Implementing ERP Systems in the Cloud: Challenges and Solutions

Ahmad Rabay'a
Department of Computer Science
Heinrich-Heine-Universität Düsseldorf
Düsseldorf, Germany
ahmad.rabaya@hhu.de

Kalman Graffi
Department of Computer Science
Heinrich-Heine-Universität Düsseldorf
Düsseldorf, Germany
graffi@hhu.de

Abstract

Cloud computing for ERP provides solutions to the difficulties encountered by conventional ERP systems. This research investigates the accompanying issues of implementing ERP systems using Cloud computing, and introduces solutions to these issues including SLA, standardization, and customers' resistance. The issues have been investigated through an exploratory study and proposed solutions have been introduced, and then validated based on data from the Cloud Security Alliance (CSA). The results of this research are simplified assembling of issues, best practices, and specifications toward implementing ERP in a cloud. The research results include: SLA is a necessary contract, but it is not sufficient, as more auditing and checking procedures must be added to the SLA to assure availability and redundancy of offered services. Moreover, bigger vendors did not welcome a standard for ERP in a cloud, and they might get convinced by standardizing only the core part of ERP in a cloud. Finally, there are different views about the potential resistance toward ERP in a cloud, but services that would let customer try the systems before purchasing them could help overcoming this resistance. The results of this work should help the market and researchers get a better view about ERP in a cloud.

***Keywords**: **Enterprise Resource Planning, Cloud Computing, Cloud Security Alliance, ERP standard, Interoperability, Cloud Security**.*

1. Introduction

Information is the most valuable asset for enterprises; it helps companies keep track of their business, customers and stakeholders [1]. Enterprise Resource Planning (ERP) is a business management software which helps organizations manage their various departmental information, more details are in figure (1) [3]. The significant improvement results from using ERP systems emerges it as a vital tool for most organizations [2]. However, ERP systems are costly, time-consuming to implement, and enclose high risk of failure and disruption to the customer's business. This introduces difficulties prevent many companies from setting up ERP systems. Researches try to investigate the potential benefit of using cloud computing to implement ERP systems with less cost, time, and risk consequences. Cloud computing is a new technology trend defines as a "model for enabling convenient, on-demand access to a shared pool of computing resources (e.g., servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort" [5]. Cloud computing is categorized into different services (IaaS, PaaS, SaaS), as illustrated in figure (2), which are delivered and consumed in real-time over the Internet using only web browsers [8].

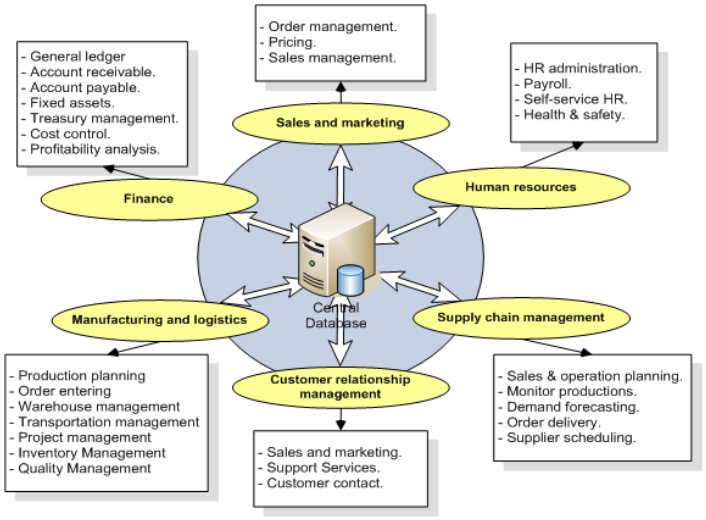


Figure (1) – ERP Modules

Cloud based systems deliver a comprehensive set of business benefits to the market over traditional systems, such as: fast and easy deployment with no need for extensive IT experiences, or build large IT backbone infrastructure. Scalability where organizations can scale up or down their IT infrastructure according to their consumption needs, and distribution of cost through multi-tenancy [9][4]. IT managers are finding cloud computing easier to use and deploy thus further reducing time and cost of meeting business needs with robust, on demand applications [10]. Figure (3) illustrates the

interrelation between the cloud layers, and how the roles of the various actors [11].

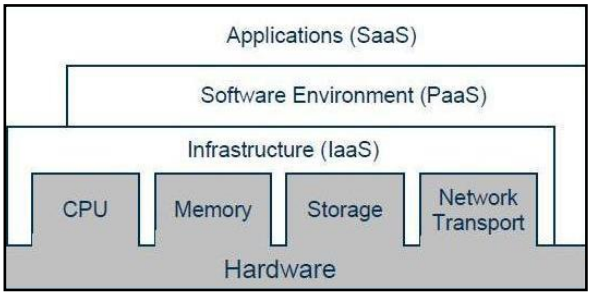


Figure (2) – Cloud Architecture [5]

1.1 Motivation

While ERP in a cloud offers customers many potential benefits, there are some concern issues that customers must consider before implementing the system. The driving force behind this research is based on overcoming these concerns to gain the potential benefits of using cloud computing in ERP. The market views towards these issues are addressed in this paper through an exploratory study. Then the results are validated by the Cloud Security Alliance. The research final results will help understand the customers' requirements to protect the customers and reduce their fears toward the cloud.

1.2 Aim and objectives

This research aims to investigate the main challenges that are restraining the market from implementing ERP systems in the cloud, and propose solutions to these challenges. The results of this research are simplified assembling and filtering of issues, proposed solutions, and specifications toward implementing ERP in a cloud based on data from the CSA. The research questions, which are answered in this research:

1. ***How important is the service level agreement (SLA), and whether it is enough contract between cloud service provider and customer?***
2. ***How a standard for ERP in a cloud could affect service suppliers, and whether customers lock-in and switching cost are enough drivers for adopting the standard.***
3. ***What makes ERP in a cloud gain resistance from customers, and how to give customers trust on cloud.***

This paper is divided into sections; section 2 addresses the theoretical background, section 3 describes the research methodology. An analysis of the market view is introduced in section 4, followed by proposed solutions and results validation in section 5 and 6 respectively. Finally, section 7, 8 introduces validity of results and conclusion respectively.

2. Literature review

Service level agreement (SLA) should be written to enforce service quality, availability, performance and stability of the offered services by cloud providers. The Software and Information Industry Association (SIIA) has published recommendations that SLA should be written to establish base for monitoring performance, indentify what is being measured and how, in addition to the number of times an incident may occur before being considered as inveterate [8]. All these points should be included in the SLA to emphasize its role as a sufficient contract between both customers and providers.

Ideally, standards enhance compatibility, interoperability, accelerate acceptance of new technologies, and generate greater value for users. The ideal picture of ERP in a cloud standard is to enable cloud users to choose the modules they prefer from the vendor they trust and integrate them together with further promises to ensure data and application integration across clouds [10]. ERP service providers tend to offer differentiated services from other vendors to get a better competing position and attract customers, but such a common standard may take this away from them, and makes it harder for vendors to differentiate their products and still comply with the standard [9]. Reaching a level of ERP standardization may theoretically let smaller vendors adapt quickly and start competing with big vendors. However, this is still dependent upon decoupling the enterprise systems into interface-ready modules, which means ERP platforms need to be reengineered and lots of time and resources required from vendors to enhance their ERP systems [2]. Therefore, such a standard might face resistance from the ERP market leaders, as they may be at risk of losing their leadership, while small players would welcome such a standard [11]. On the other hand, customers lock-in and switching cost are main drivers for adopting an ERP in a cloud standard [9]. The high switching cost, in addition to the risk of a substantial disruption, and data unlikely to transfer perfectly between ERP systems, made the corporate information officers (CIOs) think long and hard about changing ERP systems [12]. Taking advantage of the various ERP systems offered by different vendors gives customers more options and potentially less risk of being locked in, if the modules from the different vendors are standardized, interoperable, and easily integrate with each other [16]. Interoperability relies much on the need of well-defined standards inside and between clouds. The situation today is that clouds are treated individually as providers have their own APIs because there is no unified standard available to ensure interoperability between different clouds [14][15].

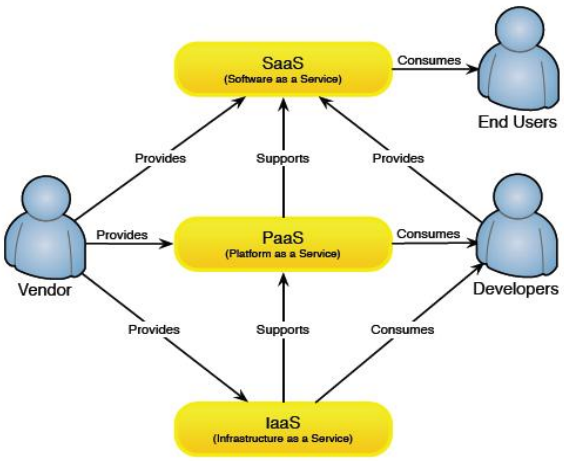


Figure (3) – Cloud layers of abstraction.

Regarding customer's resistance toward ERP in a cloud, based on the theory in [6][14][13] resistance is mostly about the security, privacy, reliability, and portability of the ERP in a cloud. The idea of users outsourcing their data outside the corporate firewalls into cloud servers, which potentially could reside anywhere in the world, along with the ease the cloud hosting companies can access the customers' data, are the rational drivers of customers' concerns towards the cloud. Moreover, ERP in a cloud is changing the nature of the way businesses do their work, shifting the work load from internal system operations toward services accessed through web browser. This change in the ordinary work practice faces resistance from customers [6]. Furthermore, cloud computing multi-tenancy option, where the same cloud instance supports multiple customers simultaneously, is considered as a risky and scary option [14]. Even though multi-tenancy improves the utilization and reduces the overall cost of the system, there are still doubts regarding the customer's data privacy [7][8].

To address these challenges of cloud computing, several groups are developing specifications and best practices for cloud computing, such as the Cloud Security Alliance, which supports development of open standard for cloud-based computing. Cloud Security Alliance (CSA) is a non-profit organization with a mission to promote the use of best practices for providing assurance within the cloud. CSA is led by a coalition of industry practitioners, corporations, associations and other key stakeholders to provide industry-accepted ways for documenting controls exist in the cloud (IaaS, PaaS, and SaaS) offerings [15]. The deliverable of the CSA is the Consensus Assessments Initiative Questionnaire (CAIQ). The CAIQ provides a series of "yes or no" control assertion questions, which are tailored to suit each unique cloud customer's requirements. The questionnaire covered 15 areas of concerns a cloud customer may wish to ask of a cloud provider, in order to provide fundamental principles to guide cloud vendors, and assist prospective cloud customers in assessing the overall security risk of a cloud provider. The questionnaire has been developed with contributions from over 50 professionals and industry experts [15]. The analysis of the questionnaire helps getting better understanding of the market view towards the cloud service offering.

3. Research method

This research investigates the market view toward ERP in a cloud. It spans from study of the knowledge base about ERP in a cloud, interviews a sample of ERP suppliers and buyers, analyzes and compares the interviews, then validates the results based on data from the Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ). Despite it was very difficult to get hold with companies for interviews, we managed to cover all the industrial sectors with the contacts who were willing to cooperate and contribute to our study. The selected participants in the sample were chosen to cover the different supplier and buyer types. The vendors sample represents 3 different types of ERP suppliers; big ERP vendor, with customers all around the world, smaller vendor, with less range of customers, and an ERP service provider that mainly serves small and medium-sized companies. On the other hand, the buyers interviewed during this research represent 3 different industrial sectors: distributers, manufacturers, and assets intensive firms. All the selected participants in the sample have management responsibilities in their firms; on ERP supplier's side, the participants were either product or marketing managers, and from the customer's side the participants were IT managers and CIOs.

Oral survey was chosen to get thorough opinions and impressions from the respondents [16]. Both ERP suppliers and buyers were included in the sample and interviewed about their views toward applying ERP in a cloud. The oral survey was made over the telephone with the selected interviewees. The interviews were varied on time, between 30 – 90 minutes. The interviews are summarized in the Table - 1.

Role	Company	Country	Interviewee	Duration
Supplier	Lawson	Sweden	Product Management	50
	Medius		After-sales Manager	50
	SYSteam		Product Manager	40
Customer	Bejoken	Sweden	Product & IT-Manager	60
	Eldon		CIO	60
	Sapa Group	UK	MIS Manager	30
	SAS Tech AB	Sweden	CIO	90
	Cloetta		IT Manager	45

Table (1) – Summary of the interviews

4. Analyzing the Market

The vendors interviewed during this study represent 3 different types of ERP suppliers. Lawson considers a big ERP vendor and has customers all around the world. Lawson is an actual Cloud ERP provider, and already have their ERP solution deployed to the cloud. Furthermore, Medius considers a smaller vendor with less range of customers, mainly in Sweden, and SYSteam is an ERP service provider mainly serves small and medium-sized companies. On the other hand, the buyers interviewed during this research represent different industrial sectors. Bejoken, Eldon, Sapa, and Cloetta consider distributers, while Eldon, Sapa, and Cloetta consider manufacturers, and Sapa and SAS are assets intensive firms. By holding these interviews, we investigated issues related to the market view toward ERP in a cloud. The summarize results of the conducted interviews are as following:

Regarding the SLA point, all participants agreed on the necessity of SLA between customers and suppliers. The three vendors agreed that it is an enough secure contract for what the customers bought, and expected level of service. However, customers agreed that it is necessary, but not enough, as more emphasis penalties and checking procedures must be added to assure the offered service. Figure (4) demonstrates the

interviewees' answers regarding whether SLA is necessary and enough or not.

For the ERP cloud standardization point, smaller vendors backup an ERP cloud standard that supports security and interoperability; however, bigger vendors do not welcome such a standard or believe in the possibility of achieving it. It was expected and reasonable that both Medius and SYSteam (considered as small vendors) would support an ERP in cloud standard, and they believed that such a standard will gain resistance from big vendors or at least they will not cooperate with it. This was obvious from Lawson's respond toward such a standard as they were not interested neither supportive for it. Moreover, all the interviewed customers supported a standard for ERP in a cloud, and agreed about its benefits. However, customers' views were varied from positive about the possibility of achieving it, to doubts if this would be possible overall. Bejoken, Eldon, Sapa and STS believed on the possibility of having such a standard and being theoretically and financially feasible. On the other hand, Cloetta did not believe in the possibility of achieving such a standard, as they thought that the market is far from being standardized. Figure (5) demonstrates the interviewees support for the idea of ERP cloud standard or not. Figure (6) demonstrates the customers' views about the possibility of achieving such a standard.

The participants' views regarding the customers' potential resistance toward ERP in a cloud were varied. One of the vendors (Lawson) believed that their offering would not face resistance as it would improve security, availability and disaster recovery comparing to traditional environment. The other vendors mentioned other issues mainly about the security between the client and the cloud, and the user's resistance to change. With regards to customers' views about the potential resistance, they were concerned mainly about that ERP in a cloud is still unknown, and less concerned about the availability, security and privacy issues, as they believed vendors will be able to handle them in their offerings. Figure (7) demonstrates the views regarding whether there is resistance toward cloud computing or not.

Moreover, multi-tenancy still not widely offered by vendors, as customers thought of multi-tenancy as a scary option, as illustrated in figure (8).

One surprising issue was found that most of the interviewed customers had no experience with any cloud services. Except Cloetta who is currently using email for local workers as SaaS, the rest of the interviewed customers have not used any cloud services in their business before. However, a participant from Bejoken assured – despite their doubts:

> *"It's a matter of 10 years; we will use the cloud for almost everything".*

Figure (9) demonstrates whether customers have used any cloud services before or not.

Many of the results were varied between the suppliers' and buyers' point of views. This variation was driven by many potential reasons, could be briefed by:

- ERP in a cloud market is not matured enough, as there is no ideal accepted definition for it, in addition to many debates about the service requirements, advantages and shortcomings.
- The absence of an ideal accepted definition for ERP in a cloud introduced many different variations of the services offered by the vendors, who all claimed that their offering is compatible with one of the cloud definitions. It was noticeable that vendors favor their own offering over customers' needs, as every vendor claimed that their offered system is the best for the customers.
- Customers do not have matured knowledge about cloud computing, which reflected from the variations of their responses toward the service. Most of the customers were scared of this new technology and how it might affect the already operating ERP system. Moreover, most of customers went through a tough journey to implement ERP systems, and they are not willing to risk such a crucial system and rush into the cloud which they consider not matured enough.

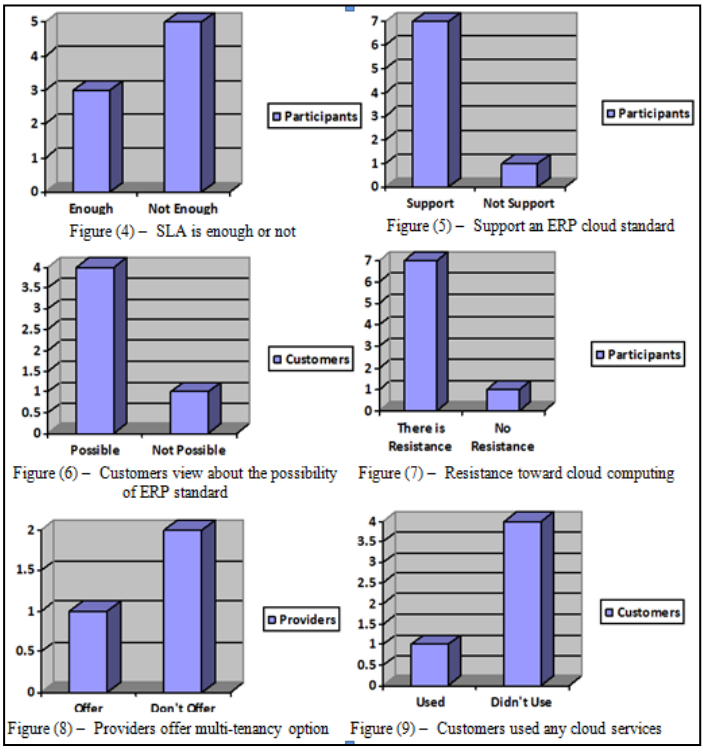


Figure (4) – SLA is enough or not

Figure (5) – Support an ERP cloud standard

Figure (6) – Customers view about the possibility of ERP standard

Figure (7) – Resistance toward cloud computing

Figure (8) – Providers offer multi-tenancy option

Figure (9) – Customers used any cloud services

5. Proposed solutions.

In this section proposed solutions for the investigated issues are introduced. These proposed solutions despite being theoretically feasible, and could give customers more freedom. Practically, there is no proof how likely the solutions will work out for vendors and customers.

Regarding the issue with SLA, despite the general agreement that SLA is a necessary contract between customers and suppliers, customers did not think it is enough. SLA needs to be regularly monitored and measured from both sides - sometimes third party, and more points and penalties must be

added to ensure the availability, financial benefits, backup, and quality of the offered service.

For the standardization issue, even though customers and small vendors would support an ERP in a cloud standard, bigger vendors and market leaders do not believe or welcome such a standard. The proposed solution is to standardize the core of the ERP in a cloud, where providers might provide the basic standardized core, and offer any distinct customized modules on top of that core. This way, customers will have standardized interoperable solutions, and providers still can offer a differentiated service and still comply with the standard.

Regarding the customers' potential resistance toward ERP in a cloud, to overcome the customers' resistance and give customers more trust on the cloud, vendors must show real examples for ERP in a cloud. Options such as the "Test Drive" service offered by "Lawson", which makes it possible for the customers to try ERP in a cloud system before purchasing. It allows customers to test real ERP in cloud system using their own business processes and data. More offered services like the "Test Drive" might give customers more confident and reduce their fear and resistance toward ERP in a cloud.

6. Results validation with CSA

To validate the found results of the market analysis introduced in section 4, CSA Consensus Assessments Initiative Questionnaire was applied. Four of main cloud computing providers participated in the questionnaire, which are; Capriza, Devellocus, Everbridge, and OneLogin.

Capriza provides a turnkey solution for enterprises to mobilize their business applications. Devellocus provides cloud-based software solutions for the retail, healthcare and financial industries. While Everbridge provides a unified communication suite that helps clients make decisions, and respond quickly during disruptive events. Furthermore, OneLogin Enterprise Identity Management solution provides a platform for managing user identities in the cloud, across all of their devices [15]. Here are the validations of the found results based on data from the CAIQ:

Regarding the issue with SLA, the CSA has a special attention for the SLA as more auditing, checking procedure, and penalties are suggested to be introduced to the SLA, which confirms with our finding in the exploratory study, as CSA suggests that there should be procedures for maintaining complete, accurate and relevant SLA between providers and customers, which ensure providers' adhere to customers information security and privacy policies. System performance shall be monitored and tuned to meet regulatory, contractual and business requirements. Moreover, cloud providers' audit plans shall be developed to address business disruptions, and security operations. Audit activities must be agreed upon prior to executing, and tenants shall be allowed to view audit reports. Most of the participated providers maintained these points in their SLA and answered with yes to the questionnaire.

In addition, SLA should manage conflicts or inconsistencies in the service, annually review all agreements, and legal counsel review all third-party agreements. All providers review all agreements at least annually, however only Everbridge and OneLogin manage conflicts or inconsistencies in SLA. On the other hand, only Everbridge and Capriza have legal counsel to review all third-party agreements.

For the ERP cloud standardization, CSA support toward a cloud standard for security and interoperability can be summarized that APIs shall be designed, developed, deployed, and tested in accordance with leading industry standards. In addition to information security and privacy policies, data security architecture, and incident response plan should comply with industry standards. All providers have their APIs and information security and privacy policies comply with industry standards. Moreover, policies and procedures shall be established in support of data security and capability to timely detect and response to attacks that target the virtual infrastructure. As well as system and network environments shall be protected by firewall, and have anti-malware programs to ensure security requirements. Controls shall be in place to prevent unauthorized access to your application, in addition to monitor privileged access for privacy breach. Security vulnerability scans should be conducted regularly as prescribed by industry best practices. Encryption methodologies should be provided within the cloud environment to encrypt and protect tenant data and virtual images, and protect the tenants data if moves through public network. All providers have applied all the previously mentioned security mechanisms, controls, and tools, while the capability to timely detect and response to attacks targeting virtual machine was not applicable for both Devellocus and OneLogin, and the last mentioned is the only provider didn’t have an anti-malware programs. On the other hand, physical security should be implemented to maintain a safe and secure working environment. Access to secure areas shall be constrained and monitored by physical access control mechanism. All the providers offered the previously mentioned physical security mechanisms,.

Policies and procedures shall be governing the providers' use of APIs for interoperability, and migration of data. APIs shall be developed and deployed in accordance with leading industry standards and adhere to legal or regulatory compliance obligations. Providers shall use open and published APIs to ensure support for interoperability, and publish a list of all APIs available in the service and indicate which are standard and which are customized. Moreover, providers shall use industry-recognized virtualization platform and format to help ensure interoperability. Virtual machine shall be allowed to be downloaded and ported to a new cloud provider, and all data shall be available in industry-standard format. In addition to have a secure industry accepted network protocol for data import and export. All providers confirmed that their APIs complied with industry standards, however, only Everbridge and OneLogin have policies governing the use of APIs for interoperability, and migration of data. Furthermore, all providers except Capriza used and published APIs to ensure support for interoperability. On the other hand, only Everbridge and Capriza used industry-recognized virtualization platform and format, and only Everbridge allowed virtual

Point	*Vendors*	*Customers*	*Cloud Security Alliance*
SLA as a contract	All Agreed	All Agreed	Conforms
SLA is an enough	Enough	Not Enough - more penalties and checking procedures must be added.	Not Enough - more auditing, checking, and penalties have to be introduced to the SLA.
ERP cloud standard	Smaller vendors support, bigger vendors did not welcome such a standard	Support a standard	Support toward a cloud standard
Cloud Security Standard.	All vendors support.	Support with positive view about achieving it	Support of data security policies and procedures.
Interoperability Standard.	Smaller vendors support, however, bigger vendors resist such a standard	Support with doubts if this would be possible.	Support of policies and procedures for governing the providers' use of APIs for interoperability.
Customer Resistance	Different views about the potential resistance	Not concerned about the availability, security and privacy issues	Focused on how to avoid and mitigate this resistance, rather than the varied sources of it.
Multi-tenancy	Most vendors do not support it in their service	Think of it as a scary option	Providers shall ensure security, privacy, and isolation of sensitive data.
Examples or scenarios	Offered as a service by one provider called "Test Drive".	Suggested by customers.	Focused on providing documentation that describes scenarios.

Table (2) – Summary of the results validation with CSA

machine to be downloaded and ported to a new cloud provider. Both Devellocus and Everbridge provided all data in industry-standard. However, Capriza was the only provider who was not having an industry accepted network protocol for data import and export, while all the others complied with that.

Moreover, on regards to the customers' potential resistance toward ERP in a cloud, the CSA focuses on how to avoid and mitigate the customers resistance toward ERP in a cloud. The CSA suggests that providers should provide tenants with documentation describing the Information Security Management Program that includes administrative, technical, and physical safeguard to protect assets and data. In addition to documentation describes the quality assurance process, and what they vs. their tenants are responsible for during security incidents. Moreover, providers should maintain safe and secure working environment, and allow tenants to monitor physical and logical control status, and view the third party audit reports. All the providers complied with the mentioned points, however, only OneLogin and Capriza allowed tenants to view audit reports and published what they vs. their tenants' roles and responsibilities. On the other hand only Devellocus did not allow tenants to monitor the control status.

On the other hand CSA recommends that tenants should be allowed to perform independent vulnerability assessment, and providers should make the results of the vulnerability scans available to tenants, in addition to provide tenants with separate environment for test processes. All providers gave their tenants the previously mentioned options, except Everbridge did not allow their tenants to perform independent vulnerability assessment, and OneLogin did not make the results of the vulnerability scans available to tenants.

Regarding multi-tenancy, the CSA's view toward it confirms with what we have found from the exploratory study. Based on the Cloud Security Alliance, policies and procedures shall be established that multi-tenant organizationally-owned or managed applications and infrastructure shall be developed and deployed such that customer's access is appropriately segmented from other tenant users. Taking into consideration isolation of business critical assets or sensitive user data, and compliance with legal and regulatory compliance obligations. Moreover, system and network shall be protected by a firewall or virtual firewall to ensure business and customer security and privacy requirements, and separation of production and non-production environments. All providers complied with the previously mentioned view toward multi-tenancy except Devellocus who found them not applicable for their offering.

To apply these suggestions customers have to make sure that SLA satisfies their various requirements, by regularly check and measure the SLA, or have a third party to do that for them. Moreover, audit plans shall be developed, and penalties must be added. That way customers can make sure to have and maintain a complete, accurate and relevant SLA, which adhere to their availability, security, privacy, and all other requirements. On the other hand, providers must standardize the core of their ERP in a cloud, and offer any distinct customized modules on top of that core. All APIs shall be developed in accordance with leading industry standards, in addition to information security and privacy policies to ensure interoperability and security. All data shall be available in industry-standard format, in addition to have a secure accepted network protocol for data import and export, and encryption methodologies provided within the cloud and through public network. That way providers can have their own ERP systems, and still comply with the security and interoperability standard. Finally, to give customers trust on the cloud, vendors must show real examples for ERP in a cloud using services that makes it possible for customers to try real ERP systems using their own business processes and data. Moreover, providers shall provide tenants with documentation describing the information security administrative, technical, and physical safeguard, and allow tenants to monitor physical and logical control status, and view the third party audit reports. By successfully applying these suggestions, it is expected that the result will have a great impact on the area of applying cloud computing for ERP. The ERP market might benefit from cloud computing to implement ERP systems with less implementation cost and time, and failure risk consequences, which would have a great impact on both industrial and academic sides.

7. Risk on validity

Getting hold with companies for interviews was very difficult, as most of the companies were either busy, or not willing to share the information they have. The selected participants in the sample were chosen to cover the different industrial sectors. We succeeded at some points, but eventually we interviewed all the contacts that responded and were willing to contribute for this work each within their area of expertise and responsibility. The validity of the results in section 4 might be affected by many factors like personal experiences, different contexts, or bias for their own firms. Furthermore, the participants' views demonstrated only one person's view at each organization, which might be affected by the participant personality, age, position, and social background. On the other hand, the results validation in section 6 was based on the Cloud Security Alliance CAIQ, which is the delivery of one of the standards groups developing specifications and best practices for cloud security. Despite that the Questionnaire has been developed with contributions from over 50 professionals and industry experts [15]. There is a risk to the validity based on data from CSA, because it is focused on general cloud standard security issues, while the study is focused more on the role of cloud computing to implement ERP in a cloud, which makes the results of the study not applicable for small systems implemented by the cloud. Moreover, the results of the exploratory have been validated based on only the CSA specifications, with only four providers participated on the CSA questionnaire.

8. Conclusions

This research was based on telephone interviews with main ERP players in the market from both sides - customers and suppliers. By holding these interviews, we investigated issues related to the market view toward the combination of ERP in a cloud computing. During this research many issues were investigated, and varied results have been acquired. Furthermore, proposed solutions for those issues were introduced, even though, practically, there is no proof about how feasible actually these solutions will be, and how likely the solutions will work out for both vendors and customers. The found results have been validated based on the CSA Consensus Assessments Initiative Questionnaire, which was answered by four of main cloud computing providers.

Despite the general agreement between all the interviewees that SLA is a necessary contract between customers and suppliers, customers did not think it is enough. SLA needs to be regularly monitored and measured from both sides – sometimes third party. As well as, more emphasis penalties and checking procedures must be added to assure availability and redundancy of the service offered by the supplier. The CAIQ conformed about the need for procedures to maintain complete, accurate and relevant SLA agreement between providers and customers. As well as more auditing, checking procedures, and penalties have to be introduced to it, which confirmed with our finding in the market exploratory study. Moreover, smaller vendors would support an ERP in a cloud standard that supports security and interoperability; however, bigger vendors did not believe or welcome such a standard. On the other hand, the interviewed customers supported such a standard, and agreed about its benefits with varied views about the possibility of achieving it. CSA supported such a security and interoperability standard and assured that APIs shall be designed to comply with leading industry standards, in addition to information security and privacy policies. Moreover, system and network environments shall be protected by firewall and have anti-malware programs. Security vulnerability assessment tools shall be used, and controls shall be in place to prevent unauthorized access to the application. On the other hand, physical security should be implemented to maintaining a safe and secure working environment. Policies and procedures shall be governing the providers' use of APIs for interoperability, as APIs shall be designed in accordance with leading industry standards and adhere to regulatory compliance. Providers shall use open and published APIs to ensure support for interoperability, in addition to have a secure industry accepted standard network protocol for data import and export.

Finally, the interviewed participants from both sides had different views about the potential resistance from customers toward ERP in a cloud . Moreover, multi-tenancy was still not widely offered and considered a scary option. CSA focused more on how to avoid and mitigate the potential customer resistance toward ERP in a cloud, and suggested that providers should provide tenants with documentation describing the Information Security Management Program and specify what they vs. their tenants responsibility during security incidents. The CSA's view towards multi-tenancy confirmed with what we have found from the exploratory study, that multi-tenant applications and infrastructure shall be designed taking into consideration isolation business critical assets or sensitive user data.

The proposed solutions to the mentioned issues are by making sure that SLA is regularly checked and monitored by both sides – sometimes third party, and more emphasis penalties must be added to guarantee the offered service. Moreover, standardizing the core of the ERP in a cloud, where providers might provide the basic standardized core, and offering any distinct customized modules on top of that core. On the other hand, options that make it possible for the customers to try products before purchasing will increase customers' confidence, and reduce their fear and resistance toward the new systems on the cloud.

The validity of these results might be affected by many factors such as; the difficulty of getting hold with companies for interviews, the market exploratory study demonstrated only one person's view. As well, the acquired results have been validated based on the CAIQ, which is the delivery of only one of the cloud standard groups, with only four providers have participated on the questionnaire. Lastly, CSA focuses on general cloud standard security issues, but the study focused more on issues related to ERP in a cloud.

References:

[1] Chung S., Snyder C. (1999): *ERP initiation - a historical perspective*, Proceedings of Americas Conference on Information Systems; Milwaukee, Wisconsin. 213-15.

[2] Yen D.C., Chou D.C., Chang J. (2002): *A synergic analysis for Web-based enterprise resources planning systems*, Computer Standards & Interfaces 24. 337– 346.

[3] Sharif A.M. (2010): *It's written in the cloud: the hype and promise of cloud computing*, Journal of Enterprise Information Management Vol. 23 No. 131-134.

[4] Prawirakusumah C. (2009): *GS10 – Cloud Computing*, IBM Boeblingen Design Center.

[5] Ohlman B., Eriksson A., Rembarz R. (2009): *What Networking of Information Can Do for Cloud Computing*, WETICE '09. 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises. 78–83.

[6] Callewaert P., Robinson P.A., Blatman P. (2009): *Cloud computing: forecasting change*, Market overview and perspective, Deloitte Consulting, Belgium.

[7] Rimal B.P., Choi E., Lumb I. (2009): *A Taxonomy and Survey of Cloud Computing Systems*, NCM '09. Fifth International Conference on INC, IMS and IDC. 44 - 51.

[8] Kapil M. and Pratap A., Cloud Computing in ERP Systems, VSRD-IJCSIT, Vol. 1 (1), 2011, 22-28.

[9] Shapiro C., Varian H.R. (1999): *Information rules: a strategic guide to the network economy*, Harvard Business School Press, Boston, Massachusetts.

[10] Dikaiakos M.D., Katsaros D., Mehra P., Pallis G., Vakali A. (2009): *Cloud Computing: Distributed Internet Computing for IT and Scientific Research*, Internet Computing, IEEE. 10 – 13.

[11] Westelius A. (2009): *The business logic and enterprise systems ventures – the enterprise system as a political tool*, 23rd Annual Australian and New Zealand Academy of Management Conference (ANZAM 2009), Melbourne.

[12] Beheshti H.M. (2006): *What managers should know about ERP/ERP II*, Management Research News, Vol. 29, 184-193.

[13] Maggiani R. (2009): *Cloud Computing Is Changing How We Communicate*, IPCC 2009. IEEE International Professional Communication Conference. 1 – 4.

[14] Gellman R., (2009): *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, The World Privacy Forum, Version 1.1. 1 – 26.

[15] Cloud Security Alliance at, https://cloudsecurityalliance.org/ March 10th 2015

[16] Baker H.K., Mukherjee T.K. (2007): *Survey research in finance: views from journal editors*, International Journal of Managerial Finance, Vol. 3 Iss: 1.11 – 25.