. Whilst the emotion can be understood, it needs to be held to the light and examined to avoid unnecessary complexity and expenditure.

We see customers deploying cloud services typically in a number of ways. At the ends of the cloud deployment spectrum are:

Private
Cloud infrastructure is deployed, whether in-house or hosted by a supplier, for the use of only one organisation, yielding few of the real benefits of flexibility or scale, but ensuring maximum visible security.

Public
Services are available to be used by anyone, either "free" or with the means to pay, such as a credit card. This provides maximum flexibility but can raise questions of security, certification, etc.

There are other options in the spectrum:

Community
An environment is established for a group of customers who have similar needs in terms of services and certifications, and access is only given to those known users. This tends to be "the best of both worlds" in terms of combining both economies of scale and security

Hybrid
A combination of environments is used, such as private environment for most requirements, with an option to "burst" out to a community, or even public environment, for less critical workloads or to handle peaks of need.

Most business users of cloud start out using Private as a first step, to gain experience and confidence with the operational model before moving on to other forms.

Privacy and security in cloud are a concern, not just because of the ways that cloud is used now, but because of fears about future developments as a result of our digital revolution and data explosion:

Big Data
This allows data from many disparate sources to be combined to yield a complex and in-depth view of a subject or person.

The Internet of Things
Everything is increasingly connected to the Internet, and therefore the cloud: cars, domestic appliances, security cameras, etc. This not only raises questions as to whether you want your car to talk to your central heating, but also other security concerns: if you can control your home from afar, so can a hacker or a foreign government.

Big Data and Internet of Everything not only build on the data management capabilities of cloud, they also emphasise the importance of confidentiality in cloud services, because they can compound and multiply the effects of any security weaknesses.

Assuring quality of delivered services

For decades, the IT industry has been trying to make its services more visibly and provably trustworthy by building audited assurances into the delivery processes. These can be verified both internally, for control and risk management, and by external auditors, to obtain certification as an independent proof of trustworthiness.

The recognised way to demonstrate that services are delivered to the quality and security levels required is to ensure that they comply with various standards. But which standards need to be met? You can determine your own requirements – an approach undertaken by some large organisations such as governments and banks. Or you can make a selection from those standards which are generally recognised. Service providers have to back up customers' chosen standards with their own compliance policies.

The relationship between requirements, and compliance to various standards, is complex. Compliance is often misused to explain a "requirement" *("data has to stay in this country, or data centre, because ...")*. But we need more clarity about jurisdictions and real business compliances to aid understanding of the constraints in cloud.

Many standards are applied to IT for assurance audits and compliance checking:

- General "horizontal" standards, e.g. quality measures such as ISO 9001
- IT service management-specific standards: ISO 20000, based on BS 15000, reflecting the best practice embedded within ITIL[7]
- Information security and risk: the ISO 27000 family, comprising to date a broad range of over 30 subject-specific standards[8], superseding the previous ISO13335
- Business continuity: ISO 22301, based on BS 25999, which itself superseded the informal PAS 56 best practice guide
- Environment: ISO 14000, which provides a guideline or framework for organisations that need to systematise and improve their environmental management efforts
- Country-specific standards (see below)
- Market sector standards: see table.

One thing to bear in mind is that the goalposts are constantly moving as standards are frequently refreshed and updated.

There are specific recommendations in some countries which may be interpretations of a current or emerging European standard. For example:

- Data protection regulations where an EU directive is implemented (differently per country) through national laws, but should become an EU regulation during 2015[9]
- Financial regulations, such as Basel III[10] and others set by the ECB and adopted by country financial services authorities, such as De Nederlandsche Bank, FSA in UK, etc.

Implementation of such standards tends to be checked by the supplier for internal control purposes, and also by external (third party) auditors when an independent certification is desirable. Those can ensure that the standards are adhered to on a number of timescales – once, on a repetitive basis, or even on a continuous basis, with increasing degrees of difficulty and cost.

There is also a change regarding the level at which quality control needs to take place. A static BTO environment is relatively easy to control. But in a dynamic AFS supply model, the environment is liable to change frequently and be much harder to control. Dynamism and agility are reasons for adopting cloud services.

So control has to be exercised at a higher and more stable level: that of the entity which manages that environment. And as that management is itself increasingly automated and managed by policy, it has to be exercised at the level of whoever designs, builds, and maintains the management environment (using a process that has been described as policy-based meta-management).

Public Companies	● Sarbanes-Oxley ● Financial Accounting Standards Board (FASB) ● International Standards: ISO 9001, etc. ● Tabaksblat: NL corporate governance code ● PAS 56: business continuity
Banking Brokerage and Financial Services	● US Securities and Exchange Commission (SEC) 17a-4 ● Banking capital regulation: Basel III ● EU Central Bank continuity requirements for SIPS ● NASD (National Association of Securities Dealers) 3010 ● NYSE (New York Stock Exchange) Regulation ● USA Patriot Act: access to financial records ● Gramm-Leach Bliley Act: governing bank separation ● Payment Card Industry Data Security Standard (PCI DSS)
Government	● Department of Defense (DoD) 5015.2 ● US National Records and Archives Admin (NARA) ● Freedom of Information Act ● Security requirements of List X and EKP (UK)
Pharmaceuticals	● FDA Good Manufacturing Practices ● FDA 21 CFR Part 11 ● Occupational Health and Safety Admin (OSHA)
Healthcare	● Privacy of health records: HIPAA

[7] ITIL, formerly known as the Information Technology Infrastructure Library, is a set of practices for IT service management (ITSM) that started as simple operational best practice, but now focuses on aligning IT services with the needs of business.

[8] Particularly relevant for this document is the recently-published ISO27018 (on the protection of personally identifiable information (PII) in public clouds), see https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en and http://www.kempitlaw.com/the-growing-role-of-standards-in-cloud-contracts-some-perspectives-on-iso-27018/

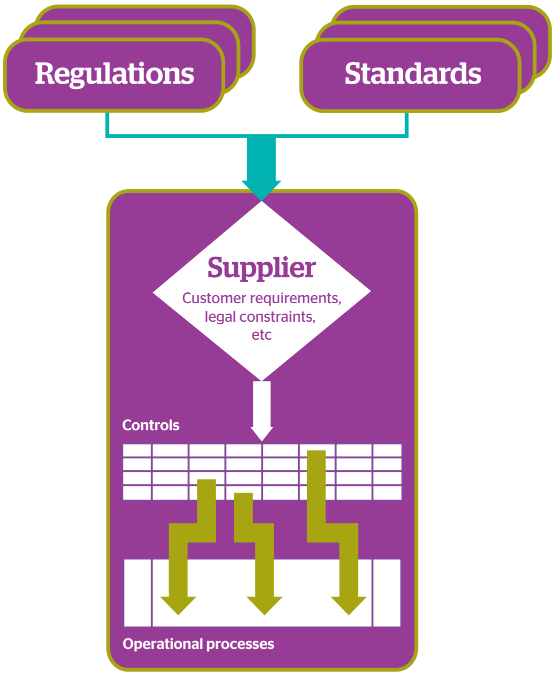
[9] See: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm

[10] "Basel III" is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector.

Building and maintaining a control framework

Suppliers have to determine which regulation and standards they need to comply with to deliver their services, either in general or for a specific service offering. To do that, they analyse and select from the various regulations and standards mentioned above, and determine a superset of controls which will cover the needs of their customers. They can then build those controls into their normal operational processes, and monitor and audit adherence to them.

Some 'meta-mechanisms' are available, such as the COSO[11] and COBIT 5[12] frameworks, allowing suppliers to assure customers that their required standards are being met on an ongoing basis and deliver formal statements to that effect: ISAE3402[13] (previously known as SAS-70) statements.



[11] Committee of Sponsoring Organisations, see http://www.coso.org/ and "The 2013 COSO Framework & SOX Compliance", J. Stephen McNally, June 2013

[12] Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance. See: http://www.isaca.org/cobit/pages/default.aspx?cid=1003566

[13] See http://isae3402.com/

The Atos control framework

Atos has a proven methodology for establishing and maintaining controls, and this provides for a well-managed cloud environment. It takes internal and external rules, objectives and targets, and combines them with our own policies and strategies to assemble a framework which can be used to run the business. These are then used within the defined business processes, to ensure that those processes are fulfilling the needs of the business and, through that, the needs of customers.

There is a governance structure, with supporting organisation structure, to ensure aspects such as controlled delegation of authorities, segregation of duties and anti-fraud management. Key performance indicators (KPIs) are defined and tracked, to ensure that the mechanism fulfils its requirements, and that exceptions are identified and managed before they can affect clients or others. A continuous improvement process (plan, do, check, act) is embedded.

Atos deploys its control framework with a separate but aligned structure for each of its businesses. These businesses include Canopy, our company responsible for the design and sales of cloud services and infrastructure.

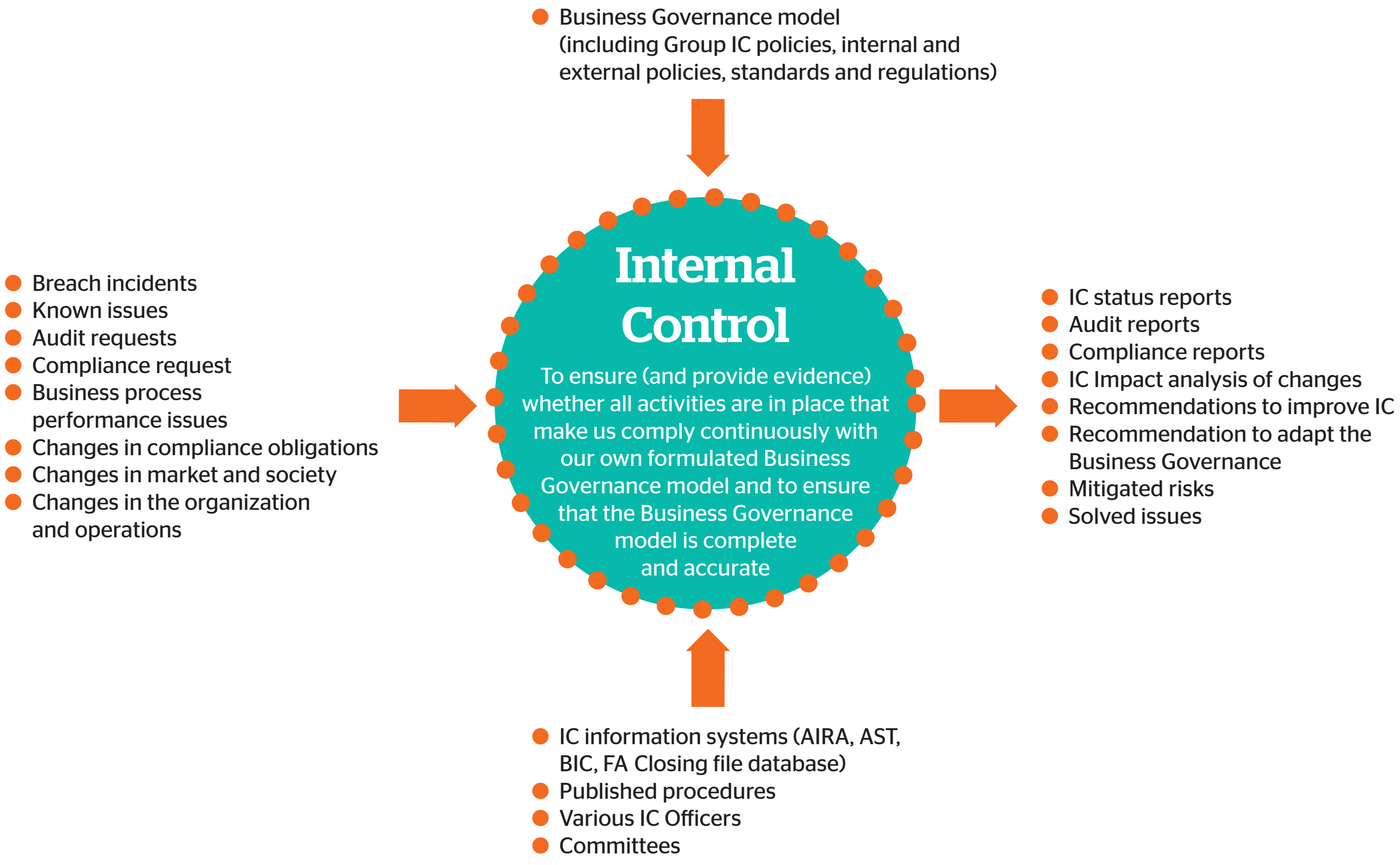
The internal control definition and objectives are clearly identified and published in the Atos Annual Report[14]. There is an identified role for internal audit to check on the process and its execution – independent of lines of management.

It includes a number of major parallel tracks:

- Process to ensure continuous compliance;
- Mechanism to handle requests for new compliances;
- Process for risk-management: for operational, business continuity, contractual and organisational risks;
- Audit management: for planned and spot-check audits;
- Issue-management process, for when issues are identified;
- All backed-up by a continuous process assessment.

An internal control framework, fed by external laws and standards, can be translated into internal control objectives. This is a matrix structure, because one internal control may reflect a common requirement from many overlapping standards.

Supporting tools are in place, to track the adherence to the identified controls, both in the establishment of new business and in



- Business Governance model (including Group IC policies, internal and external policies, standards and regulations)

- Breach incidents
- Known issues
- Audit requests
- Compliance request
- Business process performance issues
- Changes in compliance obligations
- Changes in market and society
- Changes in the organization and operations

Internal Control

To ensure (and provide evidence) whether all activities are in place that make us comply continuously with our own formulated Business Governance model and to ensure that the Business Governance model is complete and accurate

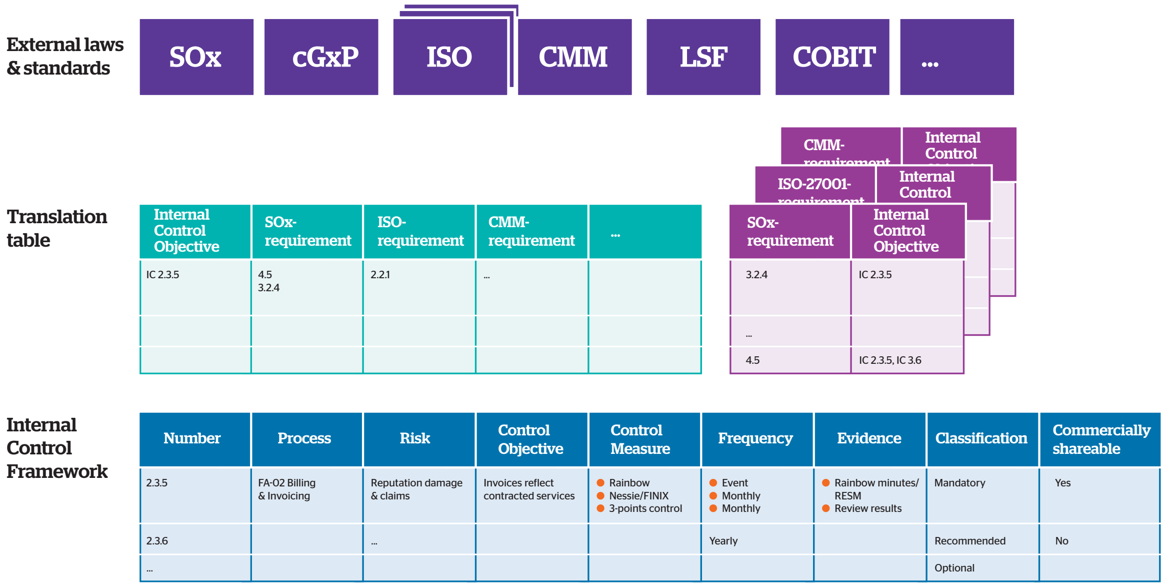
- IC status reports
- Audit reports
- Compliance reports
- IC Impact analysis of changes
- Recommendations to improve IC
- Recommendation to adapt the Business Governance
- Mitigated risks
- Solved issues

- IC information systems (AIRA, AST, BIC, FA Closing file database)
- Published procedures
- Various IC Officers
- Committees

[14] http://atos.net/en-us/home/investors.html

Supporting tools are in place, to track the adherence to the identified controls, both in the establishment of new business and in ongoing delivery. At the core of these is the Internal Control Database (ICDB), acting as the repository for all relevant information.

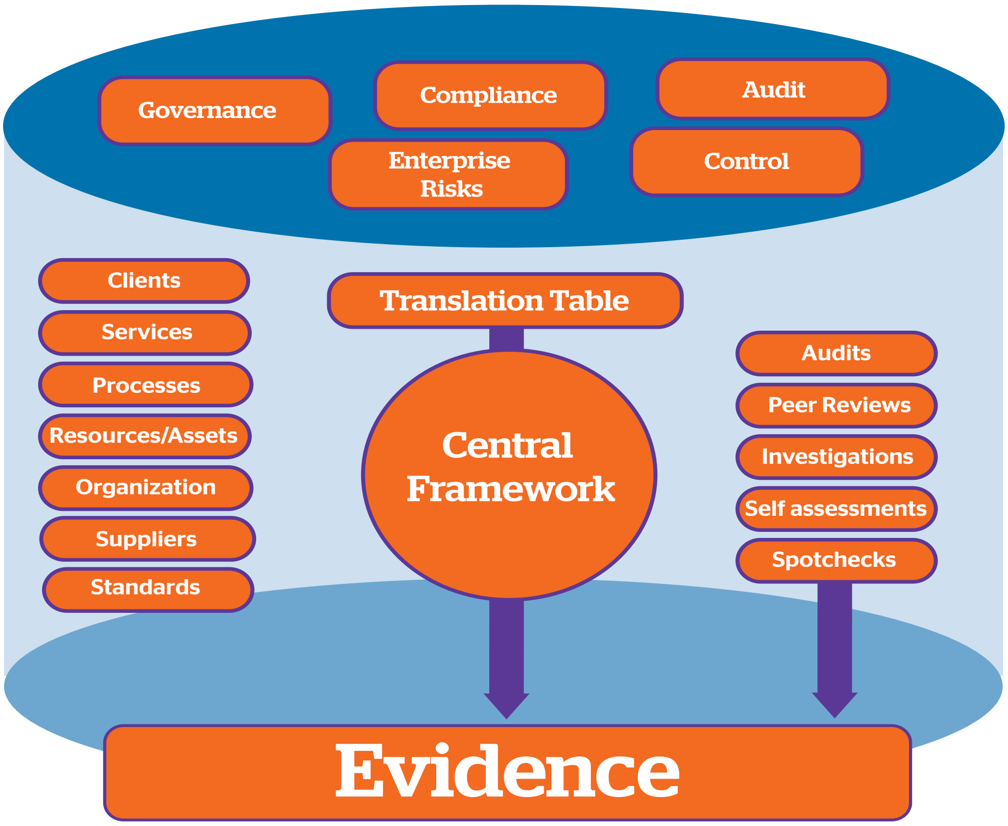
This overall mechanism provides a deterministic means of ensuring that services are delivered in line with current and changing regulations and requirements.



Internal Control Objective	SOx-requirement	ISO-requirement	CMM-requirement	...
IC 2.3.5	4.5 3.2.4	2.2.1	...	

SOx-requirement	Internal Control Objective
3.2.4	IC 2.3.5
...	
4.5	IC 2.3.5, IC 3.6

Number	Process	Risk	Control Objective	Control Measure	Frequency	Evidence	Classification	Commercially shareable
2.3.5	FA-02 Billing & Invoicing	Reputation damage & claims	Invoices reflect contracted services	● Rainbow ● Nessie/FINIX ● 3-points control	● Event ● Monthly ● Monthly	● Rainbow minutes/ RESM ● Review results	Mandatory	Yes
2.3.6		...			Yearly		Recommended	No
...							Optional	



The role for auditors

There is clearly a potential role for auditors in this environment, but it is one that is likely to change over the coming years. The IT services business has long been subject to third-party audits where, rather than allowing every customer to crawl all over their operational environment, suppliers would arrange for one of the recognised audit firms to do it on their (collective) behalf.

Initial, simple audit schemes assume that a supplier may be self-auditing, but this is only adequate for very few customers. Most will require some form of external assurance. Auditors are aware of their changing role in this environment, and the need to address changing needs (see an example from Ernst and Young[15]).

The Cloud Security Alliance (CSA) have developed their own Security, Trust and Assurance Registry (STAR) program, which allows for increasing levels of assurance:

- CSA STAR Self-Assessment is a free offering that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. This information then becomes publicly available, promoting industry transparency and providing customer visibility into specific provider security practices
- CSA STAR Attestation provides for rigorous third party independent assessments of cloud providers
- CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider, based on the requirements of the ISO/IEC 27001:2005 management system standard
- CSA STAR Continuous Monitoring (currently under development and scheduled for 2015 release) enables automation of the current security practices of cloud providers.

CSA are encouraging all parties involved in delivery of such services, including both suppliers and auditors, to join their scheme. They have a global STAR registry of all participants.

Service levels and other concerns

One perennial concern of cloud services customers is whether they will be able to obtain meaningful service levels: not just an indication of an expected level of availability, for instance, but whether there are means in place to ensure it is met, and whether penalties are applicable if it is not met.

At the simplest level, these could be promises of 100% delivery and discounts on charges if that level is not met. A more sophisticated approach could include application of the various management approaches built into best-practice systems such as ITIL, to ensure the meeting of those targets are built into operational practices, but still with an arrangement for penalties where applicable.

As described under section 5 EU and EC activities later in this document, work has taken place with the EC Select Industry Group on this subject, to define a simple starter set of expected service level elements.

[15] Building trust in the cloud, Ernst and Young, June 2014

Why "Europe"?

Politicians are often driven to build cloud services by a desire to improve innovation and create employment (see section 5 EU and EC activities below).

There is also a strong urge to create cloud services with a different ethos from those emanating from the USA: one where integrity is apparently more important than commercial considerations.

A key driver in this second ambition is clarity about where data is located, and who has access to it: to ensure adherence to regulations, especially to those concerning the protection of personal data.

This is partly reflected in the different legal status regarding protection of such data[16]:

- In the USA, it is a matter of civil law: if you don't like what someone has done to your data, you can sue them after the event
- In Europe, it is a matter of criminal law: you can be prosecuted if you put such data at risk, even before any actual infringement takes place, and can be fined very substantial sums[17].

The difference between the two approaches is emphasised by a recent statement by the European Data Governance Forum[18], representing European data protection authorities, who declared[19]:

- *"The protection of personal data is a fundamental right. Personal data (which includes metadata) may not be treated solely as an object of trade, an economic asset or a common good"*
- *"Technology is a medium that must remain at the service of man. The fact that something is technically feasible, and that data processing may sometimes yield useful intelligence or enable the development of new services, does not necessarily mean that it is also socially acceptable, ethical, reasonable or lawful."*

The whole document could be read as a manifesto for the European data protection ethos.

This issue was sharpened for Europe by the revelations by Edward Snowden on 5 June 2013 that US intelligence agencies had been collecting information under the PRISM system[20] with the active cooperation of many cloud providers[21].

The US government has given itself wide powers to undertake such activities under legislation such as the Patriot Act and FISA. This legislation obliges US companies and individuals to give US agencies access to whatever data they have on surveillance subjects, and are forbidden from disclosing to those subjects that they are doing so.

Crucially, it applies to US companies operating not only within the USA, but anywhere in the world via subsidiaries. So although American cloud providers are building data centres in Europe to assure customers that their data will remain within Europe, this does not exempt them from those disclosure obligations[22].

[16] http://www.zdnet.com/article/safe-harbor-why-eu-data-needs-protecting-from-us-law/

[17] Under current plans to revamp and align European data protection rules, there would be provision for fines of up to $125m, or 5% of a company's revenue, whichever was greater, if an individual's online information were misused: http://bits.blogs.nytimes.com/2015/03/04/europes-digital-regulator-vows-to-intervene-on-technology-abuses

[18] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[19] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp227_en.pdf

[20] See http://www.theguardian.com/us-news/the-nsa-files

[21] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[22] Atos is an SE: a European company (société européenne - SE), often referred to by its Latin name 'Societas Europaea', and thus free of such obligations, at least for its operations outside of the USA http://www.computing.co.uk/ctg/opinion/2403739/why-amazons-new-eu-data-centres-are-just-as-vulnerable-to-nsa-surveillance-as-their-us-ones

One response of the American cloud providers was to attempt to prove that European security agencies are making similar demands on European providers[23]. Whether or not this is true, most Europeans are inured to the idea that their own agencies have all the information on them that they might want. It is the thought of agencies from non-European countries acquiring that data - especially those from the USA – that creates most concern.

A recent report from Forrester[24] concludes that up to a third of technology and business decision-makers at non-US firms said they had moved any data away from US-based partners. 32% of such users in Latin America had done so. Perhaps more importantly, more than 90% of them were taking steps such as encryption to protect their data.

All the more reason therefore to establish a capability to deliver the services that are required in Europe, where they can be, and seen to be, under the supervision of, and susceptible, to European law.

In The Netherlands[25], a judge has scrapped the data retention law, saying that while it helps solve crime it also breaches the privacy of telephone and Internet users. The judge conceded that scrapping the data storage "could have far-reaching consequences for investigating and prosecuting crimes", but added that this could not justify the privacy breaches the law entailed.

European institutions have, however, been careful to emphasise that they are not trying to create 'fortress Europe' by blocking US or other countries' suppliers from delivering services to the European market. Rather, they are trying to attain a high target where all suppliers from any region adhere to the same stringent rules, rather than lower the bar just to give easy access. European suppliers simply aspire to being better at meeting the rules of their own region than are those from outside.

There are also many concerns regarding the danger to intellectual property (IP), if critical data was put into such a cloud environment. The worry is that if other national agencies can gain access to our systems, could they pass information on to our competitors? The danger is seen to come not only from the American agencies[26].

Once such European services are established, they could well be used by organisations from the rest of the world, who want the assurance that their data is being properly managed and handled. The formula could also be exported to other regions so as to establish, for instance, a Trusted Australian Cloud. There are some who harbour ambitions that, just as some places become tax havens, Europe could become the 'cloud haven' for the world.

"We need to make sure data is properly protected. Only then can people fully trust online services and have the confidence to use them, especially across borders",

EC Vice President Andrus Ansip at the European Policy Centre in Brussels, April 2015

The European Commission is addressing the need for a Digital Single Market (DSM), to

- encourage the development and adoption of EU cross-border services,

- strengthen data protection and roll out fast broadband, and

- use those to grow the digital economy.

http://ec.europa.eu/priorities/digital-single-market/docs/dsm-factsheet_en.pd

Neelie Kroes, then Vice President of the European Commission,

"While Europe is not the leading provider of cloud services globally it is known for relatively high standards of data protection, security, interoperability and transparency about service levels and government access to information. These characteristics provide a solid basis for further development of cloud computing in Europe, as users become more conscious of the need for cheap, flexible IT services, without wanting to compromise privacy."

Memo, 15 October 2013

[23] A Global Reality: Governmental Access to Data in the Cloud: A comparative analysis of ten international jurisdictions: Hogan Lovells, May/July 2012

[24] PRISM's Impact On The US Cloud Industry, Ed Ferrara and James Staten, Forrester, February 2015

[25] http://www.theguardian.com/technology/2015/mar/12/data-retention-netherlands-court-strikes-down-law-as-breach-of-privacy

[26] See "Producer ASML is hacked by Chinese government", at: http://techn4all.com/producer-asml-is-hacked-by-chinese-government/

EU and EC activities

Europe consists of 28 countries, each with its own government and legislation. If any common approach is to be determined in Europe[27], it is incumbent upon institutions such as the European Commission (EC) to be the catalyst.

In September 2012, the EC published a document[28] entitled "Unleashing the Potential of Cloud Computing in Europe" which identified the potential impact of cloud on the economies of Europe, and then outlined some steps to capture the benefits.

Three key actions were identified:

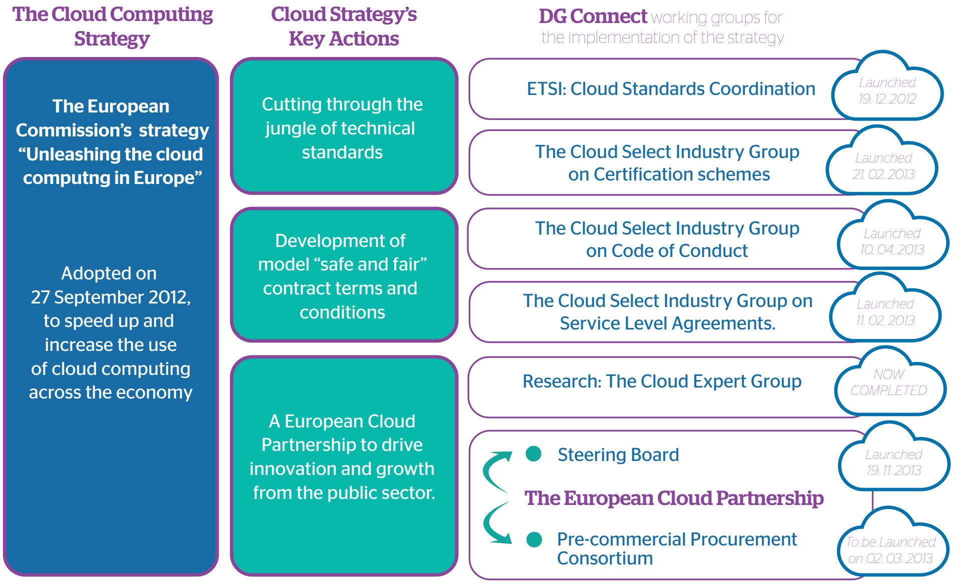
1: Cut through the Jungle of standards

2: Safe and Fair Contract Terms and Conditions

3: Establish a European Cloud Partnership to drive innovation and growth from the public sector.

This was followed by an EC Memo in October 2013, which begins by stating that:

> *"Europe should aim to be the world's leading 'trusted cloud region'. Widespread adoption of cloud computing is essential for improving productivity levels in the European economy; but the spread of cloud could slow in light of recent revelations about PRISM and other surveillance programmes. These surveillance revelations have also led to calls for national or regional cloud computing initiatives. This challenge must be addressed and also turned into a Europe-wide opportunity: for companies operating in Europe to offer the trusted cloud services that more and more users are demanding globally. The Commission is strongly against a 'Fortress Europe' approach to cloud computing. We need instead a single market for cloud computing."*


The Cloud Computing Strategy

The European Commission's strategy "Unleashing the cloud computng in Europe"

Adopted on 27 September 2012, to speed up and increase the use of cloud computing across the economy

Cloud Strategy's Key Actions

Cutting through the jungle of technical standards

Development of model "safe and fair" contract terms and conditions

A European Cloud Partnership to drive innovation and growth from the public sector.

DG Connect working groups for the implementation of the strategy

ETSI: Cloud Standards Coordination — Launched 19. 12. 2012

The Cloud Select Industry Group on Certification schemes — Launched 21. 02. 2013

The Cloud Select Industry Group on Code of Conduct — Launched 10. 04. 2013

The Cloud Select Industry Group on Service Level Agreements. — Launched 11. 02. 2013

Research: The Cloud Expert Group — NOW COMPLETED

The European Cloud Partnership

- Steering Board — Launched 19. 11. 2013
- Pre-commercial Procurement Consortium — To be Launched on 02. 03. 2013

Neelie Kroes, then Vice President of the European Commission.

> *"We need trust if we want to build an open cloud market"*

Viviane Reding, then Vice-President of the European Commission, EU Justice Commissioner:

> *"Data protection is not red tape or a tariff. It is a fundamental right and as such it is not negotiable".*

[27] Pending implementation of common law: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm and http://www.scmagazineuk.com/new-eu-data-protection-law-to-arrive-in-2015/article/395142/

[28] European Commission's communication on "Unleashing the Potential of Cloud Computing in Europe", Brussels, 27.9.2012, COM(2012) 529 final; http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy

[29] http://europa.eu/rapid/press-release_MEMO-13-898_en.htm

European Cloud Partnership

The EC has been forging closer links between government and industry in a bid to shape the best cloud landscape in Europe. Part of its cloud strategy was to establish a European Cloud Partnership[30] (ECP), where industry heads such as Atos CEO, Thierry Breton, joined senior national and EC officials to design a new roadmap for cloud in Europe.

Atos' Canopy is one of the leading providers in the European cloud industry, and has played a major role in supporting these initiatives to help change both perceptions and reality in the industry's operations. It will also play its part in developing trusted cloud arrangements throughout the world.

The ECP produced a 24-page report[31] entitled 'Establishing a Trusted Cloud Europe' which identified two groups of actions:

- Creation of a flexible common framework of best practices
- Systematic consensus building.

The potential benefits of cloud were identified:

"The expected cumulative economic effects of cloud computing between 2010 and 2015 in the five largest European economies alone is [sic] around € 763 Bn[32]. The cloud economy is growing by more than 20%[33] and could generate nearly € 1 trillion in GDP and 4 million jobs by 2020 in Europe[34], with the support of the right policy framework."

The actions regarding standards/security, Code of Conduct, fair contracts and SLA were delegated to a number of Select Industry Groups (SIGs).

At one stage, there was discussion within the ECP of the feasibility of establishing a "Schengen Cloud": a shared environment, similar to the arrangement regarding passport control within most of the European Member States, where each country would commit to trusting the data protection controls of the others.

The Cloud Legal Project

The Trusted Cloud Europe document prompted a response from the Cloud Legal Project[35], albeit one that is mostly in agreement. That team is responsible, inter alia, for the definitive tome on cloud computing law[36], which proves to be a very useful source of reference for all involved in these subjects.

It has also produced documents[37] on 'Policy, Legal and Regulatory Implications of an EU-Only Cloud' and 'Technical Issues for an EU-only Cloud', sponsored by the Microsoft Cloud Computing Research Centre. These go into some depth (20+ pages each) on their respective subjects, providing exhaustive insight into some of the issues that arise from such a development.

[30] http://ec.europa.eu/digital-agenda/en/european-cloud-partnership

[31] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935

[32] Centre for economics and business research (2010): The cloud dividend report

[33] IDC Worldwide Cloud Black Book, 4Q 2012 update, April 2013

[34] IDC (2012): Quantitative estimates on the demand for cloud computing in Europe and the likely barriers to take up.

[35] http://www.cloudlegal.ccls.qmul.ac.uk/

[36] Cloud computing law, ed. Christopher Millard, Oxford University Press, 2013, ISBN 978-0-19-967168-7

[37] Both documents were produced in draft for discussion at their 1st Annual Symposium, September 2014, but are now available in updated form at http://ssrn.com/abstract=2527951 and http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-863.html.

EC Select Industry Groups

A number of Select Industry Groups (SIGs) were established, chaired by the EC and staffed by people from both large IT services providers[38] and SMEs, often with quite divergent interests and aims. They were intended to address the task of cutting through, or at least understanding, the jungle of standards.

To date, their work has involved assembling the required "framework of best practices", but as a process of collection rather than yet of selection. Because of the nature of the groups – often 20-30 people in a plenary meeting, and/or supporting long email distributions – it has proved difficult both to take real decisions and achieve consensus.

That means that any probable European Cloud Standards do exist somewhere within the outputs from those groups, but as yet a process of understanding, analysis and selection is required to identify them. This is an exercise which Atos itself has in process, to ensure that we can best advise clients and adopt them for our own services.

ETSI - Cloud Standards coordination:

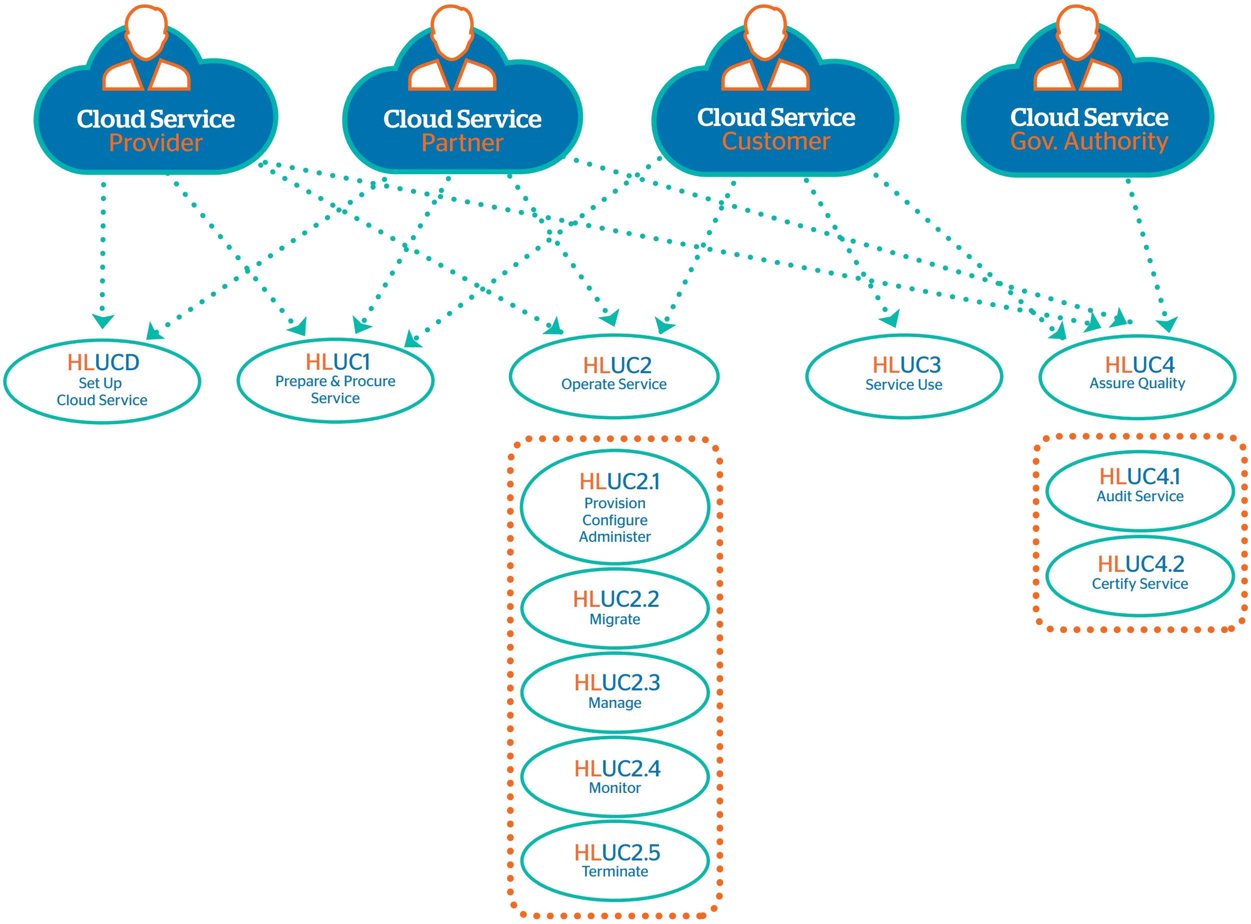
The European Telecommunications Standards Institute (ETSI) was tasked with "cutting through the jungle of standards", and mapping existing cloud computing standards in collaboration with all relevant stakeholders. This was done building on previous work and knowledge, e.g. much of the section on security was apparently derived from the work of the Cirrus project[39].

ETSI delivered an intermediary standards overview in June 2013 and delivered its final results in November 2013. That working group produced a useful analysis[40] of the applicable standards within the arena of cloud, rather than any strong recommendations as to a specific set which should be adopted, how and when.

The final report provides:

- A definition of roles in cloud computing
- The collection and classification of over 100 cloud computing use cases
- A list of around 20 relevant organisations in cloud computing standardisation and a selection of around 150 associated documents, standards and specifications as well as reports and white papers produced by these organisations
- A classification of activities that need to be undertaken by cloud service customers or cloud service providers over the whole cloud service life-cycle
- A mapping of the selected cloud computing documents (in particular standards and specifications) on these activities.

The 110 use cases were reduced to 90 and then refined into high-level use cases to cover a cloud lifecycle, as represented in the following diagram:

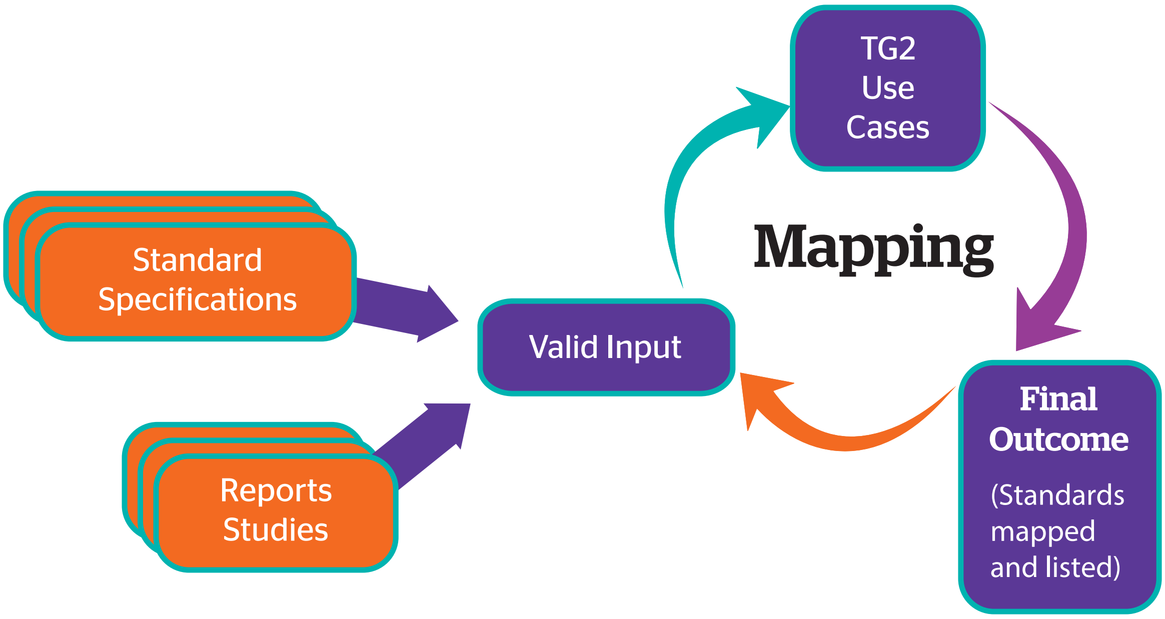


[38] Full disclosure: the author of this White Paper and some of his colleagues took part in a number of these SIGs.

[39] http://www.cirrus-project.eu/

[40] http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

The mapping process is shown in the following diagram:



The report concluded that there was possibly too much choice for customers, but that "cloud standardisation is much more focused than anticipated. In short: the cloud standards landscape is complex but not chaotic and by no means a 'jungle'.". Indeed, it concluded that once having analysed the standards against the specific use cases, "the number of relevant standards in a given activity is rarely above two".

Interoperability was seen as a specific concern, due to the rapid evolution of cloud technologies: *"Interoperability standards need to be formal and complete enough that cloud computing workflows can be automated, but flexible enough that new concepts in the underlying technology or in a particular domain (e.g. public cloud procurement) can be quickly introduced and accommodated."* A more recent report from the Cloud Standards Customer Council[41] may help clarify how this can better be achieved.

SIG - Service Levels Agreements

This working group has gone through a number of phases and produced a sequence of three reports:

- Atos produced a report describing 11 key service level (SL) indicators
- Gartner provided details derived from their standard texts on cloud service levels
- A smaller task force of five organisations addressed performance, security, data management, and personal data protection.

Some concerns arose during these discussions, the most significant of which was a tension between those who wanted to produce a simple set of specific recommendations, and those who wanted to allow for a broad range of requirements and avoid specific level recommendations. There was also a concern that the approach taken to define the levels was simplistic and did not accommodate all types of inputs, outputs and outcomes[42].

The contents of the final draft report[43] include:

- Principles: technology neutral, comparable, etc.
- Vocabulary: terms used
- Performance objectives
- Security objectives
- Data management objectives
- Personal data protection objectives.

[42] The relevance of service levels which are defined as inputs, outputs and outcomes:

- Inputs were the original, lowest-level definition: it commits to (getting the processes to) do something. Examples are responding when a server fails, answer the phone in three rings, etc. Typically measured day-to-day pr weekly. There is no guarantee that what you will do will help;
- Outputs are how most are defined these days: it commits to something like a server being available, etc. To deliver them, you have to think of some availability management-type processes. Typically measured on a monthly basis. There is still no guarantee that what the server delivers will be useful; just that it will be there;
- Outcomes are what suppliers should be aiming at: it commits to things like customer satisfaction, ease of doing business, etc. Here you have to think about things like application functionality, too. Difficult to measure, typically on an annual basis. This is what business customers really want.

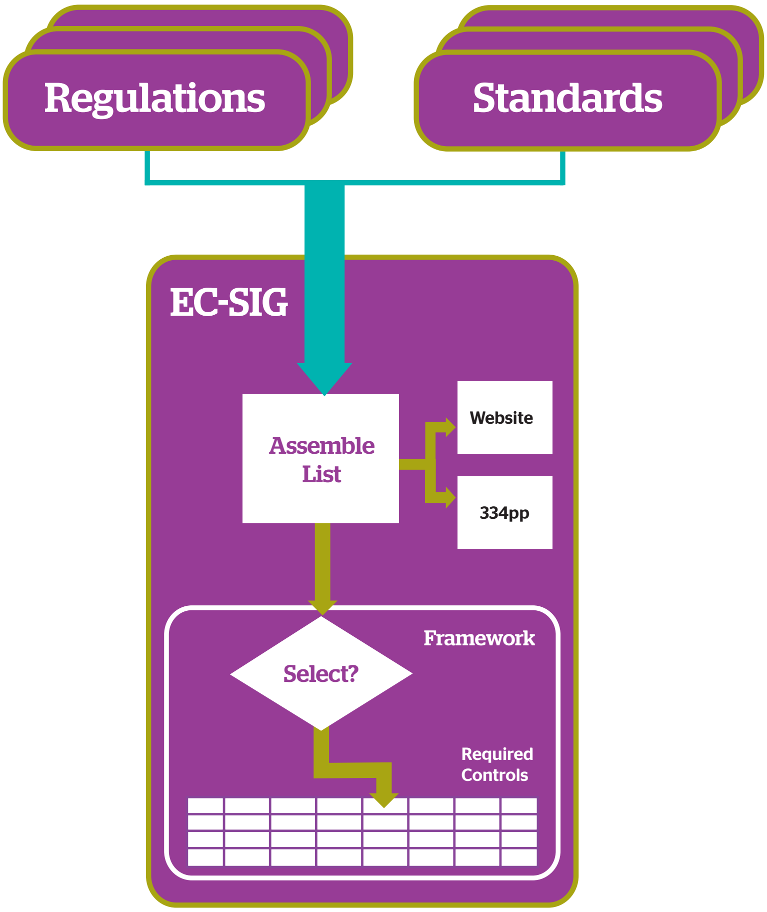
These levels are cumulative: you have to deliver inputs to achieve outputs, and outputs to deliver outcomes.

[43] Cloud Service Level Agreement Standardisation Guidelines, 22/08/2014, FINAL DRAFT https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

SIG – Certification

The process of producing a certification structure has largely been driven by the ENISA organisation. It basically consisted of two phases:

- Trilateral Research[44]: identified 24 schemes and their relationships; a 334-page document was issued, listing them all
- ENISA ran a group producing two documents:
  - CCSL, a list of schemes held online
  - CCSM, a meta-framework: formally released in January 2015.



The approach is shown in the diagram:

- Identify relevant schemes
- Map the requirements per scheme to control objectives, on the grounds that there are a large amount of similarities/ overlaps.

There was a concern that security is only a subset of the necessary controls, and there are many others necessary to deliver a sustainable service which are not yet being considered. There is also a danger of confusion arising between objectives and the measures necessary to achieve them. The process does not (yet) identify a means of standardising/ rationalising the results.

Certification contents CCSL: a non-filtered and non-judgemental listing of available schemes, as submitted by their owners . An amount of basic information is held per scheme:

- General
  - Name, Governance organisation and model, URL, target(s) for certification
- Underlying information
  - Source of standard or best practice, structure, covering which assets, available to public?, Based on (other) international standards, example requirements
  - Assessment process and certification
  - Process, accredited bodies, quality assurance, expiry, self-assessable?
  - Current adoption and usage
  - Level of use, global reach, applicability
  - Outlook and plans for the future.

Certification contents CCSM: issued in January 2015. This first version of CCSM is restricted to network and information security (NIS) requirements. It is based on 29 documents with NIS requirements from 11 countries (United Kingdom, Italy, Netherlands, Spain, Sweden, Germany, Finland, Austria, Slovakia, Greece and Denmark). It covers 27 security objectives and maps these to 5 cloud certification schemes. The framework has been implemented as an online tool .

At the time of writing (mid 2015), further schemes are being added, and work (by ENISA, aided by Deloitte) continues on analysing the security control objectives of various schemes and mapping them to the CSSM framework..

[44] A niche consulting firm, commissioned by the EC: http://trilateralresearch.com/

[45] https://resilience.enisa.europa.eu/cloud-computing-certification/

[46] See Cloud Certification Schemes Meta-framework: CCSM, http://www.enisa.europa.eu/media/press-releases/enisa-cloud-certification-schemes-metaframework

[47] https://resilience.enisa.europa.eu/cloud-computing-certification/

SIG - Code of Conduct on Data Protection

This working group was originally launched as a Code of Practice exercise: a structure for cloud providers to voluntarily say under what conditions they deliver (e.g. to which standards they adhere), and self-assure that they do so. The first discussions were based on the UK Cloud Industry Forum Code of Practice.

Atos then joined a smaller drafting team. This group submitted a draft to the Article 29 Working Party (the association of EU Data Protection authorities[48]), from which 18 comments were received. These were in turn addressed and the results re-submitted in January 2015.

The document covers data protection, security, governance requirements, and includes a process to implement adherence. Current contents[49] include:

- Structure, purpose and scope
- Conditions of adherence
- Data protection: contractual terms, lawful processing, transfer, audit, liabilities, cooperation, complaint handling, confidentiality, law enforcement requests, data breaches, termination
- Security requirements: objectives, implementation guidance, transparency
- Governance: administration, procedures, compliance marks[50], enforcement, finances
- Annexes:
  - Transparency
  - Security objectives
  - Template declaration of adherence
  - Process checklist.

On data types and locations, the work to date has not done anything to differentiate between different types of data and how they should be handled: e.g. whether personal medical records should be handled differently from telephone logs. That is largely left to the data controller to determine. This code then explains how they can be sure that the data processor will follow their instructions. The relevance of the location of that data has been discussed in a workshop with the EC and various expert parties towards the end of February 2015, and may form the subject of future deliverables.

> *“The Internet platforms of the future must be more open and interoperable and be based on standards with a significant contribution from European industry”,*
>
> The EU Digital Commissioner, Guenther Oettinger, Hanover, April 2015

[48] http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm

[49] Data Protection Code of Conduct for Cloud Service Providers, 51 pp, dated 19 January 2015

[50] "Any CSP which has been duly registered in the Code's public register is entitled to use the applicable Compliance Mark adopted by the Code of Conduct Steering Board. Separate Compliance Marks will be foreseen in order to provide transparency to the customers on the adherence choices of the CSP, and notably whether the CSP has elected to conduct a self-assessment followed by self-declaration in accordance with section 7.2, or whether the CSP has elected to undergo certification by third party auditors in accordance with section 7.3."

Cloud for Europe

One of the outcomes from the ECP is a project called Cloud for Europe[51], which is running a pre-commercial procurement (PCP) exercise.

PCP is a construction whereby government organisations can fund research and innovation (only) in particular subjects, without it being considered as state subsidy.

Cloud for Europe is tendering research and innovation to assist take-up of cloud computing in the public sector. The work to be done is defined in three lots:

- Federated Certified Service Brokerage (FCSB)
- Secure, Legislation-Aware Storage (SLAS)
- Legislation Execution (LE).

It is expected that bidders will address these challenges by innovative technical solutions.

It will be seen that there is a common requirement across these three lots for an understanding and possible codification of the necessary legislation and regulations to which the service has to comply. Underneath those structured requirements, the actual services to be provided – brokerage, storage and processing – are well-known and well-established cloud service capabilities.

Bids for funding are (currently) due in early in 2015.

General Data Protection Regulation (GDPR)

Various institutions of the European Union (the Commission, Parliament and Council) are in process of agreeing the forthcoming EU General Data Protection Regulation (GDPR), which will overtake the current Data Protective Directive.

There are currently different variations under discussion in those EU bodies, and it is pointed out that "nothing is agreed until everything is agreed". The discussion involves all 28 Member States (MS) of the EU, and so far nearly 4,000 amendments have been tabled; the previous Directive only involved 15 MS's. This time, the legislation will be a regulation, meaning that it will take automatic effect across the whole EU, about two years after it is adopted.

The changes[52] will have significant effects for all parties involved: data subjects, data controllers and data processors:

- Processor (e.g. IaaS provider) liability changes: they are liable for the entire amount of any damages, unless there is a written allocation of responsibility that says otherwise and/or they can prove it is not their fault. Fines can be huge (5% of global turnover or €100m, whichever is greater)
- Controllers have to choose a Processor with sufficient guarantees, including approved codes of conduct, certifications, etc. And they have to be able to demonstrate compliance.

Each party must appoint a Data Protection Officer, who must be sufficiently qualified to oversee adherence to the legislation.

Controllers must choose Processors who provide sufficient guarantees that they implement measures which will meet the GDPR. In turn, the Processor is assumed to know what the Controller is doing on their platform, and assist them in ensuring compliance, both of which may prove difficult in a cloud environment. Further, they are obliged to inform the Controller if their instructions breach the GDPR.

One way of at least partly demonstrating compliance is by use of relevant certifications or codes of conduct, as described elsewhere in this document. There is discussion of a "European Data Protection Seal"[52] as a means of indicating Data Protection Authority approval.

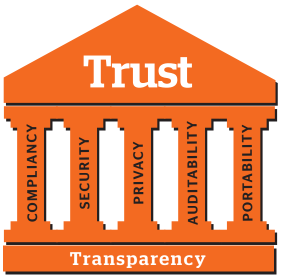
[51] http://www.cloudforeurope.eu/

[52] See Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation, from Tilburg University and Queen Mary University of London, at http://ssrn.com/abstract=2405971

[53] See https://www.european-privacy-seal.eu/EPS-en/Home

Trust

Business decisions tend to be taken on an emotional basis -- even if justified rationally. Users are less likely to make use of a service if they feel uncomfortable doing so. Trust is a characteristic of a bilateral relationship and may be limited to a specific context. For a trust relationship to exist in any one direction one party must be trustworthy and the other must trust them[54].



The House of Trust in Cloud - anchored in the EU

There are various ways in which trust can be built and shown, including:

- Long-term relationships: you have worked successfully with this party for a number of years;
- others have worked with them and they have a good reputation
- Assured and provable security properties (see the House of Trust in Cloud diagram)
- Independent certification by a recognised body
- Audits (internal and external third-party), assessments, testing, verification
- Monitoring actual deliveries against expectations.

The use and transparent sharing of control frameworks, as described elsewhere in this document, can go a long way towards establishing that a suppler is trustworthy.

Demand and supply

In order to put a suitable structure in place, across the whole services supply chain, it is necessary to make preparations on both the demand (user and customer) and supply sides.

Previously, as described in the BTO delivery model, such deployments could happen simultaneously, as systems and services were deployed as part of the implementation of a services contract. However, one of the changes brought about by the move to services such as cloud is that the services are, and indeed have to be, pre-existing. There are thus asynchronous processes for the supply and use of the services, as shown in the following diagram.

That means that the supplier has to have its environment ready, including any necessary compliances and certifications, before the customer comes along to use it. The supplier therefore needs to be able to predict to a large degree, what compliances will be required by their typical customer. In fact, they need a superset of compliances that could be required by any of their predicted customers.

One key generic requirement that arises in the move over to the use of services is the need for transparency, or rather visibility: a customer wants to understand to what controls services will be delivered and the settings of those controls. Ideally, they want access to a dashboard showing the relevant KPIs for their services.

That does not mean that they have to see all of the inner workings of the operational factory: suppliers will anyway be reluctant to give them free access, because much of what is implemented represents the intellectual property of the supply organisation. And most customers cannot anyway be expected to understand the inner workings behind the scenes of their service delivery. A useful analogy might be to consider it as the pressure and temperature gauges outside a boiler room: you can get an indication of how it is going to be inside, without having to go in.

In cloud services, key factors of that transparency/visibility which all responsible customers will want to know, include:

- Where is my data?
- Who has access to it?
- Who has accessed it?

What is needed is a form of CALS-like product traceability for data.

In current circumstances, as with systems such as the NSA's PRISM, this raises the question as to whether access by legal agencies would be tracked and shown. While most of us, as individuals, would like to know whether our data has been accessed, we may also recognise that it would defeat the object of our own country's security agencies to make it known. This is another reason for some degree of local/ regional service delivery.

When addressing data protection in cloud services it is necessary to consider which legislation/ jurisdiction applies. That can usually be determined by territory/physical location, but it may be the location of a number of components:

- The data subject: the person(s) about whom the data is held
- User of that data: typically themselves a customer of the cloud service provider

[54] See Trust mechanisms in cloud computing, Jingwei Huang and David M. Nicol, University of Illinois, http://people.cs.vt.edu/~irchen/5984/pdf/Huang-JCC13-slide.pdf

- Cloud service provider, either their local offices and/or their HQ
- Data centre(s) used to store and process that data
- Any backup copies of the data, for business continuity reasons, which could be far away from the prime location
- Operational and support staff, who could be off-shored somewhere else in the world.

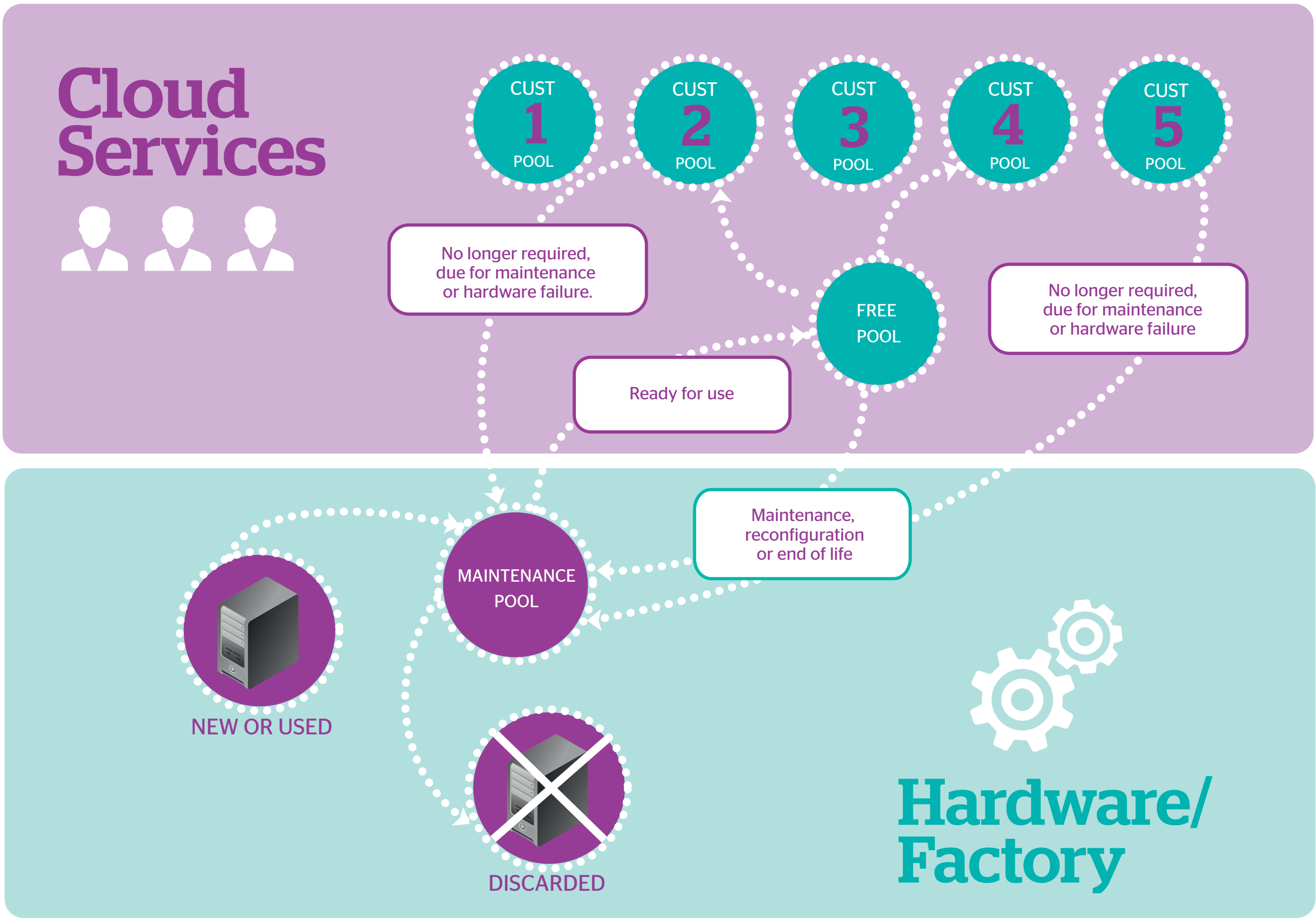
One way of overcoming at least some of these difficulties within a European context is the advent of Binding Corporate Rules (BCR). BCR are designed to allow multinational companies to transfer personal data from the European Economic Area to their affiliates located elsewhere in the world in compliance with local data protection regulations. In order to be certified, companies must demonstrate to all local data protection authorities that BCR are not merely principles and commitments but actions that have been implemented to ensure adequate safeguards for protecting personal data throughout the organisation. In a nutshell, BCR are a Group Policy on Data Protection which is officially recognised by the Data Protection Authorities in Europe .

Having determined a location, the question arises as to what the data protection regulations are in that jurisdiction. Unless and until the Europe-wide regulations are in place (see elsewhere), this can be determined per country; various sources are available to assist this process .

A key aspect here are the roles regarding the data being held and processed: who is the controller and who is the processor?

- 'Data Controller' means a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data
- 'Data Processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of and under the strict instructions of the Data Controller.

For most purposes, it seems to be recognised that the entity responsible for the application and its use of data is the data controller, whereas a supplier providing (cloud or conventional) infrastructure to run that application is only a data processor.


Cloud Services
CUST 1 POOL
CUST 2 POOL
CUST 3 POOL
CUST 4 POOL
CUST 5 POOL
No longer required, due for maintenance or hardware failure.
FREE POOL
No longer required, due for maintenance or hardware failure
Ready for use
Maintenance, reconfiguration or end of life
MAINTENANCE POOL
NEW OR USED
DISCARDED
Hardware/ Factory

[55] ATOS BCR, 21 November 2014, http://atos.net/en-us/home/we-are/news/press-release/2014/pr-2014_11_20_01.html

[56] See: http://www.dlapiperdataprotection.com/#handbook/world-map-section

Other considerations

The availability and integrity of any data held and processed has always been a primary concern within IT. It remains so within a cloud environment for all except the most casual use. Indeed, it raises the question of whether the relevant cloud services can be trusted to be the prime, or even only, repository for critical data. Cloud data should be considered for replication and/or backup, just like any other data repository.

Portability is also a concern: can I get my data out/back? That depends on a number of factors, beyond the attitude of the body holding it, including the volumes involved, the costs of doing so, what formats it will be in, and the feasibility of any necessary downtime in a real-time context. Even having retrieved your data, the question still remains whether you can process it elsewhere, or if it requires such proprietary application capabilities that this is not feasible.

Protection of Intellectual Property (IP) raises many considerations, especially where services are "free": some cloud suppliers' terms and conditions give the supplier rights not only to access but also to make use of the users' data. Users need to beware of and avoid inadvertently agreeing to such terms: easily done by just "ticking the box" without reading the terms and conditions document. Even where the supplier is not making such claims for themselves, there is always a danger of others seeing the cloud as a useful way to hack into a competitor's data.

Encryption is often mentioned as an option to overcome the fear of data being misused. Indeed, it is a necessary option[57], although not without its own issues:

- It not provide a cure for everything, e.g. data still has to be unencrypted to process and to present to end users
- it introduces complexities and risks of its own: e.g. key management is necessary
- it may not be proof against all access: some agencies may have "back doors" or the sheer processing capacity to crack simple encryption algorithms.

Corporate Social Responsibility (CSR) means that many organisations are concerned about the environmental impact of their activities; getting someone else to hold and process the data does not obviate those responsibilities. For that reason, there are increasing demands for the carbon footprint of cloud services to be made available[58].

[57] Forrester report that over 90% of businesses with data resident in clouds use some form of encryption: PRISM's impact on the US cloud industry, February 2015

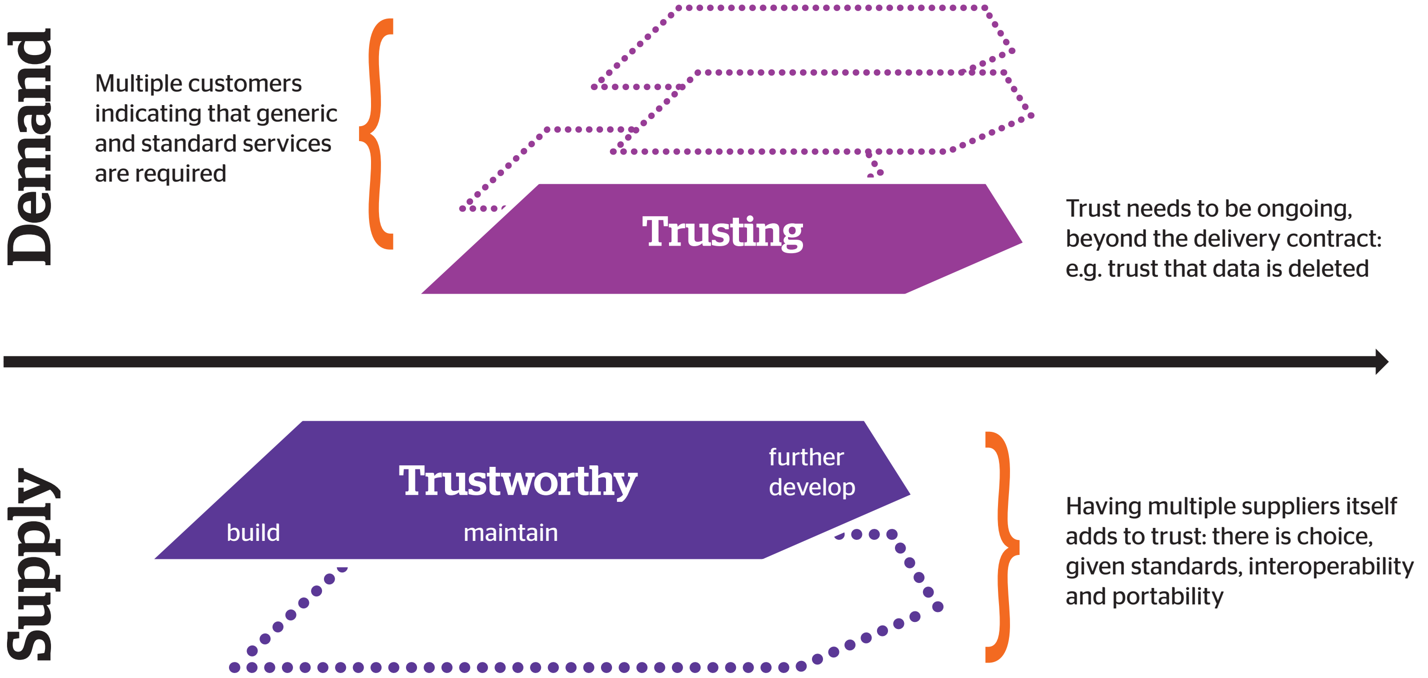
[58] Proof of Concept: Carbon Footprint and Energy Efficiency, Open Data Center Alliance, 2013: http://www.opendatacenteralliance.org/

The Trust Roadmap

Introducing improvements such as the introduction of cloud services, calls for a change in mind-set on both the demand and supply side of a service relationship. Indeed, in traditional IT supply, the IT Manager saw themselves as both demand and supply. The demand side represents the needs of the business and the supply side fulfils those needs in the most effective way.

The supply of IT infrastructure is moving over from a tangible, box-based service to one that is virtualised and evolving. It has to do so in a well-controlled and incremental process, as businesses continue to rely on the services throughout. How can we plan to get there and how will we know when we are actually there?

Trust needs to be built on both sides of the supply chain, as the following diagram shows. Suppliers need to establish a trustworthy environment: one in which customers can be confident. Customers then need to build confidence in that environment. This is more than a bilateral arrangement: having multiple suppliers delivering services to multiple customers mitigates towards standard methods of establishing trust, if not standard services.



Multiple customers indicating that generic and standard services are required

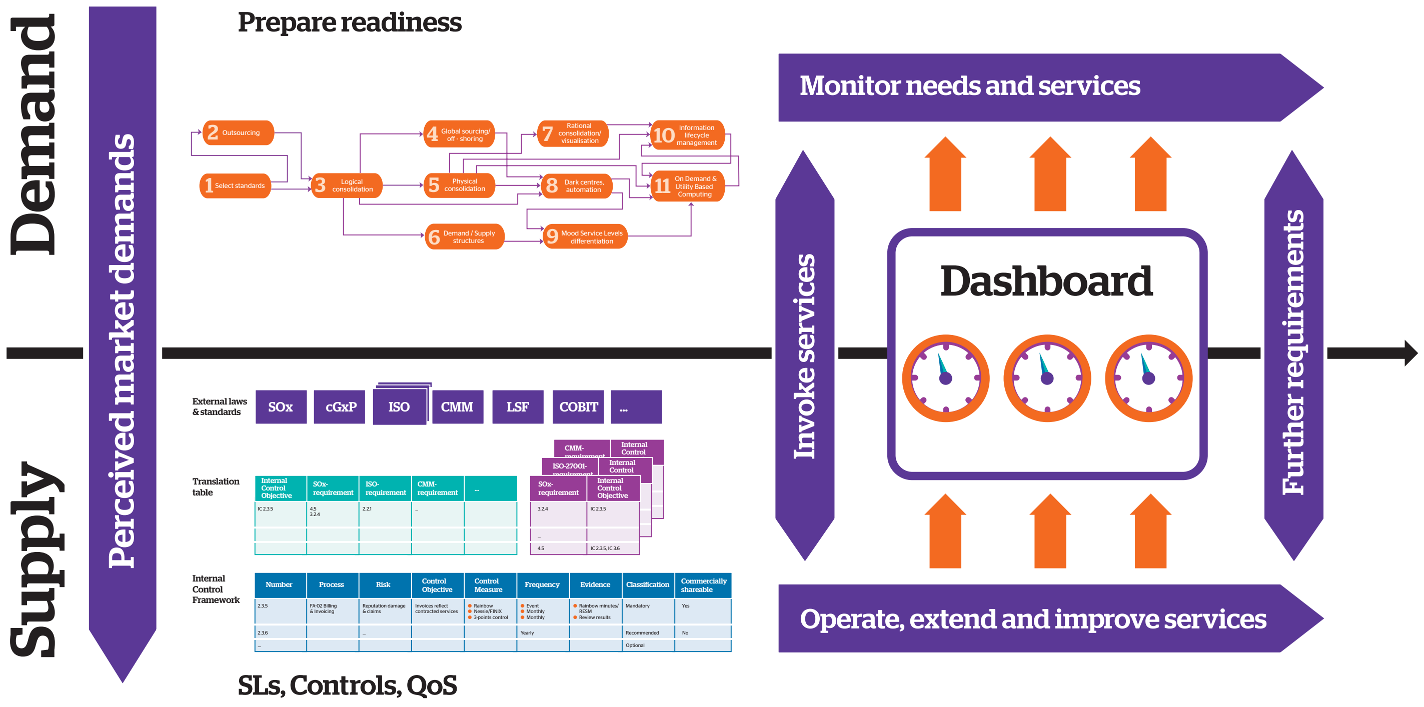
Trust needs to be ongoing, beyond the delivery contract: e.g. trust that data is deleted

Having multiple suppliers itself adds to trust: there is choice, given standards, interoperability and portability

The following diagram represents a conceptual overview of some of the activities and dynamics involved. It should be recognised that there is, as yet, no "script": this simply tries to capture some of the activities which could take place and identifies some of the issues arising.

Components of this approach are, from left to right and in approximate sequence:

- At the outset, the supplier(s) have to work from a perception of market demands, because in a cloud environment there are no "captive" customers to pre-define requirements
- On the Demand side, the organisation has to be set up to make use of virtualised services: this is more fully explained in the following Instruments section of this document
- On the supply side, not only do the services themselves need to be built, but the necessary control mechanisms to ensure their ongoing quality and sustainability: this is also described more fully elsewhere in this document
- Suppliers should adopt a principle of transparency: which regulations and standards are adopted, what framework has been assembled, how the controls are implemented and monitored, etc.
- The customer can then invoke the services: note that this is on an "as is" basis within a cloud environment
- The supplier operates the services, extends and enhances them
- The KPIs of that service delivery are made visible to the customer via some form of dashboard
- The customer continues to monitor and manage their evolving needs and how well they are being fulfilled by the services
- On a periodic basis, dialogue will take place on further service needs and possible enhancements, whether with specific customers or the market in general.


Demand
Supply
Perceived market demands
Prepare readiness
2 Outsourcing
1 Select standards
3 Logical consolidation
4 Global sourcing/ off - shoring
5 Physical consolidation
6 Demand / Supply structures
7 Rational consolidation/ visualisation
8 Dark centres, automation
9 Mood Service Levels differentiation
10 Information lifecycle management
11 On Demand & Utility Based Computing
External laws & standards
SOx
cGxP
ISO
CMM
LSF
COBIT
...
Translation table
CMM-requirement
Internal Control
ISO-27001-requirement
Internal Control
Internal Control Framework
SLs, Controls, QoS
Invoke services
Monitor needs and services
Dashboard
Further requirements
Operate, extend and improve services

Internal Control Objective	SOx-requirement	ISO-requirement	CMM-requirement	...
IC 2.3.5	4.5 3.2.4	2.2.1	...	

SOx-requirement	Internal Control Objective
3.2.4	IC 2.3.5
...	
4.5	IC 2.3.5, IC 3.6

Number	Process	Risk	Control Objective	Control Measure	Frequency	Evidence	Classification	Commercially shareable
2.3.5	FA-02 Billing & Invoicing	Reputation damage & claims	Invoices reflect contracted services	● Rainbow ● Nessie/FINIX ● 3-points control	● Event ● Monthly ● Monthly	● Rainbow minutes/ RESM ● Review results	Mandatory	Yes
2.3.6		...			Yearly		Recommended	No
...							Optional	

[57] Forrester report that over 90% of businesses with data resident in clouds use some form of encryption: PRISM's impact on the US cloud industry, February 2015

[58] Proof of Concept: Carbon Footprint and Energy Efficiency, Open Data Center Alliance, 2013: http://www.opendatacenteralliance.org/

Instruments

To prepare to use cloud services on the customer's side, Atos believes it is necessary to create a path towards a cloud-based IT services environment: a path that is likely to encompass change on the part of the customer, the supplier, and the relationship between them. One way of getting there is to adopt the equivalent of the peace process; see adjacent box.

The demand/supply relationship is complex in any organisation and changes to this relationship take time and require cooperation. For example, the traditional managed operations customer (the demand side) is the IT manager, and most IT managers measure their "empire" in terms of the number of boxes and people they manage. In an on-demand, outsourced or cloud-based environment, the IT manager may appear to have lost an empire (no boxes/people) but in fact plays a more vital role in determining requirements and liaising between business and technical experts. They show their real value, rather than having to act as a Unix system manager; use of cloud services requires a letting-go of many technological details.

The requirements for IT infrastructure services need to be defined as a set of results and conditions that move away from technical details and from a "my box" attitude to a more "our services" qualitative approach.

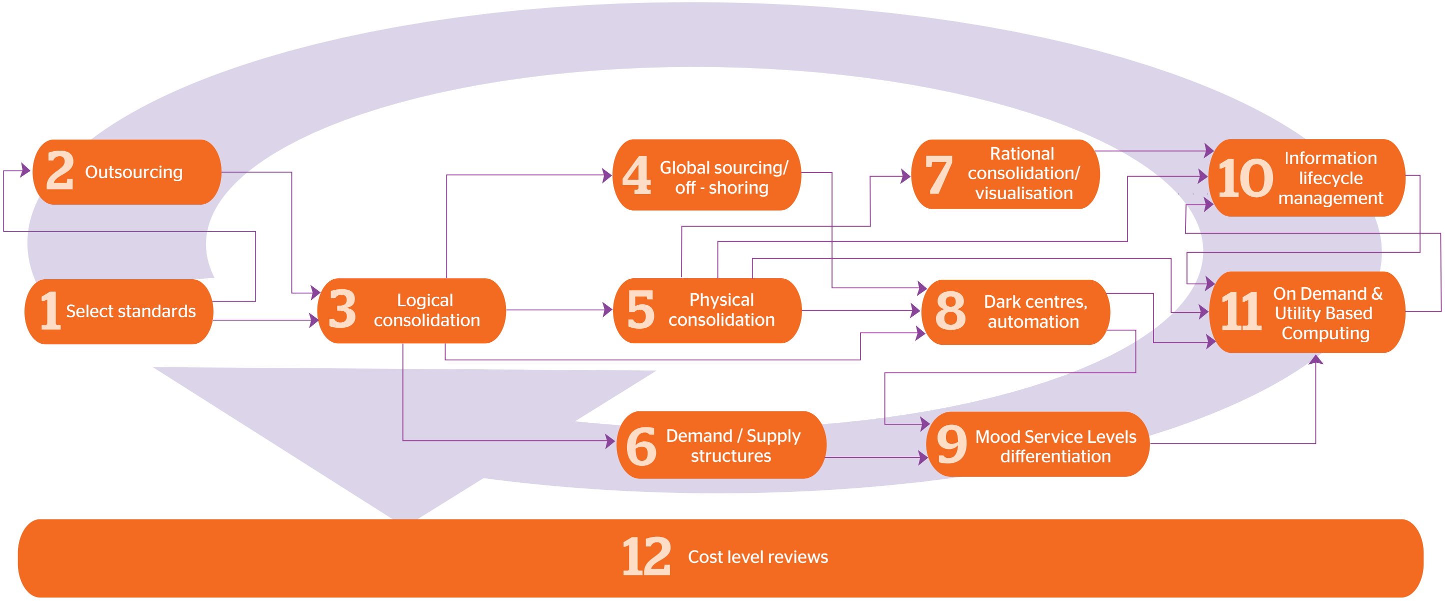
Even more reassuring, the steps are improvements to the way the IT infrastructure is deployed and managed, as well as being steps on the road towards utility computing. The process results in a rationalisation of the customer's IT environment as a whole.

That roadmap is the subject of the flow chart below, which depicts such a path as described for one particular customer. It needs to be interpreted in each case, but provides a set of ingredients and sample recipe that can be used to determine such a progression in whatever circumstances pertain to that particular customer.

The peace process

One analogy is the peace process, which has been applied with some success in Northern Ireland, but less so in the Middle East. Essentially, it is a way of getting two parties with opposing views and interests to move in a common direction, while neither fully trusts the other and no-one is sure exactly where they will end up.

Some steps in this path may not actually be clearly defined until they are well down the path, but importantly by following a set path they leave a 'trail' behind them and can feel that they are making progress together because they can see the tangible steps that they have trodden on the way. So, rather than concentrate on the goal, manage a process which moves in the right direction, and where each party can see that they are making general iterative progress.



2 Outsourcing
1 Select standards
3 Logical consolidation
4 Global sourcing/ off - shoring
5 Physical consolidation
6 Demand / Supply structures
7 Rational consolidation/ visualisation
8 Dark centres, automation
9 Mood Service Levels differentiation
10 Information lifecycle management
11 On Demand & Utility Based Computing
12 Cost level reviews

1. Standardise: choose platforms (vendor, models, OS), applications environment, service management tools, etc. Determine standards for each set/class of applications systems (e.g. SAP).

2. Ensure supply-side personnel within a business do not become an obstruction, e.g. transfer them to a supplier such as Atos, to overcome the "Turkeys and Christmas" syndrome: negotiating and implementing changes with the very staff who may feel themselves to be "victims" of that change.

3. Organise a single structured service delivery architecture, including catalogue of available services, common processes, service descriptions and levels, tooling interfaces, etc.

4. Consider an offshore component, which could be significant for mature environments, and is dependent on the systems' lifecycles. This needs to be carefully combined with standards and to allow room for possible subsequent automation.

5. Share facilities wherever they are not business-specific. Consolidate data centres into a common Tier 3 or 4 twin-centre structure, which may itself provide services to Tier 1 and 2 centres. Use common, virtualised DC-LAN and storage facilities, on an "on demand" basis, with centralised backup and recovery facilities. Networked storage allows more efficient utilisation and the implementation of different classes of service.

6. Determine a structure between the customer's businesses which coordinates their Demand functions, allowing maintenance of requirements for ongoing services, and attuned to a complementary Supply structure. Use governance to reduce the diversity of perceived business needs, adopting company-wide release management processes for common components.

7. Reduce the diversity of applications environments and run them in fewer, and shared, system platforms. Concentrate on standard Wintel and Lintel (Windows or Linux on Intel or AMD systems) environments. Use virtualisation facilities to allow the utilisation for suitable applications to be increased from the traditional below 30% to 80% or higher. Reduces the number of systems and thus some operations, hardware and software costs.

8. Run the resulting centres as fully-automated, "lights out" centres, with the services to deliver them being similarly automated. Use provisioning software to manage the environment on a utility-like basis, which can allow re-purposing of IT resources driven by business needs. Improve the support ratio from the traditional typical 1/15-30, depending on complexity, towards 1/50-60 or more, so halving relevant costs. Combining doubled utilisation with doubled support ratios gives a compound benefit on current costs for those elements.

9. Put in a simple, "managed operations on demand"-based service and contract structure, which allows transparency so that businesses can determine which of the rationalised service levels is appropriate for each of their systems.

10. Manage the management of data to reflect the business value of the information it contains, rather than one-size-fits-all and all data getting first-class service.

11. Deliver both storage and processing from a coherent utility environment, supplied, and preferably owned, by fewer preferred platform vendors.

12. Constantly check costs and adjust pricing levels to reflect efficiency improvements.

Asynchronous deployments

As described earlier, in these services the supply environment is pre-deployed: it was built to accommodate services to a number of, as yet undetermined, customers. But requirements and legislation may (will) develop over time, and new business sectors may be addressed for which the supplier may need to accommodate new requirements.

It is therefore necessary for the supplier to have a mechanism to keep the control maintained complete and up to date, and to inform existing customers of changes to the environment in which they have been running.

Trusting public clouds?

Is it possible to construct a mechanism whereby public clouds from outside Europe, which are not subject to European jurisdiction (e.g. from the big American players), can be trusted? The USA-Europe Safe Harbour[59] agreement is intended to ensure that there is a guarantee from the recipient government that if personal data is exported from the EU, it will still receive 'adequate' protection[60]. However, in light of revelations regarding the US NSA, doubts have been raised in Europe as to its effectiveness.

[59] http://www.export.gov/safeharbor/eu/eg_main_018365.asp

[60] See also: http://www.zdnet.com/article/safe-harbor-why-eu-data-needs-protecting-from-us-law/

Conclusions

Atos believes that Trusted European Cloud is achievable, but we first need consensus on what it means, and a plan for developing it.

Atos has played a leading role in discussions so far about the Trusted European Cloud, but the next steps need to be carefully coordinated by the EC towards the emergence of something identifiable as European Cloud Standard(s).

Moves so far have been more about information gathering than decision-making; but that process has been authoritative and of benefit to Europe as a whole.

Similarly, the EC has been sponsoring many relevant developments, such as those undertaken by Atos Research and Innovation (ARI), as described in an Appendix to this document.

Although the concept of cloud is relatively new, assurance of quality is well-established and it is proposed that the well-proven approach be adopted and adapted, and applied to the cloud environment.

In order to achieve success, it is needed not only to build facilities, but to try to understand why and how they might be taken up by potential customers, and then to act on that understanding. That is why a mutual roadmap is proposed: so that both sides of the supply chain can see their ways forward.

Standards are important in this field, because it is seen that success will only be achieved when customers feel that they have a real and equitable choice: several comparable cloud offerings are needed to be successful in giving customers that choice. That has been found and proven in the development of Helix Nebula, also described in an Appendix below, where Atos has cooperated with some of its competitors, on a limited basis: just enough to ensure that we deliver comparable and compatible services.

For the future, we have to deliver services which adhere to common standards, and even be portable to and from, our competitors; we have to do what they do, but just do it better. To misquote George Orwell[61], "all clouds are created equal, but some are more equal than others".

Atos firmly believes that if we successfully adopt this approach, many of us can be successful - it is not a 'zero sum game'[62] - and that, just as some places become tax havens, Europe can become the 'cloud haven' for the world.

About the author

Mick Symonds is Principal Solutions Architect for Atos, based in The Netherlands.

He has worked in the IT services business for over 30 years and has held a wide range of roles, from technician to marketing, from general management to consulting. A particular focus has been on the ongoing management of IT infrastructure services and their development.

He has been responsible for the development of Atos' global data centre and cloud strategies, and as a by-product has produced comprehensive White Papers on these and other subjects, downloadable from the Atos web site.

Most of his time recently has been devoted to the development of Helix Nebula (http://www.helix-nebula.eu/), an emerging European initiative to deliver federated cloud services to public organisations, starting with the scientific research community.

Thanks are due to colleagues who have supported and contributed to the production of this document, including Hubert Tardieu, Kay Hooghoudt, Aljosa Pasic, Michel van Adrichem, Johan Louter, Jordan Janeczko, Colleen Hawthorne, and Marianne Hewlett.

Mick can be contacted at michael.symonds@atos.net.

[61] "All animals are equal, but some animals are more equal than others", George Orwell, Animal Farm

[62] https://en.wikipedia.org/wiki/Zero-sum_game

Appendix A: Helix Nebula

The Helix Nebula initiative[63] was established in 2011, to build a federated, multi-supplier cloud for (initially) European research organisations.

It was initiated by three of the largest and most sophisticated European research organisations:

- CERN: with their Large Hadron Collider, having massive data processing needs;
- EMBL: doing genomic analysis, with large quantities of data processing and added data protection implications;
- ESA: generators of large quantities of Open Data from space and earth observations, but needing a means to deliver it.

Helix Nebula was intended both to fulfil their requirement for European and European-oriented cloud services, and also to provide degrees of assurance regarding the quality and security of those services.

The service was built in collaboration with a number of competing suppliers, supported by the EC with some funding via an FP7 project.

The objectives of Helix Nebula define the vision of an industrial strategy for a federated cloud framework to be implemented by 2020. The main Helix Nebula goals to reach this vision are:

- Establish a Cloud Computing Infrastructure for the European Research Area and the Space Agencies, serving as a platform for innovation and evolution of the overall federated cloud framework.
- Identify and adopt suitable policies for trust, security and privacy on a European level.
- Create a lightweight governance structure that involves all the stakeholders and can evolve over time as the infrastructure, services and user-base grow.
- Define a funding scheme involving all the stakeholder groups (service suppliers, users, EC and national funding agencies) into a Public-Private-Partnership model that delivers a sustainable and profitable business environment adhering to European-level policies.

The main properties Helix Nebula aims at exhibiting are:

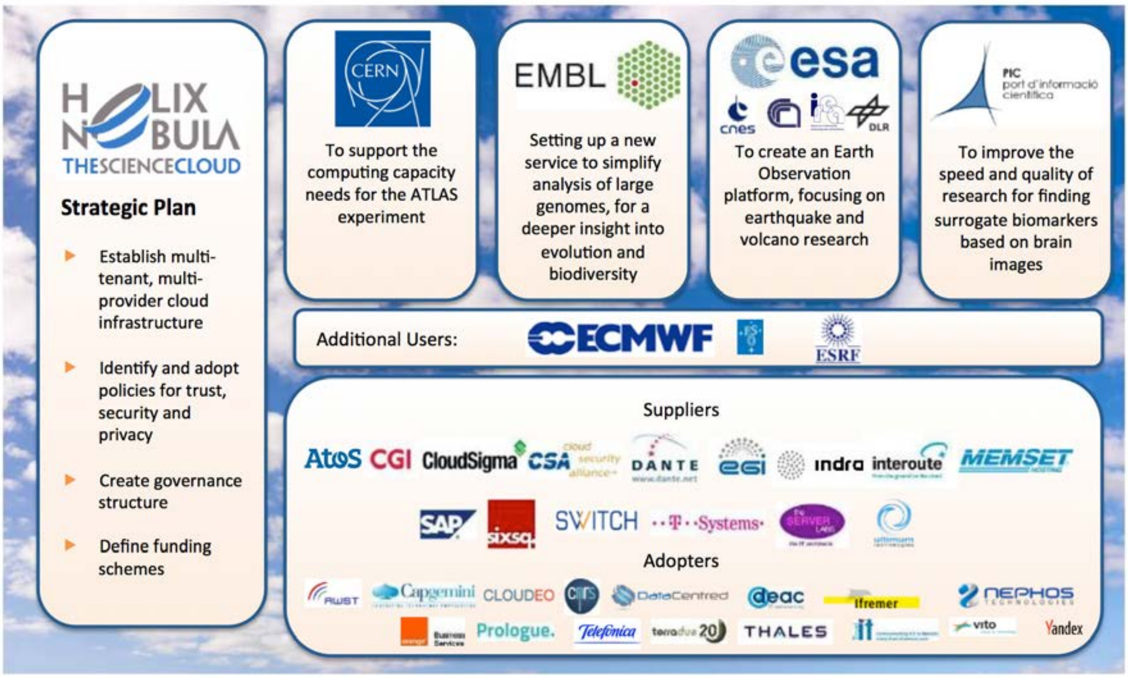
- Multi-demand
- Multi-supply
- Easy selection between providers
- Faster response to stakeholders' needs

These properties define overall a trusted domain with transparency for invoicing and other accounting over cloud resources provisioning, so consumers using the European Cloud Computing Infrastructure are not entering a vendor lock-in situation.

In recent months, some of the key suppliers have taken steps to deploy a Helix Nebula Marketplace[64] (HNX), whereby users can use a common interface to select and deploy services between and across a range of cloud providers, offering competing (and competitive) services, all coordinated and supported by a common front end. The service now consists of:

- a common market place operator and support organisation: SixSq
- four cloud IaaS platforms, totalling around 20,000 cores, from: Atos, CloudSigma, Interoute and T-Systems.

Atos recently passed a significant milestone with CERN going into production using 2,000 VMs, running in our environment in Spain, and seeking yet more capacity.



Strategic Plan

- Establish multi-tenant, multi-provider cloud infrastructure
- Identify and adopt policies for trust, security and privacy
- Create governance structure
- Define funding schemes

To support the computing capacity needs for the ATLAS experiment

Setting up a new service to simplify analysis of large genomes, for a deeper insight into evolution and biodiversity

To create an Earth Observation platform, focusing on earthquake and volcano research

To improve the speed and quality of research for finding surrogate biomarkers based on brain images

Additional Users:

Suppliers

Adopters

[63] http://www.helix-nebula.eu?

[64] http://hnx.helix-nebula.eu/index.html

Appendix B: ARI research

Atos Research & Innovation (ARI) is the R&D hub for emerging technologies and a key reference for the whole Atos group. With more than 28 years of experience in running Research, Development and Innovation (RDI) projects, ARI has become a well-known player in the EU context. Its multi-disciplinary and multicultural team has the skills to cover all the activities needed to run projects successfully, from scientific leadership to partnership coordination, from development of emerging technologies to the exploitation of project outcomes, with a strong focus on dissemination, innovation adoption and commercialization.

ARI has run a number of projects that contribute to the concept of Trusted European Cloud. They have run many projects, many supported by funding from the EC, that span security, privacy and cloud, with ongoing projects like Cumulus, Coco-Cloud, witdom, Tredisec, HC@works, Strategic, Wiser, Slalom, and the older ones like optimis or VPHShare.

Cloud4SOA offers a rating service that enables Cloud Users to evaluate their user experience while they adopt a cloud solution. It also offers a system automatic rating (based on SLA and QoS violations) that contributes to improve the User Trust. Such information is used to rank, (or even exclude) from the list of the best-fit cloud offering (proposed to application developers) provided by the matchmaking service. The solution is now offered through

http://www.opencloudpier.org/

OPTIMIS project produced a toolkit enabling secure, risk-aware and compliant cloud application construction & life-cycle management. OPTIMIS toolkit is a platform architecture enabling multi-cloud optimization based on trust, risk, eco-efficiency and cost (TREC). OPTIMIS cloud broker establishes a virtual private network overlay among the virtual machines of each multi-cloud application deployment, and a shared virtual data space that aggregates data elements among all parts of the application deployment across multiple clouds. Toolkit is available at

http://optimistoolkit.com/

CIRRUS project delivered recommendations on cloud security standards, certification schemes , as well as international cooperation. In addition a CEN workshop agreement on cloud security assurance has been launched, with an eye on future cloud trends and models. CIRRUS Green paper is used as the input to several EU trusted cloud initiatives:

http://www.cirrus-project.eu/

SLALOM project builds on the findings of the ECP's C-SIG on SLAs and on the Expert group on cloud computing contracts, as well as the ISO SC38 group on SLA standards. SLALOM will go one step further by codifying these recommendations into legal text as a standard, modular SLA and Contract template, allowing adopters to compare providers on the key metrics, without uncertainty over the rights conferred in the "small print".

CUMULUS collects multiple types of evidence regarding security, including service testing and monitoring data and trusted computing proof. It has models for hybrid, incremental and multilayer security certification with different levels of automation in the certification process steps.

http://www.cumulus-project.eu/

Coco-Cloud project is delivering machine readable data sharing agreement (DSA) that can define how user data is used, for which purpose and in which context. The main achievement is, however, the automated enforcement of these agreements in the cloud, as well as the contribution to automated evidence-based audits of privacy policies. http://www.coco-cloud.eu/

WITDOM project aims at protecting sensitive data in cloud cryptographically, by applying the privacy-by-design paradigms. WITDOM's data protection methods will be tailored to the risks associated with different classes of data.

http://www.witdom.eu/

There are more such projects due to start in 2015: e.g. Tredisec, Wiser, ...

About Atos

Atos SE (Societas Europaea) is a leader in digital services with 2013 pro forma annual revenue of €10 billion and 86,000 employees in 66 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media & Utilities, Public Sector, Retail, Telecommunications and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, and Worldline.

For more information:

Please visit **atos.net**