

The Supply Chain Cloud

YOUR GUIDE TO
CONTRACTS STANDARDS SOLUTIONS



cloud
application

The background of the lower half of the image is a dark, textured surface covered with faint, glowing blue and white hexadecimal code (A-Z, 0-9). The words "cloud" and "application" are prominently displayed in a large, bold, blue, sans-serif font, with "cloud" on the top line and "application" on the bottom line. The letters have a slight 3D effect and are semi-transparent, allowing the background code to be visible through them.

www.thesupplychaincloud.com



EUROPEAN COMMISSION	PAGE
Unleashing the Potential of Cloud Computing	4



TRADE TECH	
Cloud Solutions for Trade Security Implications for the Overall Supply Chain	7



CLOUD SECURITY ALLIANCE	
Cloud Computing: It's a Matter of Transparency and Education	10



FRAUNHOFER INSTITUTE	
The Logistics Mall – Cloud Computing for Logistics	12

I'm testing some flip books now.



AXIT AG	
Supply Chain Management at the Push of a Button	17



INTEGRATION POINT	
Global Trade Management and the Cloud – Does It Work?	18



THE OPEN GROUP	
Cloud Computing Open Standards	20



WORKBOOKS	
CRM As A Service for Supply Chain Management	24



GREENCLOUD	
Sustainability in the Data Supply Chain	26



CLOUD INDUSTRY FORUM	
Why the need for recognised Cloud certification?	31



COVISINT	
Moving to the Cloud	32



CLOUD STANDARDS CUSTOMER COUNCIL	
Applications in the Cloud – Adopt, Migrate, or Build?	38



FABASOFT	
“United Clouds of Europe” for the Supply Chain Industry	42



EUROCLOUD	
How Cloud Computing will Revolutionise the European Economy	45



BP DELIVERY	
The cloud value chain needs services brokers	48

Unleashing the Potential of Cloud Computing

Cloud computing can bring significant advantages to citizens, businesses, public administrations and other organisations in Europe. It allows cost savings, efficiency boosts, user-friendliness and accelerated innovation. However, today cloud computing benefits cannot be fully exploited, given a number of uncertainties and challenges that the use of cloud computing services brings.

In September 2012, the European Commission announced its *Cloud Computing Strategy*, a new strategy to boost European business and government productivity via cloud computing. The overall goal is to speed up and increase the use of cloud computing across the economy, to stimulate the uptake of cloud computing to the benefit of customers and suppliers alike, by making Europe not only cloud-friendly, but also cloud active. The Strategy took shape after thorough analysis of the overall policy, regulatory and technology landscapes in Europe.

So, what is the Commission doing to boost cloud computing?

Cutting Through The Jungle of Standards

The cloud market sees a number of standards, covering different aspects and suggesting different solutions to common problems. The European Commission aims at more transparency in the cloud market so as to help cloud customers understand what cloud computing standards exist and should be used by them. The Commission works together with relevant stakeholders to ensure all specific expertise is taken into consideration. To this end, the *Commission tasked the European Telecommunications Standards Institute (ETSI)* with identifying the necessary standards for security, interoperability, data portability and reversibility by 2013. With stakeholders' participation, ETSI completed its Cloud Standards Coordination (CSC) initiative in December 2013 and delivered a **mapping of existing cloud computing standards**¹.



¹http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

²<https://resilience.enisa.europa.eu/cloud-computing-certification>



Moreover, the Commission has been working with the *European Union Network and Information Security Agency (ENISA)* and other relevant bodies to assist in the identification of EU-wide voluntary certification schemes for cloud computing (including data protection) and establish a list of such schemes in 2014.

Cooperation with industry and ENISA resulted in the publication of a validated list of cloud computing relevant network and information security certification schemes in February 2014.² Certification schemes are the requirements, procedures and

means available for obtaining a certificate; certification can be used to provide assurance that a business complies with a certain standard. On-going work with the support of ENISA will further enhance the usability of this list of certification schemes by the end of 2014. New certification schemes will be added to the list and ENISA will enhance the functionality that will allow cloud computing customers to compare certification schemes and cloud computing services offerings.

Safe and Fair Contract Terms and Conditions

The Strategy called for action not only at the level of consumers and small firms, who get take-it-or-leave-it contracts, but also at the level of Service Level Agreements (SLAs) between professional users.

The Commission set up an expert group to work on model contract terms and conditions for cloud services for consumers and small firms; these models are expected by the end of summer 2014. This group will also identify and disseminate best practices on model contract terms between consumers and cloud providers.

Moreover, the *Cloud Select Industry Group (C-SIG)* is working towards delivering guidelines defining standard options for SLAs (expected before the summer of 2014) and towards a **Data Protection Code of Conduct for cloud service providers** to support a uniform application of data protection rules throughout the EU and to build trust and confidence in cloud computing. The Code was created to assist prospective customers of CSPs to evaluate and to help businesses comply with the data protection legal framework.





The European Cloud Partnership (ECP)

This initiative brings together industry experts and public sector users to work on common procurement requirements for cloud computing. In March 2014, *the ECP Steering Board presented its vision for a 'Trusted Cloud Europe'*, aiming at supporting a single market for cloud computing in Europe based on a common understanding about best practices. The Commission now seeks views on this vision, which could be used to create a cloud we can all trust in Europe. The public survey asking for these views is open until 2 May 2014 at <https://ec.europa.eu/digital-agenda/trusted-cloud-europe-survey>.



Cloud Solutions for Trade Security Implications for the Overall Supply Chain

It is a rare occasion in supply chain management that a failure to administer the supply chain process could result in a year in jail with hard labor or a \$5000 penalty. Measuring or comparing the value of enhanced supply chain solutions remains, at best theoretical since hard quantitative comparative data is rarely available. So looking at trade security is a nice environment in which to look at the potential for cloud based supply chain technology solutions and their implications for management of a global supply chain and to compare it with current industry norms.

Background

The United States implemented 24 Hour Security Rule a year after the 9/11 terrorist attacks in New York. Canada and Mexico followed a few years later and Japan implemented their version of the rule on March 1, 2014. Both the vessel operating carriers and the NVOCC / Forwarders are required to transmit the data on their bills of lading to the respective Customs organizations 24 Hours before the cargo loads on the vessel. That means that data at the origin has to be made available for review at destination before it can load it and then be visible in route. It is a classic supply chain management scenario but with security rather than economic consequences.

The ocean carriers and the NVOCC / Forwarders have, for the most part, deployed different solutions. The carriers with their larger, more established networks, have relied on their distributed server systems to comply with the regulations. The NVOCC / Forwarders being by and large smaller and less centralized, have relied on Cloud Based solutions. And, 13% of the Japan market, has opted for sending their documents in hard copy to their offices or agents in Japan where they are manually re-keyed into a system with local access to Japan Customs' system.

Distributed server systems are a system solution designed prior to the development of almost free global telecommunications available on the Internet. Distributed server systems are a set of regional mainframe servers that collect information locally or within a limited geographic region and then transmit via EDI batches of data to the mainframe server located at the shipper's destination.

Cloud based solutions use a single server located at a major telecommunications center and rely on the Internet and browser based technology to have all the users work on the same central system the same way that you shop online or book hotel and travel arrangements today.

The Japan Experiment

Japan's 24 Hour Rule went live on March 1 and both the ocean carriers and the NVOCC / Forwarders were able to achieve the basic requirement of transmitting their data to Japan Customs

on time. However, the differences between the two approaches started to become clear 45 days into the new regulatory situation when Japan Customs expressed its frustration with the quality of the data and asked the Trade to clean it up. Japan Customs, like so many importers and exporters, realized quickly that poor data consistency destroys their efforts to do sophisticated supply chain management. You simply can not do valuable analytics on inconsistent data.

The first, and biggest, issue points to one of the biggest limitations of the distributed server solution. Japan Customs requires that the ocean carriers and NVOCC / Forwarders clean up any data discrepancies and achieve a link between the data for both the ocean carriers' and NVOCC / Forwarder's bill of lading. The NVOCC / Forwarders are able to see from anywhere in the world the status of their bill of lading with Japan Customs in real time by directly triggering an amendment to the filing. The ocean carriers outside of Japan can not see the status in real time because the server they are working on capture the amendment changes, hold them for a period of time, then batch transmit them to the server in Japan, which in turn transmits to Japan Customs but doesn't send the status reply back to the originating server.

The consequence is that the users at origin shipping with the carrier can not resolve issues with well meaning users at the ocean carriers because the ocean carriers' simply can not see statuses in real time because they are not working on the server that got the response from Japan Customs.

This single directional flow of data is typical of systems deployed at all levels of the trade today. Rekeying of data at destination is also commonplace in international trade. Both don't allow for the easy correction of errors or adjustments to changes in situation.

The Cloud Based solution allows users from anywhere in the world to execute changes and to get immediate feedback from servers and users located elsewhere in the world. It also allows other users, with the appropriate permissions, to see and work with, or collaborate with, other users located along the supply chain.

Cloud Computing: It's a matter of transparency and education

By: *Daniele Catteddu*,
Managing Director EMEA, Cloud Security Alliance

Cloud computing is becoming a mature business model and many companies and governments around the globe are implementing strategies to embrace cloud services. Examples of National and Regional efforts can be found in USA, Europe, Japan, China, Singapore, Taiwan, Thailand and many others. In the private sector there is growing adoption of cloud services by large banks, manufacturers, healthcare organizations and other large corporations and small and medium businesses.

Despite the simplicity of the idea of ICT services offered as utility, on demand and pay-as-you-go, the cloud computing model is based on a complex chain of interactions between multiple parties which operate in different countries and legal jurisdictions. The complexity and opacity that sometimes characterize this cloud "supply-chain" have generated some barriers to faster adoption of cloud computing. Among the most important of these barriers are:

- » The lack of clarity around the definition and attribution of responsibilities and liabilities, the difficulties
- » Achieving accountability across the cloud supply chain, the incoherent global (and even sometimes regional and national) legal framework and compliance regimes
- » The lack of transparency of some service providers or brokers, particularly around security and risk management
- » The difficulties in performing internal and external due diligence
- » Lack of clarity in Service Level Agreements
- » Lack of interoperability.
- » Lack of awareness and expertise.

A key underlying theme in all these is the need for assurance and trust between cloud providers and customers.

But barriers can be removed and the main objectives governments, cloud service providers and cloud customers should be working towards are to increase the level of trust in the market.

To this end, the definition of security control and certification frameworks, SLAs, standardised contractual terms, and the use of continuous monitoring are key means to provide more transparency and control to the cloud customer. The European Commission strategy for cloud computing, for instance, is based on three main pillars:

- 1) The identification of suitable standards and certification schemes
- 2) The definition of model terms for service level agreements and contractual terms and conditions
- 3) Definition of common requirements in public sector organization and use of public procurement as a market quality stimulus.

Similar approaches are currently being adopted in the US and the APAC region. Cloud providers are striving to become more transparent, especially when it comes to security and privacy. **The Cloud Security Alliance (CSA) STAR**, a voluntary registry where cloud providers can publish the results of a self assessment against the CSA best practices, is a clear example of cloud providers' willingness to maintain the trusted relationship they have with existing customers and to provide assurance to potential new ones that their service will be sufficiently secure. Assurance is provided by telling customers which are the security controls and measures in place to manage risks to their infrastructures, services and data.

The objective is put the customer in a position to compare competing offerings against their requirements, to make informed decisions when choosing the service they need and to be able verify, during the service delivery phase, if reality matches what was promised.

These are certainly steps in the right direction and point to the creation of a market where security is a market differentiator, where transparency is the general rule and obscurity the exception. Cloud solution providers have business incentives to be transparent, to share information with regulators, enforcement authorities and current and potential users about their security practices, about the security incident that might occur, etc. The most obvious business incentive is based on the simple logic that the customer are more likely to buy services only from those providers which provide enough information to effectively manage their risks. In this respect, the example of an incident management process is very illustrative, in fact a cloud customer necessarily needs information and co-operation from the cloud provider to be able to manage an incident properly.

Policy makers, as we noted earlier, are playing their part by introducing a number of "soft" policy measures, as well as new binding rules on transparency and accountability. We have also noted the proactive approach of some cloud solution providers who are voluntarily sharing relevant information with the general public. What is still missing, perhaps surprisingly, is a more active role of customers.

CSA's recent survey of the cloud market, conducted jointly with ISACA¹, showed up a clear division between enthusiastic early adopters and cloud-sceptics. Between these extremes, a substantial body of potential users are still undecided about whether to trust the cloud or are even un-aware of cloud computing, its benefits and its risks. Therefore one of the biggest opportunities that we, as members of the ICT and cloud community must seize is to educate potential users on the business value of cloud services. At the same time we must promote awareness of potential risks, and how to address them when procuring cloud services – a key point here being the responsibility which the customer holds for performing due-diligence and maintaining compliance when migrating to cloud services. Beyond initial procurement and due-diligence, it is important to stress the fundamental importance of ensuring clear commitments through Service Level Agreements and continuous monitoring of their fulfilment.



About Cloud Security Alliance

Cloud Security Alliance is a not-for-profit organization focusing on best practices, standards and education in cloud computing security.

CSA's activities include awareness and educational campaigns, conferences, seminars, summer schools, webinars, educational papers, guidelines for companies and government, and finally training and professional certification through CCSK: Certificate of Cloud Security Knowledge, the only professional certification related to security knowledge of cloud computing (CCSK).. We see this as a means to raise the bar in security best practice and the quality of cloud services from a security perspective by filling the gaps in transparency, understanding and skillsets across the market. This is particularly important in the Middle East areas, where surveys and analysis show that, despite a growing interest in cloud computing, there is still low level of adoption and a significant awareness gap, which needs to be filled with advanced cloud-knowledge.

¹<https://cloudsecurityalliance.org/csa-news/cloud-maturity-study-reveals-top-issues/>

The Logistics Mall

– Cloud Computing for Logistics

Motivation

The Logistics is a highly globalized branch with the influence by frequent changes of business standards as well as global movements. In Germany, as well as in the European Union, the logistics sector is one of the major economic factors. The importance of logistics is based on stable figures and an expected future growth throughout the European Union and worldwide markets.

While in the past the logistic sector was defined as simply focused on the transport, the modern definition goes way further. The Logistics does not only include the transport of goods throughout the country or globe, but combines all services and tasks dealing with the (traditional) transport of goods and the management of transportation. Concluding this, the logistic is combining the transport with other services such as optimizing (e.g. packaging), management (e.g. warehouse management) and controlling of logistic processes.

Furthermore, the customers of logistic companies focus on efficiency and expect a well organized but fair priced service by the logistics company. On top of the mentioned exceptions the logistic service-provider often has to realize individual process chains to allow dealing with the problems containing the transportation contract. Another problem is based on the short contracts between the service-provider and the customer, which often reduce the flexibility of individual software solutions. To maintain the flexibility of individual software solutions is mostly a high-pricing solution needed and can only be established after a certain time period. On the other hand the logistics-customers asking for short-term contracts to remain flexible to service agreements or fast market changes. Therefore the complexity of logistics services rises and the IT-systems need to find solutions to cover the new requirements. Consequently both, the industry and the technological challenge of logistic services seem to be exemplary fields of application for solutions on the basis of the internet and cloud computing.

Based on the above mentioned experience the Logistics Mall was designed and developed. The Logistics Mall is a market place for the Logistics branch and is designed for the cloud computing technology. The research project Logistics Mall was launched in 2010 and is in progress until end of year 2013. The project Logistics Mall is realized by two Fraunhofer Institutes situated in Dortmund and their industrial partners. The first Fraunhofer Institute is the Fraunhofer Institute for Material Flow and

Logistics IML, with great knowledge about logistics and logistics software. The second institute is known as the Fraunhofer Institute for Software and Systems Engineering, with advanced knowledge in Software Engineering. The cooperation between both Associations is better known as the innovation cluster “Cloud Computing for Logistics”. The industrial partner involved in the research of the Logistics Mall is the Logata GmbH based in Bocholt, Germany. The launch, support and operative service are organized by the industrial partner.

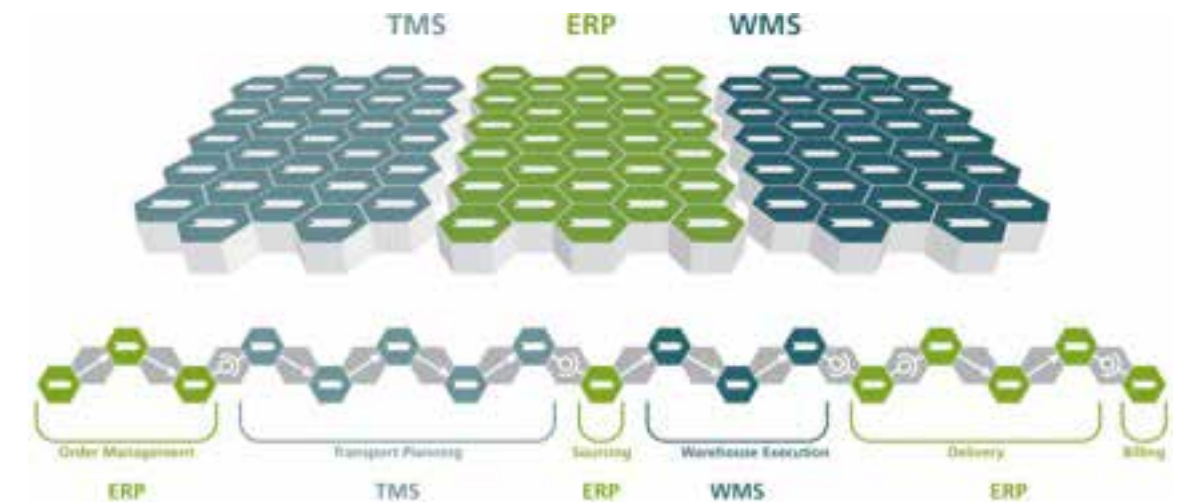
Logistics Mall

The Logistics Mall is divided into two separate pillars, which represent the main functionality of the cloud computing infrastructure. The first pillar represents the Mall Market Place (MMP). This market place offers, similar to other online shops, all available products and allows the purchase of software-bundles, individual applications or logistics services. Furthermore, the mall marketplace is open for every qualified software developer and logistic service-provider as long as the application is applicable to the cloud structure for the logistics mall.

In addition to the MMP, the Customer Access Framework (CAF) represents the second pillar of the logistics mall. This CAF manages the applications for a single customer (company) and deploys the software-services to all qualified company clients. Based on that, a customer access framework runs only for a single customer. This structure realizes the privacy of all customers and allows individual services for each client. To run the booked software-services the client simply has to log into the CAF by using a web browser.

While in traditional software solutions, the simultaneous use of different applications is the general procedure to join various applications to one workflow (see Graph 1), the cloud computing based Logistics Mall enables a different way to use. In fact, the Logistics Mall joins different applications in one workflow and allows the usage without boundaries. The mentioned workflow allows the use of various Logistics Mall apps in one view. For example a combined process between warehouse management systems and ERP-System can be used as one Service and without changing the application. The idea of the Logistics Mall – Process is to allow the integration of all required apps within the process-chains.

Summarizing the idea, the process chain can combine and connect different modules to a single workflow. This research project presents a, flexible and easy to adapt, possibility to resolve the problem of a fast moving branch such as Logistics.

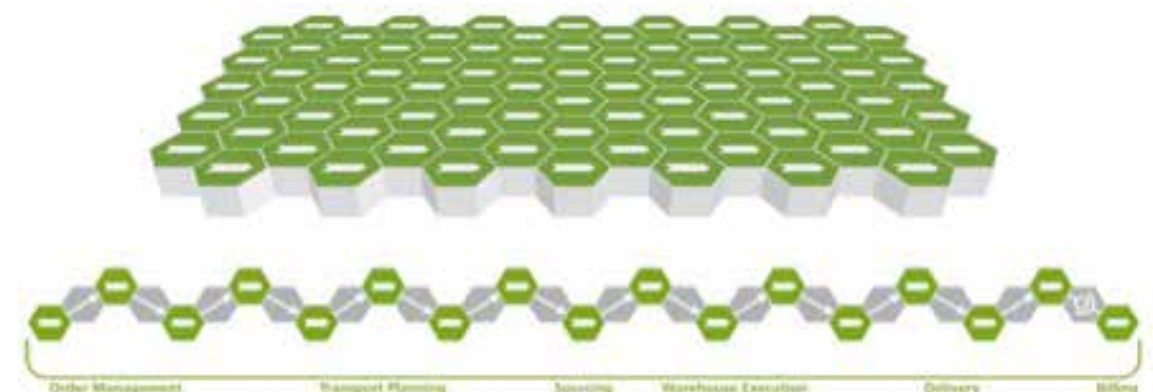


Graphic 1: The graphic shows a traditional workflow based on a number of traditional software solutions. The system structure presents different and individual applications which need interfaces to communicate throughout the whole workflow (and boundaries).

Besides of the mentioned workflow there are some other advantages for the use of cloud computing solutions like the Logistics Mall. One other advantage is based on the simple access on booked application (shortly: apps) published on the Logistics Mall. The only requirement existing to any device, communicating with the Logistics Mall, is the network-accessibility to enter the websites. Afterwards most Logistics Mall apps can be used on the device. In fact, the usage of cloud computing software-applications are not fixed on a specific hardware, or to a specific position, so that the software can be run worldwide and on nearly any device, such as tablets, computers or smartphones.

Another important difference towards traditional software solutions is that software-applications can be booked as a service, also known as Software-as-a-Service (SaaS), and will

be delivered under the agreed conditions. While in traditional software distribution the software packages need to be purchased and installed into the system hardware, the modern cloud computing solutions such as the Logistics Mall can be easily adjusted into new situations. This concludes that the spending of logistics software, especially the purchase of licences for big solutions, is dropping. Furthermore, the logistics company can react flexible onto market shifts and modify the booked software-bundles onto the actual situation or future growth expectancies. The mentioned way of software purchases over the Logistics Mall Market Place mostly not include any licences. This reduces the one time spent for expensive software licenses or high investments into new IT-Structure. Especially most small and medium enterprises can optimize their investment into the IT-Infrastructure by using the Logistics Mall to configure individual software solutions adapting their workflow.

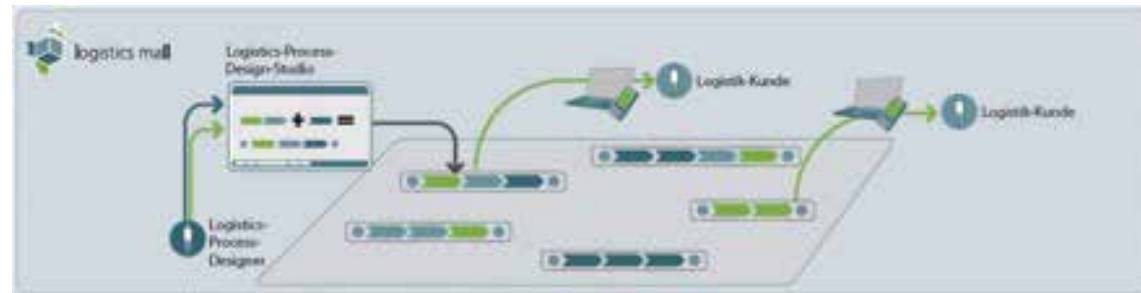


Graphic 2: The graphic shows the new workflow realized by the Logistics Mall in fact to realize supply chain wide access to all booked Logistics Mall apps

The Logistic Mall is divided into three different groups of clients which represent the various ways to interact with the service. The first group is representing the application developer. The software-applications offered on the Mall Market Place are developed by software companies and need to be adapted to the Logistics Mall infrastructure. Finally, it's necessary to adapt the software to the cloud computing infrastructure and the given standards. In fact, the software-developer needs the general

information about the interfaces as well as the basic structure of the Logistics Mall to prepare the application for the Logistics Mall. Before the application is added to the Mall Market Place and available to the customers, the application needs to be certified to the logistics mall cloud standard. This is done by the Administration board of the Logistics Mall. The number of different applications enables a wide variety of providers and applications to fulfil most customer needs.

The second group interacting with the Logistics Mall is named Logistics Process Designer (LPD). The LPD creates the individual process chains for companies to use the booked applications throughout the cloud solution. The Logistics Process Designer is organizing the workflow by simply adding the purchased service-options to a combined workflow (see Graphic 3). This is realized by logistics experts and does not require any deep technical knowledge.



Graphic 3: The graphic presents the basic functionality of the Logistics Process Designer.

Logistics Mall in Practice

In this chapter two examples of the Logistics Mall usage are described and the characterised companies exist, but stay anonymous related to privacy issues. The first practical example is fully organized by the Logistics Mall. The company is a German corporation which business idea is to develop an online shop for pharmacies, health care and wellness equipment. The company started some years ago with regional delivery only. But shortly after introducing the local delivery the company started expanding quickly. For that reason the manual computer administration, transport organization, as well as the manually handled stock-holding were too inefficient. On the other hand a big investment into good and long lasting software was impossible. That is why the idea of renting software licenses or using software on demand was actually the perfect way to invest in a highly organized and automated expansion.

Like mentioned before, the whole IT-Infrastructure is now based on the logistics mall. The booked software-modules, simply known as applications, are running on the Logistics Mall and can be accessed from (nearly) any device. Additionally, a big advantage lays in the very flexible and individual service agreement, meaning the company can easily expand their capacities for new orders or add a new application to defeat new challenges. Furthermore, most cloud computing applications can be booked through pay-per-use – contracts which allow the company, and other small and medium sized companies, the flexibility to fit the software-solutions for actual growth. Mostly, a full license for a software-solution is too expensive for a young company and cannot be adapted to the future use. Summarizing the IT-Infrastructure of the characterised company, the whole business administration is organized via the Logistics Mall starts with the order management and finalizing the administrative operations with the billing. The full integration into the Logistics Mall is offering especially start-up companies an easy access to quality software solutions.

Lastly, the third group defines the service-consumer such as logistic enterprises. This group purchases the necessary application over the MMP and consumes the applications over the World Wide Web infrastructure – as soon as the services are set up and ready to use.

an existing infrastructure. This is described by another company, a logistics service provider located in North-Rhine Westphalia. While the above mentioned way of use pictures a full integration of business processes into the Logistics Mall, this example describes a combined use of cloud computing applications and traditional software-solutions to resolve the company's workflow. This IT-Infrastructure can be characterized by using a traditional ERP-System offline on any client, in combination with a cloud computing based warehouse management system. This can be necessary if a company or bank relies on the customer data which cannot be easily transferred to the cloud solution. Another factor could be the local law, which might forbid transferring all data into the cloud based system. On the other hand, the use of modern software solutions can be interesting, even in the above mentioned situation, because a cloud-based warehouse management system can combine the positive aspects of availability and flexibility of the traditional offline system. The combined way of traditional software solutions and the Logistics Mall allows companies to extend their portfolio of software solutions, without moving all data into the Logistics Mall.

Summary

The use of cloud computing systems in the Logistics Branch is a chance to increase the flexibility, as well as the efficiency. Especially the logistics mall and its partners allow successful business services for companies with individual workflows and special needs. To apply to the logistics mall – or simply find out more, you can find the address below.

References

Logistics Mall: www.logistics-mall.com
 Logistics Mall Research Project: www.logistics-mall.de
 Innovation Cluster Cloud Computing for Logistics:
www.ccl.fraunhofer.de
 Logata: www.logata.com



Supply Chain Management at the Push of a Button – with the Logistics Platform AX4

Global economy becomes more volatile and the pace that logistics is required to keep is increasing. Businesses are continuously optimizing their processes in order to remain competitive. Life cycles of business models and strategies in industry and trade last for an average of two to three years. Logistics needs to adapt to this quickly and flexibly in order to be able to offer process support for their customers in turn.

Speed in implementing or adjusting processes must not be delayed by IT but must be accelerated by IT. However, previous systems like ERP or forwarding software have long since reached their limits when it comes to continuous management of transport chains: with a lot of parties involved and various systems.

AXIT AG's logistics platform AX4 offers cloud-based, cross-company SCM IT solutions which can be used from any point in the world, by every company along the delivery chain without having to interfere with their own existing IT landscape. AX4 integrates flexibly with the existing inhouse systems and offers seamless workflows and solutions exactly where the functions of said inhouse systems end. Here the focus lies on supply chain execution: From ordering goods up to the delivery all necessary processes can be mapped. Orders and required documents are being managed, tracking data is processed and

compared with previously calculated milestones and reports and freight charge calculations are run.

The goal of AX4 is to allow for collaboration between the various parties involved and to ensure continuous transparency of physical and informational flows. All parties involved can obtain the information which is required for them in real time – that is SCM at the push of a button. Solutions like the ones offered by AX4 allow for simple management of shipment data just as for the controlling of complex, global logistics chains with a variety of data levels (e.g. item or container levels).

For example a customer in Brazil can enter a shipment on the web and upon release it is immediately visible for the consignee in Europe. Required documents are easily attached through the web and can be accessed by other participants in different locations immediately. This is a very simple example to point out the cloud's advantages for logistics: participants in different locations work with the same software basis. They can share data and information among each other without any delay. The correct and timely availability of data improves the quality of stock, planning and information. Improved decision quality based on complete and timely information leads to increased profitability, reduced capital commitment and time savings.

Success Story Deutz AG

Deutz AG – a globally leading engine manufacturer – trusts the IT platform AX4 when it comes to managing their global 260 suppliers and forwarders. The company which was founded in 1864 is present in 130 countries on all continents with a staff of approx. 5,500.

Through AX4 Deutz AG integrates their suppliers and forwarders directly with the just-in-time and just-in-sequence

processes in manufacturing. Meanwhile more than 80 per cent of all orders for the engine manufacturer are handled through the cloud-based IT logistics solution. The integration of all parties involved through AX4 has led to increased transparency in Deutz' supply chain and thus to optimized processes. Since connecting to the AX4 solution the flow in incoming goods at DEUTZ has increased by 40 per cent. Due to

the automation of processes delivery reliability and quality could be increased. Also the economical side can convince: Due to the optimization of the delivery chain the engine manufacturer has managed to reduce their logistics cost by EUR 20,000 per year. Besides that, investment amounting to EUR 1.5 million which would have been necessary to enhance the capacities could be avoided.

One of the reservations towards the cloud is the lack of influence in individual adaptation of the solution, since we are talking about an outsourced solution here. Therefore some years ago AXIT AG has developed AX4 Open.

With AX4 Open AXIT AG gives their customers the option to configure web masks, processes and roles in AX4 by

themselves. AX4 Open connects what has not been done before: to combine the advantages of a standardized product with the high flexibility that usually is only found in individual development. The result is a reduction of project times by at least 50 per cent. Cost reductions for software implementation amount to about the same figure.

www.axit.de

Global Trade Management and the Cloud – Does It Work?

Cloud computing seems to be the buzzword of the day in discussions about business software. Should companies be paying attention? The answer is yes. Business applications in the cloud are moving us all into the next phase of computing and data sharing, especially in the arena of global trade.

Global Trade Management (GTM) in the cloud means having access to a solution that not only provides up-to-date information in a secure environment, but also allows companies to add compliance areas as their needs grow. It also means that companies can have a single source of truth that is accessible to all parties in the supply chain, while maintaining the integrity of that data in a secure environment. But, before we understand why GTM in the cloud really works, let's explore the components of GTM and the importance of not only having that single source of truth but sharing it across the supply chain.

Let's begin by looking at the components of global trade compliance which include export management, import management, trade agreement utilisation, cost analysis, tariff schedules and other regulatory information, connectivity to regulatory agencies, data sharing and risk assessment. All of these components working together on a single software platform are the foundation of a well-structured trade compliance strategy that allows companies to expand to global markets with little to no additional IT infrastructure or head count. According to the Aberdeen Group's Insight Paper, "Global Trade Management: The ROI of a Shared Global Trading Platform",

“the top investment priority for 75% of companies is to move to GTM platforms that integrate data sharing and workflows with internal users and a myriad of countries, suppliers, carriers and trading partners.”

A large part of GTM, especially when in the cloud, is providing visibility into the supply chain. You may think you have visibility now, but once companies move GTM components to the cloud, they find that by automating processes and creating a shared platform, visibility increases even more.

This process of improving visibility can be broken down into three very broad steps. **The first step** is to get the data needed by all trade partners in an accessible place where it can be updated frequently and utilised when making decisions on moving goods through the supply chain. **The second step** is automating processes that were once manual to reduce rekeying errors and make data available in a more timely fashion. **The final step** is taking the shared data and looking at trends to gather information for better decisions making. This could be as easy as noticing that product is not being classified



similarly at all locations, or as complex as figuring out which of the multiple sources for one good is more cost-effective or which trade lane has the least amount of risk associated with it. Improving visibility allows a company to see more clearly into the entire process of moving a good through the supply chain. For example, if your company is looking to change a supplier or a trade lane, using a landed cost calculator will not only show the most cost-effective way to move goods but also with which regulations a shipment would need to comply as well as savings opportunities that exist by using one supplier or trade lane over another. Understanding country threat risk assessments is another key area of compliance that companies moving to a global market need to consider. Why? Companies need to know if a situation in one country may affect the trade lane used to get goods from point A to point B. If a risk exists, an educated decision can be made earlier in the supply chain to reroute or find a different supplier. Knowing the trade lane and country threat risk assessment, and how to respond, could mean the difference in goods making it to the end user on time or not.

Now that we've explored the "what" of GTM and the cloud, let's look at the advantages of utilising the cloud model versus the traditional install behind the firewall.

If you attempt to install systems behind the firewall to gain GTM capabilities, which require constant regulatory updates as well as maintaining connectivity with entities across the world, you will keep your IT department busy. In the old days, you could wait until your goods got to the port, print off a few pieces of paper and your goods would be released. If your system was down, you could type something up as a backup. With the current requirement of data interfaces provided in advance of imports and exports, you cannot afford for that connectivity to be down or your shipments will be delayed. Most companies want this managed by a provider in the business of ensuring this connectivity.

If you attempt to maintain connectivity and data exchange formats for every broker, freight forwarder, carrier, and regulatory agency with which your company transacts, it won't take long before your IT department tells you they are in the business of building or distributing things, not keeping up with the requirements of different governments and service providers.

Doesn't it make more sense to let a SaaS provider who specializes in trade compliance keep up with the changes so you can access the information online knowing that it is being updated by someone who does that for their livelihood? While you may be sold on the idea of GTM in the cloud, your IT department and even your executive team may still be questioning the security of the cloud.

As the Cloud Security Alliance says, security controls in cloud computing are, for the most part, no different than security controls in any IT environment. Generally, GTM solutions are accessed through a private or hybrid cloud method, which provides the most integrated functionality built directly into the offering. This type of Cloud method also has a high level of integrated security where the provider bears the responsibility for the security.

The European Commission (EC) recognises the cloud as a common approach for business, and is therefore, taking the steps to include data protection rules for cloud computing. As noted on the EC website, those rules will:

- » Develop, with stakeholders, model terms for cloud computing service level agreements for contracts between cloud providers and users
- » Standardise key contract terms and conditions, providing best practice contract terms for cloud services on aspects related with the supply of "digital content"
- » Facilitate Europe's participation in the global growth of cloud computing
- » Work with industry to agree on a code of conduct for cloud computing providers to support a uniform application of data protection rules

To help make sure data security is not compromised, it is important to have security protocols for your company as well as ensure the service provider has fully vetted security on their platform. There should also be a protocol for monitoring the service of the platform as well as monitoring for any attacks or failures.

Beyond the benefits of what global trade management can provide, and considering the security of the cloud greatly depends on the provider and your company's security protocols, what are the benefits of those two together? We've talked a lot about increasing visibility and sharing data, but with GTM in the cloud you can streamline and automate many time-consuming processes.

Being able to gain visibility into the entire supply chain through one platform allows a company to bring other areas or locations on board in a seamless fashion. There are other benefits to utilising the cloud for GTM, some of which include the ability to:

- » Increase productivity without increasing costs
- » Reduce expenses related to IT infrastructure
- » Streamline processes and provide access to data to your global workforce
- » Add on services and solutions as your compliance needs grow
- » Improve collaboration between teams and reduce time wasted on emailing files
- » Connect directly to supply chain partners and government agency systems to share data
- » Access regulatory information that is updated and maintained on a real-time basis
- » Create internal data repositories to share company specific data across the supply chain

There is a lot to think about when considering business applications in the cloud. However, leveraging software in the cloud has many advantages, especially when managing and automating your import/export compliance processes. As more and more Customs Authorities and government agencies move to a paperless environment, we will see more and more relying on a single window where the exchange of data can take place seamlessly and effortlessly.

The right GTM provider is out there – are you ready to make the move?

Cloud Computing Open Standards

An architecture based on open standards allows use of off-the-shelf products and, even where these are not available, enables quicker and less expensive solution developments, which result in more robust and maintainable solutions.

The Internet provides an excellent example of the benefits of open standards. It is a hugely valuable world resource, supporting a massive amount of commercial and other activity. It has a few basic, well-defined components (host, router, network, etc.) that have clearly defined interface standards, such as the TCP and IP communications protocols, and the sockets programming interface. Companies can procure products that conform to these interfaces easily, and knowing that they will work together “out of the box”. It has even reached the point that members of the general public, with no specialist knowledge, can do this.

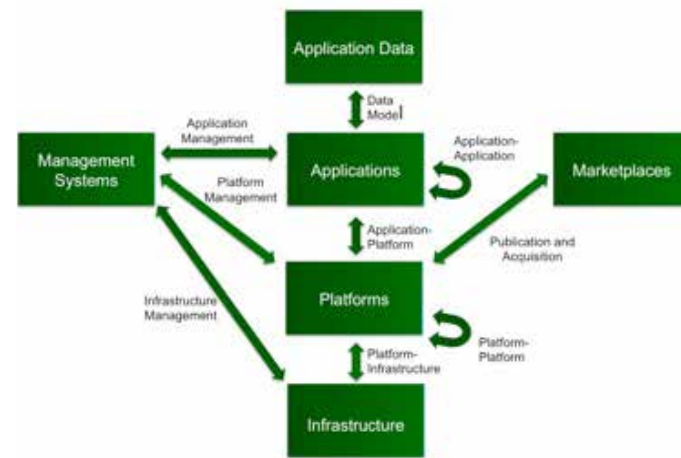
The Internet is one of the foundations of cloud computing, and the growth in cloud computing is partly due to the portability and interoperability that comes from conforming to the Internet standards. But cloud computing is more than the Internet: it provides information processing and storage, as well as communication and display. It has a different set of basic components to deliver this functionality, and the interfaces between these components do not have universally accepted, clearly defined standards. Portability and interoperability are not guaranteed, and they can be hard to achieve. How does this impact supply chains, where cloud computing brings new possibilities for collaboration, and companies want to take advantage of them?

Cloud Computing Portability and Interoperability

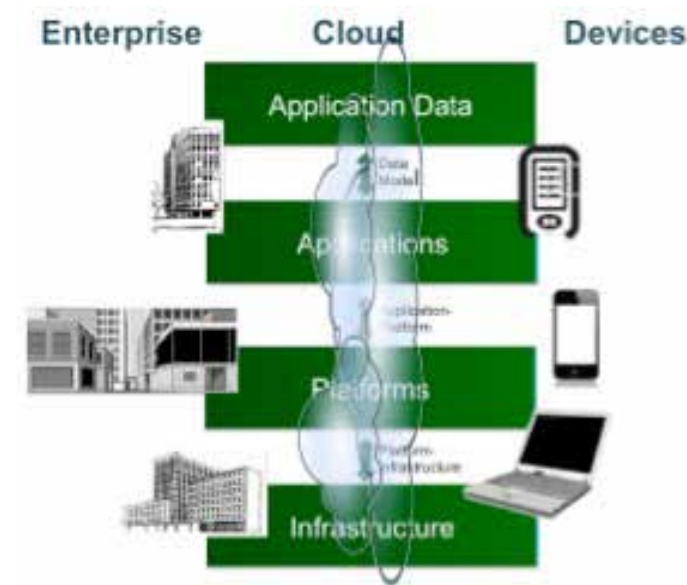
A supply chain is a business ecosystem in which the participants exchange information and add value. In such an ecosystem, consumers and providers can use cloud systems to support common business processes. This is a growing trend, in supply chains as elsewhere, and there are a number of companies offering cloud-based supply chain solutions.

A system that involves cloud computing typically includes data, application, platform, and infrastructure components. These can be as in traditional enterprise computing, or they can be cloud resources that are (respectively) software application programs (SaaS), software application platforms (PaaS), and virtual processors and data stores (IaaS). In its Cloud Computing Portability and Interoperability Guide, The Open Group defines a Distributed Computing Reference Model (DCRM), illustrated below, which describes the key high-level components of such a system, and the interfaces between them.

The Management Systems and Marketplaces are particular kinds of application, shown separately because of their particular relationships to platforms and infrastructure. Marketplaces, which include vendor app stores and customer-operated marketplaces such as the UK government’s Cloudstore, are a relatively new kind of component, that has come to prominence through mobile and cloud computing.



The Application Data/Applications/Platforms/Infrastructure stack is present in enterprise systems, cloud systems, and user devices.



The published and emerging standards that apply to the interfaces are listed in the *Cloud Computing Portability and Interoperability Guide*.

Cloud and the Supply Chain

Supply chains typically operate at the application level. For them, the key interfaces are data models, application-application interfaces, and application-platform interfaces. Application management interfaces may also be relevant, and publication/acquisition interfaces for supply chain application components.

Data models describe the structure of data and are used by applications. They enable the applications to interpret and process the data. They apply to data that is held in store and

accessed by applications, and also to data in messages passed between applications. A supply chain is likely to have a set of important data models that are specific to its needs. These can be defined in various ways, for example using the EXPRESS data modeling language for product data, standardized as ISO 10303-11.

It does not make sense to try to define standard functional interfaces for supply chain applications in general. Different industries have different procedures and terminologies, and these will be reflected in different interface definitions. Even so, interoperability can be increased by following good design principles. *The Cloud Computing Portability and Interoperability Guide* describes seven application design principles that can improve interoperability in cloud-based systems:

- » Loose Coupling
- » Service-Orientation
- » Stable Interfaces
- » Described Interfaces
- » Use of Marketplaces
- » Representational State Transfer (REST)
- » Basically Available, Soft State, and Eventual Consistency (BASE) Transactions

It does however make sense to define standard interfaces for a particular supply chain. Increasingly, applications are web-based and intercommunicate using web service APIs. A set of defined APIs is thus the appropriate application interface standard for a supply chain.

Interfaces between applications and their supporting platforms are found in traditional solution stacks, in the resource environments of cloud and enterprise services, and in user devices. They are programmatic interfaces, for which standards are needed to enable application portability. These can and should be generic standards, not supply-chain-specific.

Supply Chain Standards for Cloud

To some extent, the ability to achieve portability and interoperability of a supply chain’s applications is in the hands of its participants. They can get together to define the specific data models and APIs that they need within the chain. What they cannot do by themselves is to define data models and APIs needed to interface with other applications, or to define the interface to the standard platform on which the supply chain and other applications run.

Each participant will have a different set of applications to integrate with the supply chain. They may be concerned, for example, with sales, purchasing, design, manufacturing, demand forecasting, or inventory management. These applications will have their own data models and interfaces.

Integration of such applications requires a common platform on which they inter-operate. Today, an application platform should include much more than a traditional server operating system does. A modern cloud platform could for example provide capabilities such as data synchronization, identity and entitlement management, and process orchestration. And it should also provide access to the new technologies that, with Cloud, are disrupting our ideas about enterprise computing.

The March of Technology

Cloud computing is not the only new technology in town. Other technical phenomena such as mobile communications, social networks, big data analytics, the Internet of things, and cognitive computing give enterprises opportunities for business innovation. This may impact on supply-chain-related applications. Networked sensors and controls, for example, are integral to many manufacturing processes. Social media and big data analysis are starting to be used for demand forecasting. Enterprise business departments want to be able to use these technologies, together with information processing, storage and communication technologies, easily, as and when needed, but they do not want to devote substantial time and effort to understanding and operating them.

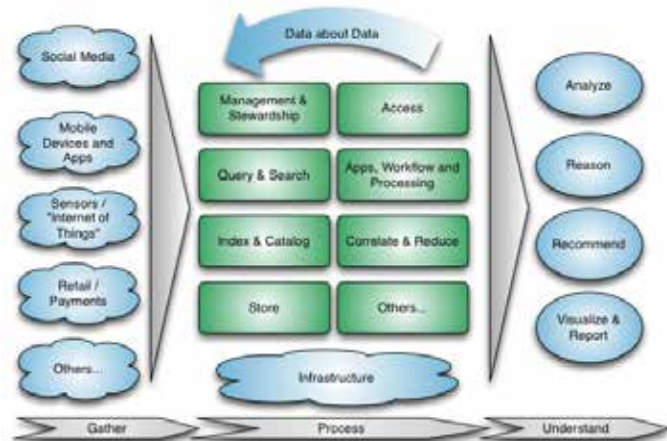
Industry analysts agree on the importance of these developments. Gartner uses the term *Nexus of Forces* to describe the convergence and mutual reinforcement of social, mobility, cloud and information patterns that drive new business scenarios and says that, although these forces are innovative and disruptive on their own, together they are revolutionizing business and society, disrupting old business models and creating new leaders. Gartner sees the Nexus as the basis of the technology platform of the future. IDC predicts that worldwide IT spending will exceed \$2.1 trillion in 2013, up 5.7% from 2012. Smart mobile devices will generate more than 50% of this growth. From 2013 through 2020, a combination of social cloud, mobile, and big data technologies will drive around 90% of all the growth in the IT market. IDC uses the term *third platform* to describe this combination.

Also, we are seeing a revolution in the way that business uses information technology. Increasingly, business departments are buying technology directly, by-passing their IT departments. Users are buying business solutions enabled by cloud services and other new technology. Business and IT are not different worlds any more. Business analysts are increasingly using technical tools, and even doing application development, using exposed APIs.

The New Platform

The Open Group Open Platform 3.0™ Forum has been established to help enterprises to use these technologies, by identifying a set of new platform capabilities, and architecting and standardizing an IT platform by which enterprises can reap their business benefits. The platform will enable enterprises to create, evolve, adopt and use solutions based on current and future emerging technologies to achieve business value. It will do this in a business environment in which end users access the technologies directly and develop innovative business solutions

The requirements for this platform are described in the *Open Platform 3.0 Business Scenario*. The Forum is working on its definition – and welcomes input from other bodies, such as the European Supply Chain Institute.



Conclusions

Using open standards cuts costs and saves time – when the right standards are available.

Cloud computing is founded on the Internet, which is blessed with excellent standards, but beyond that there are few standards for cloud. The additional cloud components that store and process information, unlike the Internet and web components that they use to communicate and display it, are generally not portable and interoperable today. Supply chains can benefit from cloud computing. Supply chain solutions are typically at the application level, and their key portability and interoperability interfaces can be characterized as data models, application-application interfaces, and application-platform interfaces.

Data models and application-application interfaces are supply-chain specific. The participants in a chain can define the interfaces of these kinds that they need. Application-application interfaces today should generally be defined as web service APIs. Interoperability can be improved by following good design principles.

A standard platform is needed to support the application components and facilitate integration between the supply chain components and other applications. Increasingly, these applications are using technical phenomena such as mobile communications, social media, sensors, and controls. *Open Platform 3.0™* is being defined by The Open Group to address this need and support business operations as they are evolving today. The Open Group welcomes input to this definition from the IT industry in general, and from the supply chain community in particular.



About The Open Group

The Open Group is an international vendor- and technology-neutral consortium upon which organizations rely to lead the development of IT standards and certifications, and to provide them with access to key industry peers, suppliers and best practices. The Open Group provides guidance and an open environment in order to ensure interoperability and vendor neutrality.

Further information on The Open Group can be found at www.opengroup.org
“Open Platform 3.0 is a trademark of The Open Group”.

CRM As A Service for Supply Chain Management

By: Ian Moyse - Sales Director, Workbooks (CRM Vendor of the Year 2014, 2013)
Eurocloud UK Board Member & Cloud Industry Forum Governance Board Member

CRM (Customer Relationship Management) has been a hyped acronym for many years and can mean many things to many people. Many debates abound in this area from if it is the correct terminology to describe what it is used for, how much does it really cost, what ROI can really be achieved, how to get users to adopt its use, routes to market to sell it and when do I need a CRM?

The fundamentals are that CRM provides a way to manage customer information, share it securely, track customer interactions and record activities across the business is required by most business sectors and sizes. Sure there are nuances by vertical and specific requirements that at times can be better served by specialised applications, but for the masses the requirements are pretty similar and easy to achieve.

Another shift is that this market is increasingly fulfilled by cloud solutions, where according to Gartner Software-as-a-Service (SaaS) delivery of CRM applications represented 34% of total worldwide CRM application spending in 2011 and more than 50% of all Sales Force Automation (SFA) spending was on the SaaS platform. So Cloud CRM is at the tipping point of outweighing on network solutions in the not too distant future

and becoming the defacto form factor of delivery. How does this effect supply channels and why does cloud change the possibilities and potentials in this arena? Increasingly there are a number of fundamental needs in supply chains that a good CRM can assist with aiding top and bottom line business benefits.

Recording relationships between multiple parties of suppliers, customers, contractors, alliances and consultants is an important part of understanding a supply ecosystem. Knowing who your supplier options are, who they have relationships with and who they compete with can aid in faster and more effective business decisions. Organisations and how they relate today is ever more complex with contractors working for multiple companies, directors being on the board of multiple organisations and sister, parent and subsidiary company relationships increasingly being important to understand. A CRM should make it easy to record these relationships between people to people, organisation to organisation and people to organisations, thus making it easy to spot relationships that could be important to not overlook and enabling you to leverage these where you might not have,

A challenge with CRM systems across supply channels is that invariably they will all adopt a CRM specific to their needs and not wish to coordinate or have a system enforced upon them by other companies, meaning a mix of CRM systems will be used throughout that supply channel. So having the same shared CRM is unlikely to happen, particularly where larger companies will likely afford the big brand and big cost CRM systems that the smaller to mid size firms can ill afford to license let alone deploy



and configure. These however can easily be integrated using simple methods of export and import templates being configured which once done can allow regular manual or automated passing of details from one to another.

Consider also exposing your CRM details to customers and suppliers through other means. Imagine having partners able to manage and update their own details, to update product books or product information for example or be able to track leads and opportunities you are working on their products without having to ask you to produce labour intensive reports. How about allowing customers to view and update their support calls, to view their renewal or transaction details online directly fed from your CRM system and to deal register their opportunities with you without re-keying. With a good web based CRM you can either give such a customer or supplier a login to your CRM with locked down secure access to only their data or expose the relevant data to them only through a secure self-service web portal. This latter option meaning no CRM license is needed by the external company and that they do not need to know your CRM or have it forced upon them.

Consider also the ability to aggregate and expose transactions to customers and suppliers where some CRM systems can process quotes, orders, invoices and supplier orders all inside the CRM system itself.

This enables you to map a customer order through to selecting a supplier option with supply pricing all from within the one system that maintains both customer and supplier details. This also gives benefits such as allowing the easy visibility and reporting of sales margins, supplier reports, product analysis and more all with easy visibility to sales and marketing without any need to ply requests for information from the finance department.

Utilising a Software as a Service CRM system can allow far more flexibility across supply channels and easier access to sharing information between businesses and within your own company.

When selecting a CRM ensure that you consider a wider range of possibilities and ensure that you approach the project with these directives of best practise in mind;

- » Ensure you have clarity on the project objectives from your relevant departments.
- » Employ internal Executive Sponsorship to ensure the CRM project is driven and will happen.
- » Ensure user involvement during planning, what would improve their success?
- » Understand that gaining User Adoption is critical, choose a proven system.
- » Do not blindly recreate existing processes in a new system (without review/appraisal)
- » Consider which vendor you will partner with and their support and track record.



Sustainability in the Data Supply Chain

“The amount of greenhouse gases in the atmosphere reached a new record high in 2012, continuing an upward and accelerating trend, which is driving climate change and will shape the future of our planet for hundreds and thousands of years...carbon dioxide is the single most important greenhouse gas emitted by human activities, such as fossil fuel burning and deforestation.” -- World Meteorological Organization

The World Meteorological Organization’s (WMO) annual Greenhouse Gas Bulletin¹, released in November 2013, shows that “between 1990 and 2012, there was a 32% increase in radiative forcing – the warming effect on our climate – because of carbon dioxide (CO2) and other heat-trapping, long lived gases such as methane and nitrous oxide.” It goes on to say

“Carbon dioxide, mainly from fossil fuel-related emissions, accounted for 80% of this increase.”

If you relate this disturbing trend back to reports linking total global CO2 emissions to an exponential increase in Information Communication Technologies (ICT) activities, it’s clear that if we are to avoid a planet full of waste, hypergrowth and pollution, we need to act now. We can start by taking a look at ICT and the need for major industry contenders to adapt business operations and objectives to more sustainable practices throughout the supply chain, for both the future of our planet and the future of our economy. In short, we’re doing everything with computers, but at what cost?

Big Business is putting their supply chain through bootcamp. Everything from the selection of materials and ingredients to work conditions is being audited to ensure that the most humane and sustainable practices are implemented. It’s exciting to see major multi-national, multi-billion dollar companies taking steps to commit to safe and sustainable business practices. But how far into the supply chain are we auditing and is it really enough?

The realization of the depth to which we have to dive into our supply chains to discover the hidden, yet significant flaws in current business practices is staggering. A great example of this deep dive is the now famous Starbucks discovery – the nitrous oxide canisters used for whipped cream made up a significant portion of their greenhouse gas emissions. Interestingly, with all of the supply chain efficiency and sustainability discussions taking place at conferences and symposiums throughout the world, we found that very few recognized the significance of their data’s carbon footprint when analyzing their supply chain.

The “green approach” used by the ICT industry is traditionally focused on the manufacturing side of the industry, concentrating on the energy efficiency of hardware and lowering the environmental impact of manufacturing processes. While this is an important concern, it’s increasingly less dominant in the energy consumption (and thus, the environmental impact) of the industry as a whole.

We developed practices that allow us to manufacture energy efficient hardware in an energy efficient fashion, but with that we’re also witnesses to (and participants in) an unprecedented rise in demand for energy – in many cases to operate data centers. If we follow the data supply chain back to the data centers on which our global information systems rely, and beyond that to the energy grids powering the data centers, we get to the root of the ICT carbon footprint – fossil fuel-based energy grids.

“Fossil fuel combustion accounts for about 90% of total global CO2 emissions, excluding those from forest fires and the use of wood fuel (EDGAR 4.2, JRC/PBL, 2011).”²

Our new and increasing dependence on global information systems to communicate, power business and drive innovation is reported upon daily. Yet when examining the supply chain, most industry contenders do not acknowledge or perhaps fully understand, the pollutive impact of their online data worldwide. This is surprising, since energy efficiency is often presented as a defining characteristic of one’s greenness in the ICT industry.

If only a few are looking at the negative impact caused by data operations, then fewer will be aware that the ICT industry had rivaled the aviation industry in global CO2 emissions as far back as 2007 (Source: Gartner³) and likely surpassed it in 2012.

What is most alarming is the fact that the very entities ignoring the CO2 conundrum are likely its biggest contributors, with global data operations doubling roughly every two years.

Think for a minute....

All of our international and domestic travel, all over the world, every day, produces LESS CO2 than our status updates, tweets, online photos, videos, databases, customer accounts, web-sites, computing and online storage.

¹ (http://www.wmo.int/pages/mediacentre/press_releases/pr_980_en.html)

² <http://edgar.jrc.ec.europa.eu/CO2REPORT2012.pdf>, page 20. Oliver JGJ, Janssens-Maenhout G and Peters JAHW (2012), Trends in global CO2 emissions; 2012 Report, The Hague: PBL Netherlands Environmental Assessment Agency; Ispra: Joint Research Centre

³ <http://www.gartner.com/newsroom/id/503867> and <http://www.ihs.com/news/gartner-datacentre-co2.htm>

Cloud computing is the fastest growing sector of the ICT industry, and often touted as a solution for reducing negative environmental impact. Moving to the cloud makes good business sense, since its utility-style billing ultimately costs less and its infinite resource availability offers necessary scalability while allowing flexibility in both operations and investment. Early adoption of cloud-based services by individuals and small businesses is also indicative of this trend, even more prominently than the slower, but inevitable move by enterprise businesses and governments.

Nevertheless, the push towards clouds, whether public or private, is becoming the new standard on which future applications will live, particularly as the Internet of Things is further realized.

GreenQloud, which utilizes renewable energy-powered data centers in Iceland and Seattle, has already addressed some of the more significant problems and drawbacks that prevent businesses from widespread adoption of clean cloud services, including cost effectiveness, migration hurdles and readily available clean, renewable energy-powered electricity. However, even though businesses realize and recognize the importance of sustainability and the need for action, and may want to adopt the technology, regulatory compliances, possible technological challenges and perceived security concerns may dissuade skeptics from moving to the cleaner, more sustainable public cloud platform. As a result, GreenQloud released a new product, QStack, meant to meet enterprise companies where they are in the adoption cycle, providing both private and hybrid cloud services to guide these companies to a more sustainable cloud future.

Cloud computing offers undeniable advantages in operations. By distributing resources on an as needed basis, it reduces hardware overhead and facilitates a sustainable consumption of computing power and storage. Using less hardware also means a reduction in the pressure on the manufacturing processes, increasing the lifecycle of the hardware.

Moving to the cloud also means the beginning of the end for hardware fragmentation – the usage of open source, platform agnostic technology allows for a more efficient advancement in hardware innovation, and accelerates and refocuses efforts in developing more sustainable software solutions.

To help facilitate change and to act responsibly as architects and innovators of this new technology, cloud providers need to be receptive to the pain points of business – namely resolving regulatory compliance restrictions and security concerns, and create software-based solutions that bridge the gap between the cloud and adoption of it.

Products such as QStack enable enterprises and organizations to build private clouds on their own existing infrastructure, as well as scale and migrate workloads to GreenQloud’s clean, renewable energy powered public cloud. This solution allows businesses reluctant to or restricted from moving wholly to a public cloud environment to utilize the key advantages of public cloud software, such as that of GreenQloud’s public cloud. This private/hybrid solution allows for a more conservative investment into IT infrastructure, solves the problem of scalability in the face of rapidly changing demands, lends more

transparency to energy usage in the data supply chain, and encourages the adoption of sustainable cloud practices by helping companies meet their “by 2020” goals.

When we talk about sustainable cloud practices, it’s important to look specifically at data centers and energy suppliers, as recent reports indicate that the lion share of CO2 emissions generated by ICT is increasingly a result of operations rather than the manufacturing process where supply chain analysis places most of its focus. Even as the manufacturing process of big industry looks to become more sustainable, this effect is offset by the increasing demand for energy from data centers.

PUE vs. GPUE

According to Gartner⁴, 12% of all data center expenditures are related to energy and are the fastest rising cost. Because of the increased power capacity required for increased performance of the data centers, power usage effectiveness (PUE) metrics⁵ introduced by The Green Grid⁶ have become the template for data centers to analyze and control their energy consumption and cost, serving as a benchmark for indicating a data center’s greenness.

$$\text{PUE} = \text{Total Facility Energy} / \text{IT Equipment Energy}$$

However, in many cases the PUE only serves to outline efficiency and doesn’t accurately account for greenness at all. GreenQloud wanted to improve this formula and introduced its own GPUE (Green PUE / Green Power Usage Effectiveness) metrics⁷ as a means to “weigh” the PUE to better see which data centers are truly green, in the sense that they indirectly cause the least amount of CO2 to be emitted by their use of dirty or clean energy. These metrics are designed to lend more transparency into the actual greenness of the energy consumption at data centers.

GPUE gives the truly green data centers a boost in the battle with their “green washing” counterparts. It’s very easy to calculate the CO2 emissions created for each usable KWh for the IT equipment. Here’s the definition and the presentation format for GPUE:

$$\text{GPUE} = \text{G} \times \text{PUEx}$$

(for inline comparison of data centers) or

$$\text{GPUE} = \text{G} @ \text{PUEx}$$

(a better display and for CO2 emission calculations)

The “G” is the key factor here and it’s a simple calculated value:

G = Weighed Sum of energy sources and their lifecycle KG CO2/KWh

$$\text{G} = \sum (\% \text{EnergySource} \times (1 + \text{weight}))$$

⁴ Gartner Press Release 29/09/2010 <http://www.gartner.com/newsroom/id/1442113>

⁵ White Paper #49-PUE: A Comprehensive Examination of the Metric <http://www.thegreengrid.org/en/Global/Content/white-papers/WP49-PUEAComprehensiveExaminationoftheMetric>

⁶ <http://www.thegreengrid.org>

⁷ GPUE – Green Power Usage Effectiveness <http://www.greenqloud.com/greenpowerusageeffectiveness-gpue/>





What's the + 1 for? It's there so when we "weigh"(multiply) the PUE we get a number that's not less than the PUE. This gives us a better feeling of the scale because we're used to the small PUE value range.

The weights are simply taken directly from the "lifecycle CO2/ KWh for electricity generation by power source" table that was published in the 2008 Sovacool Study⁸ (e.g. the weight for un-scrubbed coal is 1.050 (kg of CO2/KWh) while hydroelectric river generation has a weight of 0.013). An unknown energy source or a "mix" will get the same as the maximum value which for now is the same as coal.

Example:

PUE 1.20, 50/50 Coal/Hydro
 $G = 0.5 \cdot (1 + 1.050) + 0.5 \cdot (1 + 0.013)$
 $G = 1.531$, GPUE_x = 1.84 or 1.531@1.20
 Kg CO2 per usable KWh = $(G - 1) \times \text{PUE}_x = 0.64$ Kg

It's very interesting to see the GPUE side-by-side to the PUE of these "green" data centers in the GPUE graph.

Company	Database Location	Energy	G	PUE	GPUE	KG CO2/KWh
 greencloud	Iceland	70% Hydro, 30% Geothermal	1.021	1.1	1.12	0.02
YAHOO!	NY, USA	21% Coal, 27% Nuclear	1.497	1.16	1.74	0.58
Google	OR, USA	34% Coal, 3% Nuclear	1.490	1.20	1.79	0.59
Google	NC, USA	50% Coal, 39% Nuclear	1.630	1.21	1.97	0.76
	NC, USA	50% Coal, 39% Nuclear	1.630	1.50	2.44	0.94
	IL, USA	73% Coal, 23% Nuclear	1.819	1.22	2.22	1.00
	TX, USA	37% Coal	1.936	1.20	2.32	1.12
YAHOO!	NE, USA	74% Coal, 15% Nuclear	1.834	1.5	2.75	1.25

The data table is mostly sourced from the Greenpeace report "Make IT Green"⁹.

These percentages don't quite add up because these are the local grid suppliers, the rest is what we call a "mix". Some of those data centers also didn't have a public PUE (underlined) so for demonstration purposes we gave them a PUE of 1.5 and did the calculations. GreenCloud's data centers in Iceland have PUEs of 1.1 and 1.15 because they only use 100% renewable energy (geothermal and hydro). GreenCloud's GPUE will roughly be equal to its PUE_x and that's the point. Truly green data centers will have a GPUE close to their PUE_x and dirty energy data centers won't.

Let's take a step back, however, and overlook for a moment the efficiency of hardware and data center power effectiveness. As adoption of online services and cloud based businesses becomes more widespread, the strain on existing data centers and the demand for new ones increases, putting even more stress on existing energy grids, and therefore the environment.

However, a cloud offering that is powered by renewable energy and located cool climates not only eliminates the need for over-

investment in infrastructure - in fact reducing costs by reducing cooling requirements, by up to a saving of over 30% - but also cleans up the data supply chain from an operations standpoint. Having a sustainable cloud offering available, even with increasing adoption of cloud services, reduces the impact to the environment significantly. This is one of the many reasons GreenCloud opted to power its cloud with renewable energy.

As we progress in our adoption of cloud computing, the demands on energy suppliers will reach a point where expansions are needed. By adopting a stance focused on sustainability and clean energy we can accelerate the growth of renewable energy suppliers and technology. As we use more and more of the resources available to fuel our increasing need for energy across industries, using mixed and preferably renewable energy-only platforms will be necessary.

⁸ Benjamin K. Sovacool. Valuing the greenhouse gas emissions from nuclear power: A critical survey. Energy Policy, Vol. 36, 2008, p. 2950. http://www.nirs.org/climate/background/sovacool_nuclear_ghg.pdf

⁹ Make IT Green: Cloud computing and its contribution to climate change <http://www.greenpeace.org/international/en/publications/reports/make-it-green-cloud-computing/>



GreenCloud is making strides to encourage a transparent approach to CO2 emissions through the data supply chain. The company has been leading this initiative in the cloud computing industry since its founding in 2010. GreenCloud eliminates several significant barriers to cleaner cloud practices: cost, lack of renewable energy, automation and migration. To expand on this, it has no premium pricing for green services and is often less expensive because it is green.

Being headquartered in Iceland, GreenCloud has an abundance of renewable clean energy at its fingertips, and continues to explore new avenues where it can utilize and nurture the renewable energy market into mainstream. For example, GreenCloud recently selected its first US data center location with Digital Fortress™ in Seattle, Washington not only for its strategic location in better servicing the Pacific Northwest, but also for its 95% renewable energy power threshold. Finally, GreenCloud's advanced industry standard API controls (EC2, S3 compatible) enable full automation of IT services, and its solutions are designed from the ground up to facilitate easy migration between cloud providers and adaption to the emerging technologies.

Customers have access to live data metrics to not only effectively and efficiently manage their infrastructure, but also to supplement their CSR activities, and use the energy and carbon data to strategize their operations. They can also opt to share their metrics directly from the private console to their company's social media.

GreenCloud is committed to furthering its transparency on energy usage and CO2 emissions by producing content that educates stakeholders, industry contenders and the general public to understand, practice and demand environmental responsibility.

Additionally, it has participated globally in many conversations, events and strategies to eliminate "greenwashing" from company reporting practices and raise awareness of the ICT industry's impact on the environment. The goal is to encourage the industry to take responsibility by examining and reviewing the supply chain, and subsequently taking steps in order to reduce the alarming damage they inadvertently cause.

GreenCloud was honored to participate in the Global Green Growth Forum (3GF) in Copenhagen, Denmark in October of 2013, Sustainable Brands in November and most recently, 2Degrees Live in February, where sustainability driven delegates from around the world convened to discuss actionable strategies for increasing a global focus on sustainable practices through four key themes energy, water, food and greening the value chain.

Event discussions included strategies for growth while efficiently utilizing resources to drive competitive companies, localizing and augmenting energy resources for hyper efficiency (such as Ikea's plan to be energy independent by 2020 through turning stores into power plants by capturing wind and solar energy on roofs and changing 1.2 billion incandescent lightbulbs for LED bulbs - source: USA Today), financial strategies for stronger environmental profit and loss, devising more sophisticated measurements for waste analysis, and opportunities in regions such as China, Indonesia, Africa and Latin America. Among all of the compelling commentary, debates and actionable strategies, one quote that stands out from the 3GF event in Denmark (and there were many) was from Hannah Jones, Vice President of Sustainable Business & Innovation for Nike, who cut to the core of sustainability conundrum and encouraged the participants to "position sustainability as an innovation imperative." Likewise at the 2Degrees Live event, there was a significant focus on hardcoding sustainability into company culture, making it a business priority rather than a checkbox for regulatory compliance or public relations.

The participants of these events collectively offered actionable examples of how they implemented sustainable practices into their company culture, supply chain and overall operations, signalling that the time of contemplation is over and the age of acting on sustainable principles has begun.

While GreenCloud has sustainability as a core aspect of its corporate identity, it's working with key industry figures, major academic researchers and the general public to put sustainability front and center in the ICT industry. After all, GreenCloud's existence was born from the idea of leading the ICT industry into a sustainable future where both business practices and environmental responsibility will benefit from clean, sustainable cloud technology.

Why the need for recognised Cloud certification?

By: Richard Pharro, CEO of APM Group Limited
and member of the Cloud Industry Forum Governance Board

Cloud solutions represent the most significant development in the delivery of IT in a generation, offering end users the three-fold benefits of reduced costs, enhanced operational availability and on-demand scalability.

Furthermore, Cloud technology levels the playing field for all IT consumers enabling them to participate regardless of size due to the unique pay-as-you-consume financial model, thus enabling small and medium-sized enterprises (SMEs) to access the same technology and gain the technical agility that has previously been the reserve of large enterprises.

According to the Cloud Industry Forum's fourth annual Cloud adoption survey, 69 per cent of UK businesses have formally adopted Cloud services within their organisation. This is an eight-point increase or 15 per cent annual growth and a compound growth of 44 per cent since the first survey conducted by CIF in 2010. The research also found that satisfaction with the use of Cloud solutions remains high at 91 per cent.

But while the overall adoption rate increases year-on-year, end users (and notably SMEs) consistently identify three barriers to adoption of Cloud solutions. Two are technical (relating to data security in the Cloud and portability of data) and are the subject of significant technical developments and standards work. The third barrier relates to the issue of trust. In a market of online delivery models with many new vendors, how does a potential customer know that the company with which they wish to work will provide a secure, stable, and effective solution that enables them to retain control of their data throughout the contract and after it expires?

Plainly, greater clarity about data protection, privacy and sovereignty is needed. Standards setting organisations and certification bodies certainly have a role to play in this by defining, encouraging and validating best practice for Cloud Service Providers (CSP) and improving end user education.

However, Cloud is still a relatively young technology and very few clear Cloud standards have thus far emerged. The most promising work in standards development is the ISO/IEC SC83 working group, which aims to introduce a universal best practice standard for Cloud Computing; however, as is the case with all ISO standards, they take time to materialise due to the level of consultation required.



Richard Pharro

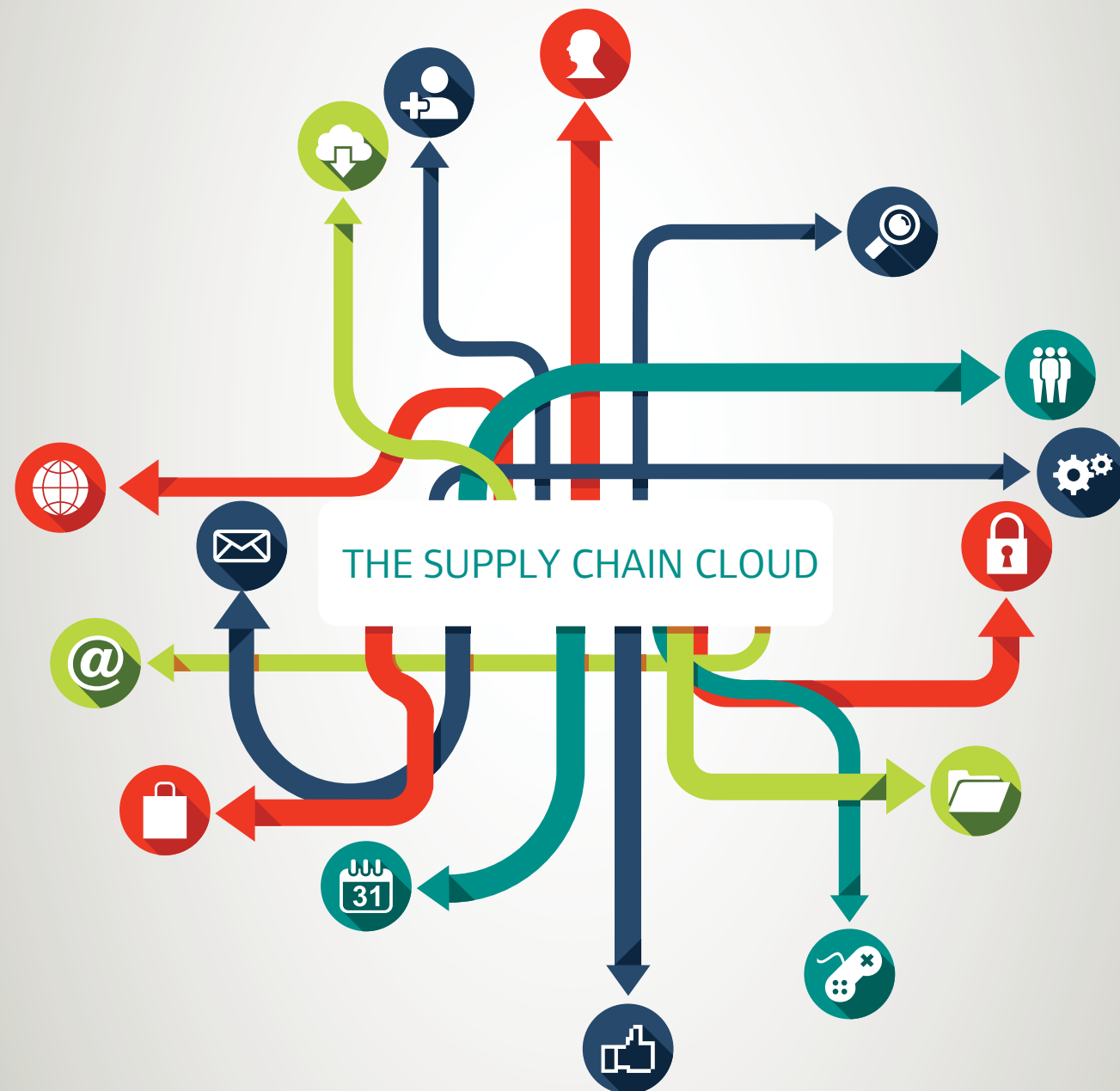
One standard that is rapidly gaining ground in the UK is the **Cloud Industry Forum's Code of Practice (CoP)**, which aims to ensure that end users have enough information available to make an informed decision about their migration to the Cloud. This information relates to three areas of concern: **transparency, capability** and **accountability**. Equipping end users with this information is the first step towards trust.

The use of the CIF Certification Mark on a vendor's website serves two clear purposes: it makes a public declaration of professional and commercial intent on the part of the Cloud Service Provider and it provides a visual mark of recognition that engenders confidence in the end user that the organisation is open and professional in its commercial activities.

CSPs need to ensure they operate their businesses and services in a fully open and transparent manner where it is clear to their customers – existing and new – that they are trustworthy and capable of offering the services they claim to be able to offer. The CIF CoP is one of very few schemes which offers this much needed reassurance to end users regarding the organisations they choose to work with.

After all, let's not forget whom certification is ultimately for: the end user. In this relatively young industry, in which it's easy to seduce customers with false claims over security and data protection, certification provides much-needed independent endorsement of providers' promises. As in any market, independent validations that allow customers to make more educated buying decisions have to be of value. The Cloud Industry Forum has taken important steps in providing this foundation in what is a fast changing and, to many, a new technology sector.

Quite simply, certification schemes, such as CIF's CoP, enable professional Cloud Service Providers to demonstrate with clarity their ethics, practices and processes through an independently recognised and credible body in order to build trust with prospective customers.



Moving to the Cloud

Introduction

As we all know, maintaining a seamless process to work with a supplier or customer network is one of the greatest challenges faced by manufacturers and suppliers today. Many organizations have thus introduced supply chain management systems, ERP infrastructures and other computerized systems over time to manage their supply base more effectively. Regardless of industry, this has oftentimes led to the development of isolated supply chain solutions that are hand-tailored to meet the specific requirements of a particular industry, company or even a single plant or production line within an organization.

While these individual solution setups typically work great for the job they had been originally created for – e.g. enabling supplier connectivity with a given, steady set of trading partners – they are typically cumbersome to enhance when additional requirements need to be met.

Now, couple that with the fact that user expectations have massively changed in recent years – thanks to the ever-growing popularity of devices like smartphones, tablets and e-books and cloud-services like Google Docs, Dropbox and Facebook. Today's users are embracing the flexibility, accessibility and availability these solutions offer. And this in turn also revolutionizes the supply chain solution landscape.

This is why nowadays, companies are increasingly looking to leverage cloud-based supply chain solutions to replace all or at least some of their existing in-house supply chain management infrastructure. Firstly, because cloud-based supply chain solutions promise to facilitate the integration of smaller or less tech-savvy trading partners into a company's supply chain due to the inherent benefits of scalability, ease of adoption and cost-efficiency. Secondly, because users all over the world are increasingly expecting to access and leverage business applications and services through mobile devices just like they're used to do in their private lives. And thirdly, because integrating social media networks into the supply chain framework proposes faster and more effective communication with employees, customers and suppliers. As a result, cloud-based technologies can dramatically improve the sharing of information across trading partner networks and streamline supply chains.

Cloud Computing: Security at Risk?

While all of the above benefits are legitimate, it is also true that many organizations shy away from introducing cloud technologies because of security concerns. In fact, a flawed

cloud implementation can indeed increase the risk of a data security breach significantly, and require extensive custom work to handle multiple partners, applications and technology standards. But as we shall see, most of these concerns are not unique to cloud deployments and others can be addressed with solutions and tools that are readily available today. But before we take a closer look at the most common security challenges faced by companies that move their supply chain to the cloud (and also learn how to resolve them), we should first further refine our framework of interest.

To begin with, we're examining cloud security primarily from the perspective of an organization that is seeking to implement a supply chain solution using the so-called **Software-as-a-Service** (SaaS) model. In such a scenario, an organization is licensing a supply chain application for use as an on-demand service (a popular example is Salesforce CRM) from a cloud provider. This is by far the most common use case since only larger companies have the need as well as the financial and/or human resources to support **Platform as a Service** (PaaS)¹ or even **Infrastructure as a Service** (IaaS)² deployments. Besides, there's another important distinction: in a PaaS or IaaS deployment, essential elements of the security framework (e.g., installing OS & application updates; firewall settings) are under the control – and hence responsibility – of the cloud customers themselves. In a SaaS model, though, the customer is ultimately depending on the cloud provider to ensure proper security practices.

Security Risks

In this section, we'll examine three security risks typically associated with cloud computing and ascertain precautions and counter-measures to minimize or even eliminate the potential security breach.

Data Security

In a SaaS deployment, an organization's business data is no longer being stored on-premise, but has instead moved to the cloud provider. It is probably not surprising that according to a survey amongst small and midsize businesses in published by Microsoft in 2013, 60 percent of study participants in the USA and 56 percent of European respondents stated that data security was a major concern and an inhibitor to cloud adoption³.

Yet it is the cloud provider's responsibility to apply appropriate security checks to safeguard the data from security breaches provoked by insecure applications or malicious employees. The best practice to ensure data security is the use of strong encryption techniques – simply because the stored data is essentially worthless without the correct decryption key. However, encrypting the data is not sufficient on its own. It needs to be coupled with a sophisticated authorization model to warrant detailed control regarding data access.

¹ PaaS is the delivery of a computing platform and solution stack as a service (e.g., Google Apps, Windows Azure).
² IaaS means the delivery of (typically) virtual IT infrastructure as a service (e.g., Amazon Web Services).
³ "Small and midsize companies in the cloud reap security, privacy and reliability benefits", Microsoft Press Release, 11 June 2013



Vulnerabilities to watch out for:

Cross-site scripting[XSS] | Access control weaknesses | OS and SQL injection flaws | Cross-site request forgery [CSRF] | Cookie manipulation | Hidden field manipulation | Insecure storage | Insecure configuration.

Data Segregation

Multi-tenancy is a key component of cloud computing and as such allows for substantial cost savings because it significantly reduces the amount of memory and processing overhead used by (virtual) applications are sharing processor. However, multi-tenancy also means that data from various customers is stored at the same (physical or virtual) location, making intrusion of data from one user by another possible. If the cloud application is not safeguarded against the vulnerabilities of bypassing security controls through means of handcrafted parameters, such as injecting malicious code through SQL parameters, sensitive data might be accessed by unauthorized individuals. To prevent this scenario, cloud customers should be careful to select a cloud provider with a SaaS model that ensures a clear boundary for each user's data on both, the physical as well as the application level.

Vulnerabilities to watch out for:

SQL injection flaws | Data validation | Insecure Storage

Data access, authentication and authorization

Every organization has security policies in place that govern access to data on a user basis. Typically, individual users are assigned to one or many user group(s) with distinct data access allowances

(e.g., engineers might have access to engineering and R&D data, but not to financial or sales data). When moving to the cloud, companies must take into consideration that data access is no longer limited to their own employees. In fact, certain employees of the cloud provider will need to have access to specific data sets in order to be able to maintain, enhance or troubleshoot the SaaS application. It is thus imperative for cloud customers to contractually ensure that their security policies are obeyed by the cloud provider and that there are clear rules in place that govern who has which data access rights in what circumstances. In short: the cloud provider needs to be capable of incorporating company specific security policies to their SaaS model⁴.

A secure cloud environment thus has to have robust authentication and authorization procedures in place to enforce a company's security policies even outside the firewall. The majority of enterprises use a variation of Lightweight Directory Access Protocol (LDAP) servers to handle their employees' credentials (Identity and Access Management⁵). But when companies move to a cloud application, oftentimes SaaS applications insist on storing user credentials in the cloud as opposed to the local LDAP server. This in turn means that the company using such a service is no longer able to centrally control an individual user's credentials, but has to maintain at least one additional user database in the cloud. Administrators hence have to manually add/remove users (provisioning & deprovisioning) from the SaaS application(s) user database(s) as new employees come on board and others leave the company (or simply take on new roles with different data access requirements). Quite obviously, this task becomes more and more complex and error-prone the more disconnected SaaS applications (from an IAM perspective) are leveraged.

⁴ Blaze M, Feigenbaum J, Ioannidis J, Keromytis AD. The role of trust management in distributed systems security, secure Internet programming, issues for mobile and distributed objects. Berlin: Springer-Verlag; 1999. p. 185–210.
⁵ "Identity Management includes the creation, management and removal (deletion) of a digital identity. Access Management includes the authorization of access to only the data an entity needs to access to perform required duties efficiently and effectively." Cloud Security Alliance, SecaaS Implementation Guidance. Category 1 // Identity and Access Management". 2012. Page 11.

Vulnerabilities to watch out for:

Data Access Flaws | Disconnected Identity and Access Management | Non-integrated Provisioning and De-Provisioning

Remedies

In comparison to a conventional, on-premise solution, we have seen that moving to the cloud requires some additional considerations to be made with regard to security. Fortunately for cloud customers, tried and tested methods to mitigate the associated risks already exist. Some of the risks associated with questions of data locality or data segregation can be prevented by signing appropriate contractual agreements with the cloud provider. In other cases, as for data and network security, data encryption can lessen the threat and potential harm caused by security breaches. At some point, however, the encrypted data eventually needs to be decrypted so that authorized employees can access the information they need. Evidently, this requires an Identity and Access Management (IAM) implementation that encompasses the SaaS environment and doesn't stop at a company's firewall boundaries. Essentially, IAM needs to be thoroughly rethought to make it "fit" for a cloud environment since identities are no longer tied to a single directory service only, but come from various sources of identity⁶. Rather than tackling this in a silo, let's look at other industries that have solved the same problem. Oil & Gas companies have a lot of cross-enterprise and cross-country communication involved, oftentimes due to joint ventures or project-based partnerships. As a result, a diverse, loosely coupled workforce with special identity and security requirements needs to be enabled to securely access relevant information and applications.

Similar requirements with regard to security are shared by the healthcare industry. Again, highly sensitive information is being shared both internally as well as externally. Healthcare companies thus need an ecosystem that enables them to interact with back-end systems, collaboration functionality and sophisticated medical machines without sacrificing security.

Key stakeholders need to be able to securely collaborate and exchange confidential, high-value information with suppliers, partners, customers and employees.

In both (and many other) use cases, tried and tested solutions are already in use today that can (and should be) leveraged by manufacturing companies seeking to move their supply chain to the cloud. We're talking about cloud-based identity and access management solutions which are ideally suited to meet the requirements of the cloud because they themselves are delivered through the cloud. Such an IAM system offers a single, secure point-of-access to an organization's internal and external information, applications and systems required to achieve optimum enterprise collaboration and performance.

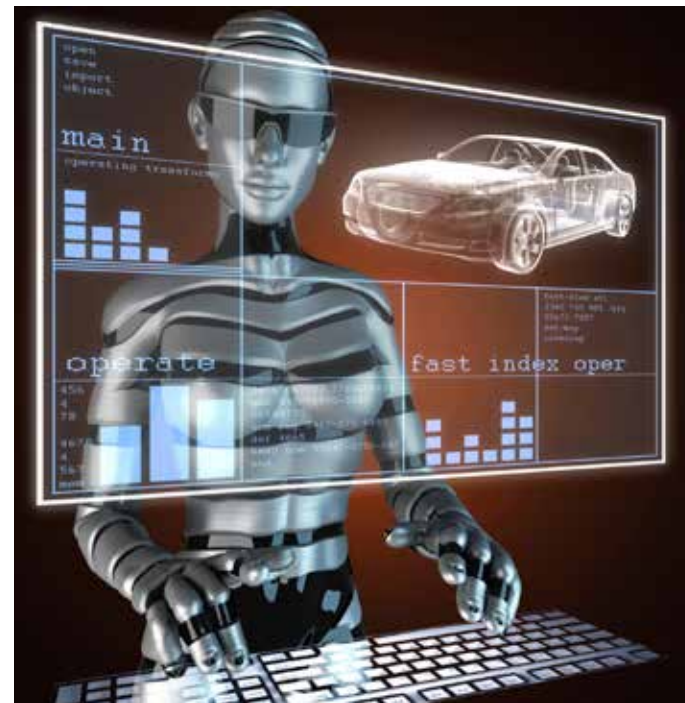
Authentication

First, there's the important question of how and where user authentication is being handled. Authentication means the checking and validating of a user's (or an IT system's) security

credentials before access to shielded assets is being granted. Prior to the rise of cloud computing, such an authentication process would typically be carried out by means of a locally installed LDAP server (oftentimes AD). Some SaaS providers still delegate this process to the customer's internal LDAP server reasoning that companies thus remain in control over user management. However, this approach can cause substantial complications down the road when external sources of identity from contractors, suppliers or (consumer) cloud services need to be integrated. In addition to that, concepts such as BYOD ("Bring your own device") and the use of social networks are quickly gaining momentum across industries and locations. Ideally, every new source of identity should be fully integrated into the existing IAM infrastructure to ensure maximum security as well as highest comfort by enabling single sign-on technology (SSO)⁷.

Unfortunately, conventional on premise IAM platforms fall short in terms of embracing these important cloud standards and cannot come to the rescue. Since they were originally designed to interact only with on premise applications, conventional IAM platforms rely on proprietary security tokens as opposed to open standards and hence offer only limited SAML support (if at all).

IAM Solutions that are delivered and operated in the cloud (Identity and Access Management as a Service – IAMaaS) are better equipped to meet these requirements. Instead of having to individually set up, configure and continuously secure multiple identity sources on a local LDAP server or IAM infrastructure, IAMaaS solutions are designed from scratch to operate in a cloud environment. Consequently, cloud-based IAM solutions come with a so-called Security Token Server (STS) that can exchange both, proprietary as well as open standard security tokens and are thus already prepared to include additional sources of identity.



⁶ See <http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>, page 136.

⁷ "Single Sign-on (SSO) is the functionality within access management where [sic] user is authenticated once and the credentials for the session are trusted across different applications within a security domain." Cloud Security Alliance, SecaaS Implementation Guidance. Category 1 // Identity and Access Management". 2012. Page 11.



When selecting an IAMaaS provider, companies should make sure that the solution features strong authentication mechanisms for verifying the credentials and confirming a user's authenticity. Strong authentication means that at least two of the three types of authentication factors – knowledge, possession and inherence⁸ – are used to identify a user. In addition, organizations should also verify that the IAMaaS solution offers risk-based authentication to maximize security and also raise user acceptance. In contrast to a static authentication scheme that is configured once and for all, risk-based authentication enables a dynamic authentication process by taking into account the user's security profile, the time of the request and the type of request. Based on these circumstances, the IAMaaS system determines a risk rating for both, the task in question as well as the user. By comparing the two ratings, the system determines the authentication level required to access the requested resource: for higher ranking tasks (e.g., submitting an order), a higher level of user authentication may be required (e.g., a one-time password pin delivered to a pre-defined mobile phone). Besides bringing additional security to the table, risk-based authentication also benefits the end user because additional credentials will only be requested if and when a task is highly sensitive (e.g., deleting customer data) or something is unusual (e.g., login attempt from a new device).

Federation & User Management

As we've already seen above, the growing importance of cloud services makes it necessary for IAM platforms to extend the reach of their identity services to include external sources of identity. The method of choice in this context is Federated Identity Management, which provides the policies, methods and tools to manage the identity and access of users to resources of partner organizations. In other words, it enables the reuse of a user's credentials outside of an organization's core security domain so that users don't need to remember multiple logins and can still securely access data or systems of another security domain seamlessly (Federated Single Sign-on). Besides, Federated Identity Management also facilitates user lifecycle management by completely abolishing redundant user administration through central administration.

Hence, a comprehensive IAMaaS platform needs to provide a convincing model for the centralized management of user information including credentials. The solution needs to be able to create new accounts (provisioning) for all suitable systems, applications and services inside and outside a company's firewall. In the same manner, the IAMaaS solution must be capable of revoking access rights and deleting user accounts across all attached systems, applications and services (deprovisioning).

This is especially important with regard to compliance, since access rights or accounts must be disabled as soon as a user's role changes or he/she leaves the company to prevent unwanted data breaches. The IAMaaS solution must hence be capable of real-time synchronization of provisioning and deprovisioning.

In essence, the IAMaaS solution should be able to leverage your enterprise user store as the single source of truth for identities and entitlements across on premise and SaaS applications.

Since the IAMaaS provider is typically storing all the data needed for user authentication, it is essential that the solution offers import/export functionalities for identities and security policies to prevent a potential "vendor lock-in".

Authorization, Access Management and Auditing

The next (and final) step in safeguarding an organization's digital identities relates to authorization and access management. The concept of authorization governs an individual user's right to access a particular resource or system. It is imperative that user access is being granted or disallowed in real-time with respect to the authorization policies in place at the time of the request. It is crucial to restrict fully trusted (e.g., administrative access) as well as completely anonymous access as much as possible, since both access types can cause severe issues if not controlled appropriately.

Access management makes sure that user access is always matched against the user's credentials as well as the attributes associated with that identity. It is important to note that access management and associated policies must be implemented for all layers of the cloud environment, namely infrastructure, platform and SaaS. Failure to do so results in the risk of compromising security as a whole because access control is made useless if an access policy is not enforceable on all architecture layers.

Likewise, an organization is well advised to ensure proper mechanisms for audit and reporting are in place. The IAMaaS solution must not only be able to meet the basic audit requirements conventional platforms offer, but also be capable of monitoring access to cloud services. Comprehensive and meaningful audit logs that include cloud-based applications, systems and services are thus an essential element of a future-proof IAMaaS solution.

⁸ Knowledge factor: something only the user knows (e.g., password); possession factor: something only the user has (e.g., device); inherence factor: something only the user is (e.g., fingerprint).

Summary

The need to manage individual identities across a broad network of internal and external employees, customers, partners, and other stakeholders grows in importance the more cloud-based services are to be integrated in company's IT infrastructure. And this trend is unstoppable. It is thus essential that users are able to securely access the information they need, whether it be on premise applications or SaaS offerings.

As we have seen, such a future-proof, cloud-based IAM solution should be based on open standards and protocols to avoid the risk of a vendor lock-in and also to foster innovation. Straight-forward, enterprise-class SLA's and support models ensure that compliance requirements – including data availability and data locality – are appropriately met. Lastly, the IAMaaS provider

should exhibit a satisfactory track record of successful IAM implementations, ideally across multiple industries and for businesses of all sizes up to enterprise-scale deployments.

The Covisint platform supports the most demanding enterprises and the largest global implementations, managing over 18 million digital identities, supporting over one million daily messaging transactions and providing single sign-on (SSO) access to over 1,000 on-premise and cloud-based applications. Covisint has been recognized as a pioneer of cloud computing, offering solutions and services that leverage a Platform-as-a-Service (PaaS) model. Covisint's Cloud Engagement Platform is based on a highly scalable, reliable, and secure Service-Oriented Architecture (SOA) that has been successfully deployed for over 12 years.



Applications in the Cloud

– Adopt, Migrate, or Build?

By: Claude Baudoin – cébé IT & Knowledge Management

Cloud Computing: Growing Up Fast

Just a couple of years ago, we were witnessing — and some of us were deploring — the “irrational exuberance” (to quote former Federal Reserve Chairman Alan Greenspan out of context) as well as the uncontrolled fears of many customers and decision makers about cloud computing.

When we look at past technology adoptions (e-mail, the Web, object orientation, Public Key Infrastructure, and Service Oriented Architecture come to mind), the speed of adoption has been accelerating, but each time there was an extended period during which technology enthusiasts and business managers disagreed on the strategy to adopt. Too often, the new trend seemed to be a solution in search of a problem.

But a strange thing has happened with the emergence of cloud solutions: the discussion has quickly become much more reasoned, with a surprisingly good balance of proactive concern for the risks and a genuine desire to experiment with new solutions. The situation has also benefited from the uncommonly rapid emergence of guidelines, if not real standards, from various institutions. And the message of greater agility in responding to business requirements, elasticity in the face of variable demand, and replacing capital investments with operational expenses has resonated with the business stakeholders.

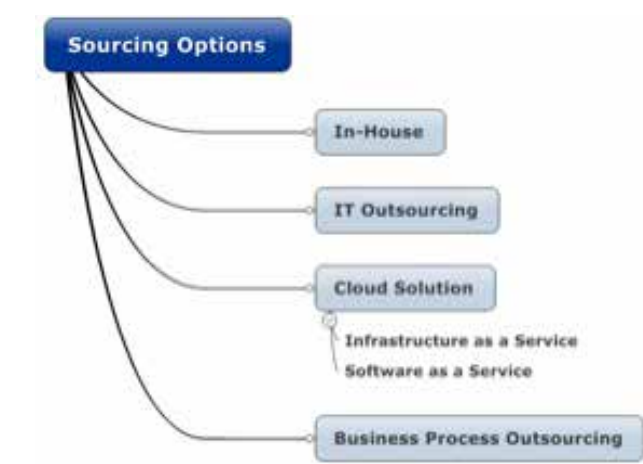
In fact, while there are still few broad-scope Enterprise Resource Planning (ERP) solutions in the cloud, contrary for example to what happened early in Customer Relationship Management (CRM), there has been much progress in the more focused field of Supply Chain Management. This is illustrated by a recent Forbes article [1] and by the emergence of Web sites that compile information about a growing number of commercial solutions [2].

While companies have become able, over a remarkably short period, to consider cloud solutions, there is still relatively little pragmatic advice, as well as real experience, to inform their decisions. The first key questions that decision makers face — and they should indeed address these questions before they let the techies focus on selecting specific technologies or providers — are these: should we be looking at cloud solutions? And if so, what form of deployment should we consider?

A Brave New Sourcing World

To answer these questions, it helps to have a clear mental model of the IT sourcing options that an organization has. The diagram below depicts the current options in a very simple manner. We used to have three options: keep everything in house, move our systems to an outsourcer while having our own people (e.g., the buyers) run the process, or outsource the business process entirely. In the last case, it does not matter much what systems the provider uses, or where those systems are located, as long as the process performance and quality targets are met.

Cloud computing adds a fourth option with two variants: Infrastructure as a Service (IaaS) and Software as a Service (SaaS). There is in fact a third service model, Platform as a Service (PaaS), but this is generally used by software development teams that need a certain environment for a limited amount of time, therefore it is not an option we need to consider for an end user-oriented capability.



The choice between the main options (in-house, ITO, Cloud, and BPO) is usually made, and should be made, on the basis of strategic considerations:

- » Is the business capability in question (such as procurement or logistics) a core competency of the organization and a competitive advantage? If it is, then BPO is out of the question.
- » Does the organization have the maturity to abandon some control over the systems it uses, while maintaining good governance in areas such as enterprise architecture, standards, security, metrics, and vendor management? If not, then any form of outsourcing will be risky.
- » Is there a good, trusting relationship between IT and the business? If not, a move to the cloud is risky for IT, because at the first sign of trouble, the CIO will be blamed for selecting this option.
- » In the table below, which summarizes the benefits and the challenges of the cloud, is the organization able to leverage the advantages while managing the risks?

Benefits

- Rapid deployment
- Elasticity
- Cost proportional to usage
- Self-provisioning
- Professional management and support
- Periodic upgrades
- Applies to many types of resources
- Decreases IT staff needs

Challenges

- Hyped by vendors
- Concerns about availability
- Concerns about security
- SLAs that guarantee little
- Data recovery
- Data residency
- Vendor lock-in
- False business expectations
- Integration across systems

Let’s now make a bold assumption: there are organizations that are keen to obtain the benefits of the cloud, mature enough to understand and manage the risks, enjoy a good IT-business relationship, are able to manage vendors well, and understand the areas of IT governance they need to keep enforcing. This may certainly not be the case of all enterprises, and if any of these characteristics is lacking, then the organization needs to fix its dysfunctions first before considering a move to the cloud; otherwise, we can predict with confidence that there will be trouble.

Let’s focus on organizations that meet those criteria. They all use applications that, while important to their business, are not their core competencies. Let’s be very clear about the distinction between what is and isn’t an SCM core competency:

- » the way the processes are defined and streamlined may be a core competency,
- » the people who execute the process (buyers, manufacturing managers, logistics partners, etc.) may have superior knowledge and ability to execute compared to competitors,
- » the data they use may be unique or contain richer content,
- » but the software application (or applications) that supports the process may be commercial software, with or without a lot of customization, or a homegrown application that does not embody unique algorithms,
- » and the computer systems on which the application runs are certainly not homegrown.

What should these organizations do?

Several of the key decision points are latent within the fourth bullet point in the above list: The questions that need to be asked are those:

- » Is this about adding a new capability (e.g., when starting a new company), or is there a solution already in place in-house?
- » Is usage expected to ramp up significantly over time?
- » If a solution is already in place, is it a commercial package with no customizations, one with significant customizations, a homegrown application, or a legacy product that is no longer supported?
- » Has a lot of money been sunk in software licenses for the existing product?
- » If it is a commercial product, does the manufacturer, or a third party, offer it on a SaaS basis?

A SaaS solution will be most advantageous if the organization is deploying a new capability, or has a small-scale deployment in which it has not sunk much money, but expects to need to scale up significantly; if the software is commercial and not very customized; and if there is a SaaS provider for it. If these conditions are not met, then SaaS may not be the correct model, but this need not imply that nothing can be done. There is still the possibility of migrating the existing environment to an IaaS solution.

Migrating Existing Applications to a Public Cloud

So let us now assume that we have an existing application, perhaps a commercial one for which there is no SaaS provider, or a homegrown system that the organization wishes to keep because it does wondrous things, or because the cost of retraining users would be large. We now move to the question of what steps need to be followed to migrate this application to an IaaS solution.

Let’s first take a look at how this decision impacts the benefits and risks of cloud adoption.

On the benefit side, rapid deployment is no longer an advantage for the software itself, because you are not renting the use of an existing installation, but need to execute the migration. For the same reason, you lose the advantage of receiving automatic upgrades from time to time: if you want an upgrade, you have to apply it yourself. The other advantages remain. In particular, if you need to scale up, you have elasticity at the hardware level (computing power, size of database, etc.). You will also enjoy the professional management of the infrastructure.

On the challenge side, most of the issues remain unchanged, and require the same mitigation measures. The only one that disappears is vendor hype about the application, since it is an application you already use.

At this point, the Cloud Standards Customer Council (CSCC, www.cloud-council.org) rides to the rescue, with a white paper on application migration [3] published in late 2013. The paper complements the CSCC’s Practical Guide to Cloud Computing [4] and prescribes six steps customers should take to ensure a successful migration:

1. Assess the Applications and Workloads
2. Build the Business Case
3. Develop the Technical Approach
4. Adopt a Flexible Integration Model
5. Address Security and Privacy Requirements
6. Manage the Migration

Step 1 involves understanding who uses the application, whether usage is fairly constant or not, etc. There is a big difference between a manufacturer that uses certain raw materials at a constant rate because its plants have a fixed production capacity, vs. a distributor of seasonal goods that needs to buy and ship large amounts during a single month of the year, and much less the rest of the time. Another factor is the frequency at which the application is maintained, since updating a system that is managed by a cloud provider may be more complicated than it was in-house.

Step 2, the business case, is about validating the costs and savings of the migration. Clearly, the migration process will have a certain initial cost. After that, the IaaS environment should not only cost less than the on-premises one (otherwise, there is clearly no ROI), but it is important to assess the total cost of ownership of the solution. Certain on-premises costs tend to be hidden, or rarely estimated. For example, what is the expected life of the hardware on which the application is running? Therefore, how much replacement cost will be avoided, and when? What is the market value of any equipment that might get decommissioned and resold as a result of the migration? Is there a financial advantage to writing off the remaining book value that cannot be recovered, and not having to invest in more CapEx for new hardware to run this application? On the other side of the equation, if the migrated application is a commercial one subject to license fees, how will the migration affect those costs? If you were running the application on a small server, and your cloud provider will run it on a larger machine shared with other “tenants” of their infrastructure, can this increase your license fees? All this needs to be calculated in advance to inform the decision.

If the future environment provides additional capabilities, for example faster remote access from the Internet or even perhaps a mobile access capability that was not provided by the in-house application, what is the monetary value of the additional productivity or process performance? If a mobile interface allows a logistics employee to beat a courier service deadline and get a replacement part to its destination a day early, what is the value of that, and how often might it happen in the course of a year? Once the business case is built, it is important to “socialize” it among business and financial managers, not just among IT managers, so that in the end the decision to proceed is a business decision, not a technology decision, and everyone stands by it if any issues arise during the migration process.

Step 3, 4 and 5 consist of enumerating, planning, and executing a number of technical tasks required as part of the migration. We will not spend time on these – they most concern the project manager, and the CSCC guide is quite explicit about those. Maintaining the integration with other applications, and ensuring security of the data and proper access control, are such

important considerations that the CSCC paper separates them into their own sections, steps 4 and 5. There are no revolutionary techniques involved in these steps, but the shortcuts that one might have taken when the applications were in-house cannot be tolerated when they are migrated to the cloud.

Let us take an example to illustrate this point. Suppose that an application used in the Purchasing department to place orders is made available from a number of physical workstations located in a certain office. If the access control to the application is weak or loosely managed, the consequences may be limited. For example, an employee who left the company on bad terms may not be able to physically enter the area in question in order to lay his hands on an otherwise unprotected system. But once the application is in the cloud, and probably accessed through a Web interface rather than through dedicated client software, the inability to enter the building no longer protects the system from misuse – only a good access control system, with effective “user deprovisioning” procedures, can do it.

Finally, Step 6 is about actually performing the migration, which usually involves a trial run first, followed by an assessment of what went well and what didn’t, the implementation of corrective actions, and finally the real migration and cutover to the cloud environment. This is not something done by IT on its own, but it needs careful collaboration between IT and the business – a choreography of synchronized moves for which the CSCC paper provides a detailed inventory in one of its appendices.

Conclusion

In most cases, starting small and expanding after initial success has been proven as the most prudent approach to application migration to the cloud. It often makes sense to start with the most cloud-ready applications — those with minimal security and privacy risks — or applications that derive the most immediate advantage from the cloud’s elasticity. Enterprises can run a pilot program for one or two of these types of applications, test thoroughly, and gather customer feedback so that improvements can be made before expanding the scope of the effort.

Such efforts tend to take on a very technical, IT-centric focus during their execution. Cloud adopters must remember that the migration to the cloud is primarily a business decision, and should keep it business-focused throughout.

Success is not measured by how many technology acronyms are thrown at the problem: it is measured by whether the organization is able to improve its processes, focus on its core competencies, and use the new sourcing model to respond better to change.

References

- [1] Forbes: “Where Cloud Computing is Improving Supply Chain Performance: Lessons Learned from SCM World.” February 2014. <http://goo.gl/ONc7R9>
- [2] The Supply Chain Cloud: Cloud Computing Solutions for the Supply Chain” www.thesupplychaincloud.com/
- [3] Cloud Standards Customer Council: “Migrating Applications to Public Cloud Services: Roadmap for Success.” December 2013. www.cloud-council.org/wp-download/index.htm
- [4] Cloud Standards Customer Council: “Practical Guide to Cloud Computing.” October 2011. www.cloud-council.org/webPG-download.htm

About the Author



Claude Baudoin is an independent consultant in Information Technology and Knowledge Management based in Austin, Texas. He has 40 years of experience as a software development manager, IT Director, research lab manager, and advisor to C-level executives. His corporate career spanned the IT services, electronics manufacturing, and oilfield

services domains, in France and in the United States. Since retiring from Schlumberger in 2009, he has been applying his knowledge of enterprise architecture, cloud computing, collaboration, social media in the enterprise, and more to various clients worldwide. Claude holds an engineer diploma from Ecole Polytechnique in Paris and an MS degree in Computer Science from Stanford University. He is the author of two software engineering books and of two patents, and a frequent author of conference papers and journal articles.



“United Clouds of Europe” for the Supply Chain Industry

Editorial by Helmut Fallmann, CEO, Fabasoft

As a proudly European cloud provider, I’m pleased that Fabasoft is supporting the European Supply Chain Cloud. Such initiatives are vitally important not only for companies looking for the right cloud solution but for European industry as a whole.

The recent PRISM and NSA revelations have severely damaged the image of US cloud providers and thrown the topics of data security and data protection into the limelight – rightly so. In Europe we should be looking towards independent European standards, as documented in the ENISA guidelines for example. Now more than ever there is a need for a strong, standardised, European cloud market based on common, European values and trust – this is a concept that I like to refer to as the United Clouds of Europe.

If Europe doesn’t want to roll over and concede the cloud computing market to the US, it’s time to act collectively and decisively.

In the US cloud computing has long since established itself as an economic driving force. US online giants Amazon, Apple, Facebook and Google have been focusing on data storage and software in the cloud for a long time, offering customers cheap and simple solutions and IT applications via cloud platforms. With generously dimensioned, nationwide, on-demand infrastructure and services the US has put itself in pole position for global IT business.

If Europe doesn’t want to throw in the towel and concede this future market to the US, it’s time to act collectively and decisively.

European ICT policy needs collective action

Just a few decades ago Europe’s computer industry was bursting with multinational variety. Today virtually nothing is left from the once strong brands of Olivetti, Nixdorf, ICL or Bull. The Americans, in contrast, have taken over the world market with Microsoft, Apple and Hewlett Packard. Europe has only managed to establish a powerful alternative to US industry in air and space travel with Airbus Industries and Arianespace – this has been achieved through cross-country co-production.

At the start of last year US President Barack Obama gave the green light for the extension of the “Foreign Intelligence



Helmut Fallmann - CEO, Fabasoft

Surveillance Act” (FISA), which enables US intelligence services to access all data from non US citizens saved on large, global databases, without the knowledge or consent of the data owner and without judicial approval. Moving away from the media hype surrounding the Snowden affair, businesses should strongly consider where they want their data to be stored and under what data protection laws when evaluating cloud services.

Establishing a European-wide cloud market

Europe needs a powerful action plan to achieve a fundamental consensus between European cloud companies. The call for “United Clouds of Europe” is closely aligned to the “European Cloud Strategy” as part of the European 2020 initiative “Digital Agenda for Europe”. This strategy aims to revamp the European single market into the most competitive ICT market in the world by 2020 on the basis of ultra-fast internet connections.

I believe that there are four virtues for a European cloud solution: Data security, access security, legal security and quality security.

EU Commission demands “European” thinking

The Vice President of the European Commission, Neelie Kroes, responsible for this initiative, has called for “European thinking” in order to fully exploit the multi-billion Euro potential and millions of jobs that cloud computing could bring to Europe. A European approach needs three main steps:

- Consistent standards and certificates for the comparison of cloud services by customers.
- Secure and fair contracts in which the nature of data usage and the responsibility for data ownership and data saving are clearly defined.
- The establishing of a European cloud partnership through which the cloud market can be collectively pushed.

A collective European strategy is a must and work is already in progress with the establishment of the ENISA guidelines and an increasing awareness of and preference towards European solutions. This is a trend that needs to be continued.

I believe that there are four virtues for a European cloud solution: Data security, access security, legal security and quality security. Strong European data protection laws, legal security with clear standard contracts and clear contractual partners, certified minimum quality standards and guaranteed service levels assure high-quality solutions.

Minimum standards and legal security

Europe needs certified minimum quality standards for infrastructure, data security and data protection. Cloud service users must have assurance that their data in the cloud is saved by European cloud providers in European data centres. Additionally, uniform license agreements should achieve additional legal security. End users should be able to easily compare cloud services, know exactly what service they are purchasing and rest assured that these minimum standards are fulfilled.



Protection of digital identities and consistent functionalities

For European-wide usage, providers should ensure that their offerings are multilingual and accessible. Moreover, the best possible protection of digital identities, search functions across all “United Cloud Services of Europe” as well as collective standards for support, monitoring of user experiences and reporting are all key features that need to be included. With the support of digital ID, for example, national ID cards are used to authenticate individuals online as state-verified digital identities.

Openness and interoperability

The decisive factor will lie in an unrestricted openness to new technology “Made in Europe”. Only through a standards-based interoperability of cloud services with single-sign-on and the support of all relevant platforms, mobile end devices and standardised content formats can a large collective market be established for cloud services. Interoperability gives users the freedom of choice to use the optimum combination of tools and services they need and the flexibility to adapt their services packages as it suits them.

The supply chain is a key industry for cloud services

The supply chain industry provides an optimum case study for the implementation of cloud services. There are a number of stakeholders, ranging from large-scale corporations to SMEs, involved in often complex processes. Communication and collaboration is therefore key. The cloud provides the optimum platform for enabling secure communication between different companies across different countries without compromising compliance requirements or the security of internal IT infrastructures. It’s a much cleaner and dynamic form of data management and collaboration as there is one central storage of information protected by controllable access rights. Transparency and traceability replace infinite document versions on multiple mail or ftp servers. Single sign-on replaces complex ftp procedures.

The supply chain industry provides an optimum case study for the implementation of cloud services.

The flexibility and interoperability of cloud platforms also allows hybrid solutions and the agile development of customised applications.

The certificate management application developed for Daimler and Goodyear Dunlop based on the Fabasoft Cloud is a classic example of a specific need that can be quickly and elegantly solved by cloud services. Rather than all stakeholders needing to locally install any software or hardware, the app can be rolled out via the cloud to all those who need it based on a simple subscription model – the essence of an efficient on-demand model.

I hope that this guide gives you a valuable insight into cloud services. Our team are more than happy to provide you with further information so please don't hesitate to get in touch.

Best regards,



Helmut Fallmann
CEO, Fabasoft



Fabasoft Cloud GmbH
Honauerstrasse 4
4020 Linz
+43 732 606162-0
www.fabasoft.com
cloud@fabasoft.com

How Cloud Computing will Revolutionise the European Economy

Today's list of typical pro-cloud arguments is far from complete. In the future, Cloud Computing will enable a broad range of further new possibilities the world has never seen before. Already today it is becoming apparent, that the Cloud is accelerating economy and productivity on a global basis, and that it will change our private and business lives significantly in the time to come. Europe's economic position in a globalized world will strongly depend on the ability to combine and adopt the cloud-based possibilities with the given historical strengths of Europe's industries.

Cloud Computing Today

When you ask Cloud providers about their strongest arguments for the Cloud, you will hear arguments like cost optimisation, higher flexibility, higher agility and – even when often questioned today – higher security. Compared to the given possibilities of a customer's currently existing self-operated IT infrastructure, these arguments appear valid and convincing in the majority of the cases. But at the same time, they are just reflecting the short term effects of Cloud Services, as long as today's IT-capabilities are still being transformed into a cloud-based business model.

The cost optimisation argument appears absolutely valid and can be summarized with the term CAPEX to OPEX. In fact, Cloud customers do not need to invest in their own HW and infrastructure anymore, as they just pay for what they consume. And because the provided Cloud services constantly get maintained and updated to the newest version, customers save on operational costs due to less internal administration efforts.

Even when cloud services provide "just" a unified set of functionalities to all customers alike at the same time, the argument of higher flexibility still counts, since customers are able to access the provided service according to the triple A's: at any time, at any place and with any device. The only need is an Internet connection.

The agility argument appears as a consequence of the achieved cost optimisation and flexibility gain, which often results in company-wide, optimised processes across locations or even with involved partners. While Small and Medium Enterprises would benefit most from these Cloud Services, the adoption rate is behind expectations. SME's quite often fear the loss of control about their data and feel uncertain about cloud security. On the other hand, a wide range of large enterprises and global actors have already implemented the "Private Cloud" within their Intranet, subsequently "cloudifying" their self-operated data centers or by involving Infrastructure-as-a-Service- or Outsourcing-Partners and by adding Public cloud services for specific needs in certain areas. This way, large enterprises have already managed to enable the key benefits from the Private Cloud, both operationally and commercially.

The specific resentment of SME's against the security of Cloud Computing is quite understandable, especially since it is currently amplified by the prominent media coverage regarding Edward Snowden's NSA disclosures. But quite often it is disregarded, that the security level within the SME's self-operated IT stays far behind standards due to limited possibilities of IT- and security investments and the lack of qualified and professional IT expertise at the same time. For them, IT so far was just understood as a tool supporting their core business but rarely became part of an SME's corporate strategy. In opposite to this, for cloud providers IT- and Cloud-security is key for their market acceptance; if they fail on cloud security, their market existence would be endangered. That explains why the security level of Cloud providers is generally higher than in self-operated data centers.





Cloud Computing in the future

The benefits from today's state-of-the-art Cloud Computing in general have been enabled from just the transformation of existing, self-operated, on-premise IT solutions to a cloud-based provisioning model, and of course further enhancements have been added here and there, mainly due to the nature of Cloud as an Internet-based service.

This way, the capabilities of Cloud Computing have not been exhausted yet—quite contrary, the transition of today is just a starting point.

The growth of data related to the Internet were predicted from 1,8 Zetabyte (1021 byte) end of 2011 to about 7,8 Zetabyte by 2015 according to a recent IDC/EMC study¹, out of which 2,2 Zetabyte were cloud related. Cisco² identified a growth of mobile data transfer by 11-fold till 2018 and anticipated, that by 2020 about 50 billion will be connected to the Internet³. Those devices will produce an endless number of sensor data, which needs to be stored, the only place capable to handle such volumes will be the Cloud.

The synonym "Big Data" stands for these endless volumes of collected data. The method of selecting the interesting and relevant data out of these endless volumes, Big Data Analysis, is currently entering the Market and will be broadly implemented in a couple of years. The findings of this Big Data Analysis will lead to new findings and they will accelerate innovation in all industrial branches. Industry 4.0 is the buzzword, representing this innovation process.

When devices of all kind get connected to the Internet, it stands to reason, that applications are required to control these devices, which are not given so far. The development of these new applications of course will also happen in the Cloud, as this is the easiest, cheapest and most efficient way of getting software developed and deployed on a worldwide basis. For the realisation of these new applications creativity is key, which for sure opens broad opportunities for start up's just as for R&D departments of established companies.

The described possibilities will not be restricted to the Industry, similar trends can be identified in all branches and areas of life, terms like Smart Energy, Smart Living, Smart Cities are circulating. Automotive and Mobility, Healthcare and Wellness also can be named; the world is getting smart.

Cloud Computing in Europe

The outline of the 4th industrial revolution on a global basis becomes visible more and more, where Cloud Computing is the enabler and the converter at the same time. But in contrast to former industrial revolutions the Internet will amplify the speed of transformation.

The US and the EU economies are generally almost neck and neck in size (2012: US-GDP4 16,56 trillion US\$, EU-GDP5 12,89 trillion Euro), in the number of companies of all branches (US6 27 Million, EU7 21 Million) and in the number companies among the fortune 5008 (US 29, EU 33).

But when it comes to IT and Cloud, the US is by far dominating. According to PWC's ranking of the Top 100 software companies⁹ 67 were US-based, just 19 EU based. It needs to be questioned, what this dominance of Global Players means for Europe's economy in face of the 4th industrial revolution.

When Commissioner Neelie Kroes introduced the EU Cloud Strategy in September 2012, she stated, there is no question, that the Cloud will come. But she questioned, whether "the Cloud will come to us or with us." The answer is quite clear, but the way to achieve this aim is challenging.

The EU Cloud Strategy¹⁰ outlines actions to deliver a net gain of 2.5 million new European jobs, and an annual boost of €160 billion to the European Union GDP (around 1%), by 2020. Since the NSA scandal happened, Europe's stakeholders seem to identify the return to our own strengths as the only real option. This target will for sure not be achieved when just trying to copy what the US-based Global Players offer.

The chance for Europe only lies in tapping possible synergies of Europe's traditionally strong branches and market segments with the capabilities, provided from, but by far not only restricted to European Cloud Providers.

The main differentiator between European and US cloud offerings relies on safe and fair contract terms with granted service levels and data security and data privacy commitments, all based on harmonized European-wide regulations. Those measures aim for an increased acceptance by European SME's and will be further supported by Certification schemes like the EuroCloud Star Audit, which covers all relevant areas and which will be audited by independent cloud experts.

About EuroCloud Europe

EuroCloud, EuroCloud is an independent non-profit organization and consists of a two-tier setup where every European country can apply to participate in as long as they respect the EuroCloud Statutes. In less than three years, 30 countries have a EuroCloud presence and in 21 European countries a local Eurocloud association is formally established.

For more information visit:
www.eurocloud.org



The cloud value chain needs services brokers

By: Maurice van der Woude,
founder and CEO of BPdelivery B.V.
2014, Renkum, The Netherlands

Introduction

With the emerging of Cloud, it has become less obvious that the parties involved delivering Cloud solutions are capable of taking care of the full value chain themselves. Traditionally, all suppliers want to do all activities by themselves, but let's be honest, it has become impossible to know all about the processes needed behind one delivery.

There is a huge diversity in demand, and the Cloud industry needs to identify that and start working together. It is not necessary to have all expertise under one roof. Why should you? Leave the right expertise to the right experts and start partnerships. Making your company a fixed part of the value chain is more lucrative for a business model than stick to the old market, where we tend to do all ourselves with 50% quality or less. Leaving unsatisfied customers. Do what you do best, and leave the rest to others within your value chain. By being part of a value chain, business comes to you, while you are able to grant business to your chain partners.

The Channel Market

When you come to think of the cloud value chain where resellers are involved, it is easy to say to resellers that they will have to change the way they offer their products. **But every reseller is having the same issues: They understand that they need to change but they have no idea how to do that.** Resellers are no business changers, most of the time resellers have a technical background and pushing them in a more consultancy like role, does not seem to fit. It would be like asking someone who is a custom to walking on sneakers, force him to wear leather shoes. For now it seems safer to stay in their current comfort zone instead of trying something new, with the risk of losing it all. And who can help them with that business change? There are no proven business cases for this. For the distributors it is quite easy to adapt their distribution packages towards cloud, but how do the distributors offer that new package when they have no idea what the business user, standing at the counter of the reseller, actually needs to run his business? And what can be the answer of the reseller, with all his technical knowledge but little knowledge on the customers business processes?

The Service Providers

Service providers will have a difficult time when their customer demands a multiplicity of solutions from different suppliers with different Cloud solutions running on, in the worst case scenario, multiple platforms. And if that service provider only had one customer, things would be easier, but most of the time that is not the case. Service providers want to deliver their technical solutions and do not want to get caught up in all the business processes that are behind one delivery. In the European Small and Medium Business market (SMB) there are a lot of small technical providers that deliver their solutions to their customers, but are having the greatest difficulties in getting the invoices right, or their internal business processes to function as an oiled machine. Service providers leave money on the floor there, where implementation of the administrative and technical business processes would save them a lot of money on a daily basis.

If the above were the only situations at hand, the market could concentrate on solving these particular issues. These issues however, are identifiable by the fact that there may be more parties involved behind one delivery, and delivery does not take place in the traditional one-on-one situation. Where more parties are involved with Cloud deliveries, that is where Cloud Services Brokers can come into play.

A Cloud Services Broker (CSB) plays an intermediary role in cloud computing deliveries and consumption. Cloud brokers make it easier for organisations to consume and maintain their cloud services, particularly when they span multiple parties involved. The Cloud market is about high volumes with small products, because the solutions have to be able to run on any device, anywhere. So not only high volumes play a significant role, also the large variety of solutions affects the value chain. Not every reseller and service provider is capable to handle that on his own.

Cloud Services Brokers

According to Gartner a Cloud Services Broker comes in three flavours:

Cloud Service Intermediation: An intermediation broker provides a service that directly enhances a given service delivered to one or more service consumers, essentially adding value on top of a given service to enhance some specific capability. It may be solutions that connects customer demands and offerings from suppliers. The services from BPdelivery certainly qualify for this. To ensure cloud makes the music, it will need orchestration, not only on a technical level, but certainly on business level where processes need to be carried out in a consistent way.

Aggregation: An aggregation broker service combines multiple services into one or more new services. It will ensure that data is modeled across all component services and integrated as well as ensuring the movement and security of data between the service consumer and multiple providers. These aggregation brokers will exist primarily in the cloud as service providers in their own right, forming a layer of service provisions that approximates the application layer in traditional computing. This aggregation part will be the more technical Broker service.

Cloud Service Arbitrage: Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated aren't fixed. The goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator. In this case the customer will have more solutions to choose from, avoiding the risk of vendor lock-in.

BPdelivery

BPdelivery is a broker service that makes it easy for service providers (internal and external) to provide all their different customers with their products, all at different pricing and pricing models. The unique concept is that BPdelivery is able to provide the full delivery process, from applications to hardware, IP-telephony and the invoicing. Apart from that one of the unique selling points is that BPdelivery does not touch the relationship between the providers and their customers. Also the service comes whitelabeled, so the customer is not even aware of the fact that the full delivery process is carried out by a third party. With this cloud intermediation broker service, all parties involved do what they do best on their own, while service and demand are connected with each other. The true Cloud Broker knows what is going on in the market and knows about the business processes.

Research Area

It is a new market, and Gartner predicted that this market will become a standard somewhere around 2014. BPdelivery believes that evolving this market will be needed to ensure the growth of

Cloud in Europe and beyond. We already identified the need for this kind of broker services and we expect this market to grow on a large scale. A short video on Gartner's vision can be found on BPdelivery (http://www.bpdelivery.com/?page_id=128)

In February 2013, F5 created an extensive whitepaper titled: "Integrating the Cloud: Bridges, Brokers and gateways". Though this whitepaper may look quite technical, the business issues are discussed with the part on Cloud Service Brokers. They identified that the hybrid cloud is the type of Cloud that is used most of the time. It is only logical to derive from that, Cloud brokers are needed to ensure the (inter)operability of hybrid Clouds.

The Value Chain

Before Cloud Services Brokers will become a fixed part of the value chain, Cloud solution providers need to realise that they will fulfill the technical deliveries, where the Cloud Services Brokers take care of the business processes behind it, like adding value and connecting solutions and improvements of the delivery processes itself. In this way the Cloud Value Chain is best served because all parties are doing the things that they do best. The market realises that with the uptake of Cloud solutions, more parties should be involved in the value chain. It will be impossible for one party to cover all the different areas needed, especially when you are active in the Small and Medium Business market.

Do bear in mind that the Cloud Services Broker is not a consultant. A consultant may advise on process improvements, but they do not actually deliver the process improvements. BPdelivery is the party that caters for that and has the business advisors to make sure the right path for your company will be chosen.

