ICT Governance Acquisition Requirement Principle: Toward the Selection of the Suitable Exploitation Mode of a Secure e-Business Architecture for Small and Medium Enterprises

Khadraoui, Djamel and Christophe, Feltus

Public Research Centre Henri Tudor

13 July 2009

ICT Governance Acquisition Requirement Principle: Toward the Selection of the Suitable Exploitation Mode of a Secure e-Business Architecture for Small and Medium Enterprises

Djamel Khadraoui, Christophe Feltus

Public Research Centre Henri Tudor, 29, Avenue John F.Kennedy,
L-1855 Luxembourg-Kirchberg, Luxembourg
(e-mail: christophe.feltus@tudor.lu)

Abstract:

The importance of the Governance of IT is becoming more and more important in the enterprises especially since the accounting scandals of 2002 and more currently through the ongoing market crisis. While all political leaders say that the world economy's is at grave risk, development are done to firstly elaborate appropriate framework to enforce and guarantee the stability of the financial sector and by extension to all sectors of the industrial economy and secondly, to enhance the governance all of these public and private companies. Sarbanes-Oxley is one of these laws that aims to provide guarantees over the company's accountability. The ISO/EIC 38500 [14] is one standard that provides a framework for effective governance of IT. This framework provides guiding six principles: Establish responsibilities, Plan to best support the organization, Acquire validly, Ensure performance when required, Ensure conformance with rules and Ensure respect for human factors. The principles "Acquire validly" aims at ensuring that the acquisition of IT components and of the exploitation mode is realized with the assurance that it is aligned with the business strategy
A lot of SME from the industrial but also from the financial sector is still unable to correctively choose the optimal compromise for exploiting their e-business solution regarding their business needs. Effectively, choosing the best way for an IT infrastructure exploitation accordingly with the security requirement is a professional activity that can't always be appropriately conduct by a SME staff. Although a lot of criteria influence the exploitation mode to be chosen – independency regarding an IT company, cost and profitability of the solution, technology used – security remain the major influencing factor.
This document has for objective to analyse the aspects of security measures related to the e-business, according to the geographical place of the e-business architecture: in the company itself, outsourced, or an intermediate place between those two. The first part of this document defines what we understand by "exploitation mode", the second analyses the security aspects related to each component of an e-business architecture according to its exploitation mode, and finally the last part makes an analysis of the security of general architecture, always according to its exploitation mode.

Keyword: e-Business, Small and Medium Enterprise, Security, Exploitation Mode, ICT Governance, Acquisition Principle.

1 Introduction

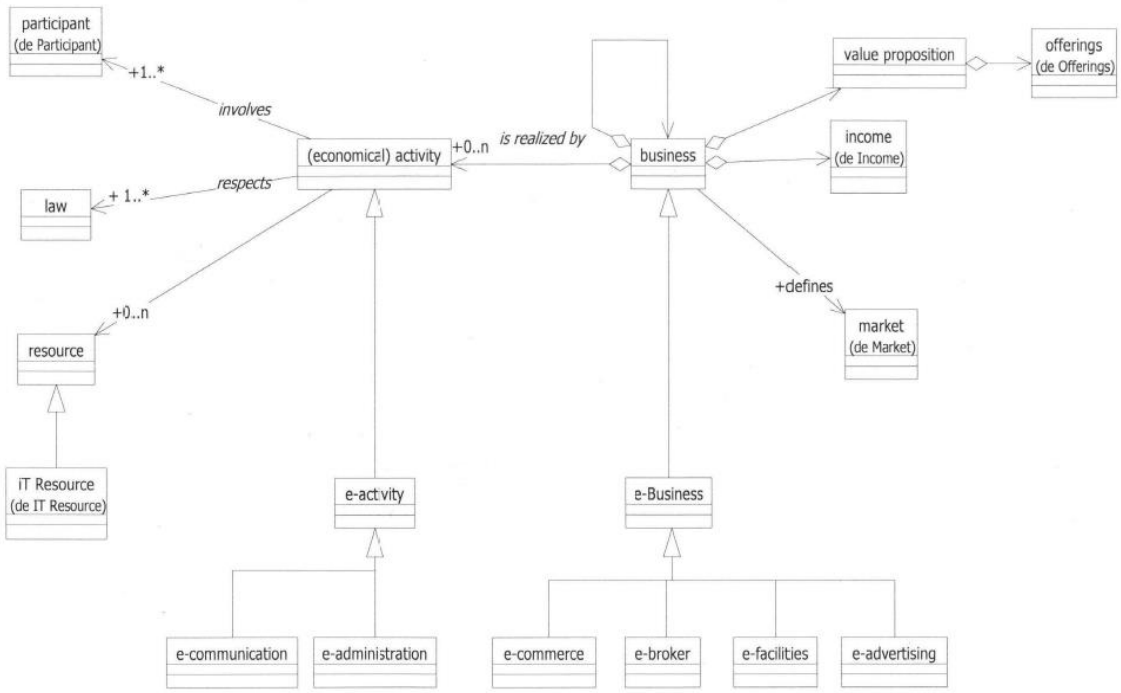
The exploitation modes of secured e-business architecture components depend on a great number of factors. Among those arise on one hand the factor related to the availability of in-house competences, and on an other hand, the factor related to the exploitation of the components on site or not. Both factors have an important impact on the security level.

Due to that, it is more than important to defined more precisely what we understand by e-business. As the picture 1 shows it, the e-business is a subset of a more total business activity. This business defines a market; it has incomes and proposals for values (products or services). This business constructs a whole of activities. It respects laws, uses resources, and

implies participants who can be an administration, a company or an individual. Each one of these participants is at least a customer or a supplier.

The e-business consists of e-trade, e-broker, e-facilities and e-advertising. In this definition, e-communication and e-administration are regarded as "e-activities", and not as e-business.

As the exploitation modes are based on competences of the company, the definition of SME does not relate to the size or on the sales turnover of the company, but well on its internal competences in data processing. However, a nuance is made concerning such e-business solutions which require only very few competences.



Picture 1: e-business activities

2 Exploitation modes classification

This second chapter of the paper defines four various exploitation modes, independently of a particular component. Those exploitation modes are based, in on hand, on the fact that the solution is located inside or outside the company and, on the other hand, regarding IT competences as internal or external.

The exploitation modes are thus different each other by the localization of the IT solution and the availability of competences necessary to manage the exploited solution.

Four exploitation modes are thus distinguishable:

- **Fully internal** is the traditional exploitation mode: to set up a IT solution, hardware and software are buy by the company, and one or more IT specialists are assigned to the management of the solution.
- **Intermediary 1** is the case of a company which wishes to have inside IT solution, but which does not have competences to manage this solution. The solution will thus be deployed in the company, but will be managed by an external person receiving benefits.

- **Intermediary 2** is the case of a company which wishes to manage the IT solution, but which do not have in particular the means of deploying it on its site for various reason (non-available computer room...)
- **Fully external** is the case of a company wishing to deploy an application that requires material resources or competences not acquirable inside the company. The company decides not to install the IT solution inside, and to let an external company manage it.

Exploitation mode	IT Solution		Competences	
	Internal	External	Internal	External
Fully internal	X		X	
Intermediary 1	X			X
Intermediary 2		X	X	
Fully external		X		X

Table 1 – Exploitation modes qualification

Exploitation mode	Software		
	Internal development	**Purchase**	**Rented**
Fully internal	X	X	
Intermediary 1		X	
Intermediary 2	X	X	
Fully external		X	X

Table 2: Software acquisition type

Moreover, these exploitation modes can be more precisely defined, according to the way in which the company will acquire the software and the hardware.

- **Software**: the software can be:
  - Developed inside the company - the company software development leads on an application that is managed by the company itself. The final solution can be internal or external.
  - Bought (several types of licences) - the solution is existing or specially developed for the need of the company. It includes the hardware necessary to its use.
  - Rented - the software is accessible by a remote application. It is a concept of 1-to-many: for one solution,

there are several customers. It is the case of the ASP[1]

- **Hardware**: the hardware when not included/understood in the price of the software, can be
    - Bought
    - Rented

The various possibilities of software acquisition for each exploitation mode are classified in Table 2

Taking into account the exploitation mode selected, the acquisition of the software will also be imposed:

- Fully internal:

  If the selected exploitation mode is all inside the company, then the software either will be developed inside the company, or bought.

- Intermediary 1:

  It is not possible for a small and medium enterprise to develop its own software, and it cannot also rent it because the machines are inside. It remains only the possibility of purchase the solution.

- Intermediary 2:

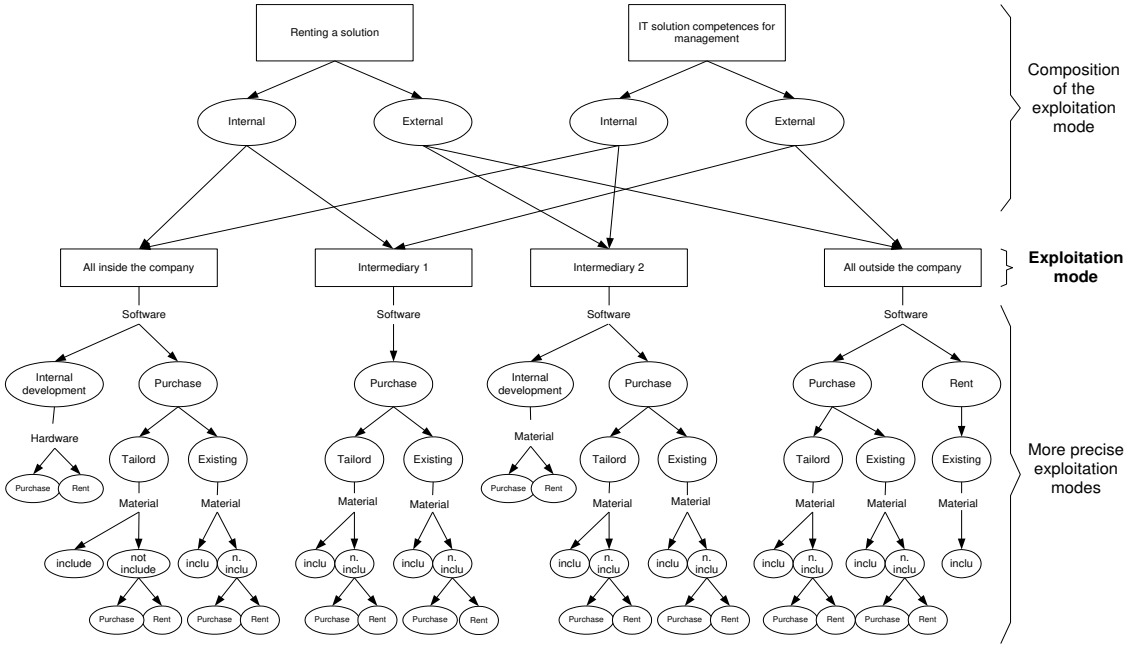
  A company that wants to externalise the localization of the solution but that wishes to manage it can develop the software or buy it.

- Fully external:

  In this exploitation mode, the company will have to reach the remote application. It can thus buy or rent the software.

This combination of possibility in the final analysis brings to define several mode of more precise exploitation as represented in picture 2.

[1] Application Provider Service

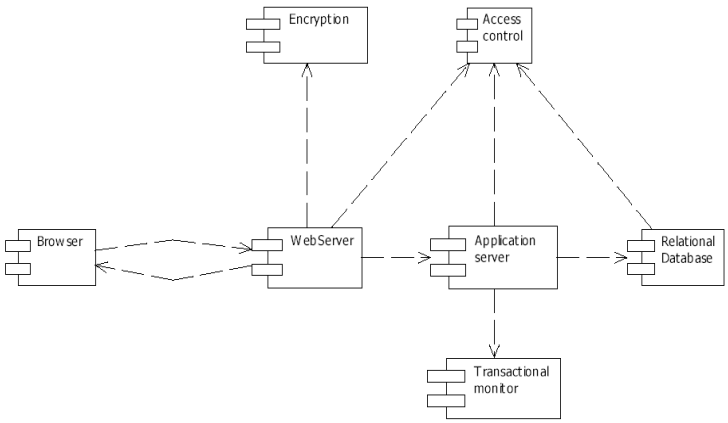


Picture 2 : Exploitation modes composition

3 Component by component security based analyze regarding the exploitation mode.

Always based on the results of the AccessPME project, the components of an e-business activity were modeled in UML and allowed to obtain the result of picture 3.

The continuation of this part will attempt to explain for each of these components the existing advantages and disadvantages to exploit those according to four modes defined in chapter 2



Picture 3: UML component diagram modeling of an e-business secure architecture

3.1 Webserver

Fully Internal

Without pointed competences, it is possible to make an Internet page by using a text editor as “wysiwyg” for example, and than install the

software on the computer which would be connected to Internet. For such a use, the software must be simple to use and to administrate; Apache is a counterexample of simplicity, because its use requires particular competences.

The deployment and exploitation costs of this kind of Web servers is obviously very weak: a computer, a connection to Internet, and the software which can be free, but the budget is inversely proportional to the security level: it does not have an automatic back up data, the availability is low (the traditional ADSL is slow with upload, and the server is not designed to receive a mass of simultaneous connections), and the software can not be very robust against attacks. The total security level is not sufficient to make e-commerce. Many delicate handling are necessary to the good deployment of the servers, and this handling must absolutely remain in the field of the specialists.

For the type of e-business defined in this document, this exploitation mode is not possible.

Fully External

Two under-exploitation modes exist for the Web servers: hiring or purchasing. For hiring, the principal criteria, which differentiates the existing solutions, is the fact that the server is dedicated or not for the e-business solution. A lodging on a divided server is interesting if the site must be available quickly, the budget is limited and the necessary disk space is small (in general, smaller than 100 MB). A hosting on a dedicated server is advantageous when the site is complex and dynamic, when the peaks of traffic can be significant, when the necessary disk space is about several Giga and when security components must be installed (firewall, VPN…)

The significant points to find by a provider are the transfer volume per month (limited or not; when limited, possibility of extending volume in the event of going beyond), the volume available on the server, the redundancy of the data, a guaranteed uptime, and the fact of being able to know the server geographical site. In our research, we did not find a provider who guarantees a minimal bandwidth for the server, and we did not find limiting number of simultaneous users. It is thus significant to be able to evaluate this load him self, and to be able to test the solution before buying it.

The case of the purchase of the software and its installation on a “hosting server” is similar to the hiring of software with dedicated server, only the fact that any software can be installed, whereas in the case preceding the Web server software is pre-installed.

This solution is heavier financially, but has the advantage to be more customizing.

Intermediary 1

Deciding to have an internal web server without managing can represent an expensive solution: the specialized material, a fast connection, and an external administrator can be expensive. The principal advantage of this exploitation mode is that the files contained in the server are internal, and they never circulate on the network (since the management of the contents of a distant web server is often done via the protocol ftp which does not encrypt the data).

For availability reasons, it is necessary to invest at least in an expensive SDSL line, a special material designed to be a web server, an external person who manage the solution, and in elementary security devices: a closed part, a smoke detector, an electric redundancy system…

Intermediary 2

As for the case fully internal, it is possible that SME installs a web server, which is simple for installation and administration. It is thus possible for SME to rent a “hosting server”, and to install it. However such a server will never be configured to have a sufficient security level to make electronic trade.

Such servers simple for administration are not appropriate for all the e-business types. Neither e-publishing nor e-advertising remains possible, the online sale proves to be impossible.

We thus see that the two secure exploitation modes for the web server are fully Internal and intermediary

3.2 Database

When we exploit databases, no available management competences are necessary in internal. Then, from the four exploitation

modes remain only two: intermediate 1 and fully external.

Intermediary 1

According to a databases availability study, the under exploitation modes available are: purchase of the existing software (the development of a specific database is too expensive) with bought material and purchase of existing software with rented material. Therefore it will be necessary to buy or rent the material, which will be able to support these solutions. According to the use of the database, a simple computer could be sufficient, and in other cases a mainframe will be necessary. In this under-exploitation mode, exist two types of software: free databases and proprietary databases. Let us see advantages and the disadvantages of these two alternatives.

The principal advantage of the free databases is the fact that it is immediately availability and without fees. However the cost of purchase should not remain the only aspect. A disadvantage is that no support or service, and interventions suggested by the software developers can be very expensive. Other potential difficulties for SME are characteristics of the free software: the majority of the software turns under Linux, which represents an additional difficulty for the beginner user in informatics. Moreover software is in permanent evolution, and thus requires regular updates.

For proprietary databases, the price strongly varies according to the use. The advantage of buying a proprietary database is the after-sale service and support (for limited duration).

Database forms part of e-business architecture and must be available via Internet, then the company will have to be provided with the particular protected infrastructure. This remaining out of price for a small structure, SME will not be able to reach a security level sufficient to protect the significant and vital data for the company.

Fully external

With this exploitation mode, the two possibilities are "Purchase of existing software, material not included", and "hiring of the solution".

Many hiring solutions exist on the market, whose characteristics strongly vary according to the solutions supplier, the data will be saved every day, every week, or never; the information exchanged between the customer and the database will be encrypted (SSL 128 bits) or not; an after-sales service could be included; the notice period of contract breach will vary from 0 days to 2 months and the number of requests made per month can be limited. It should be noticed that in the case of the fully external exploitation mode, during the online ordering solution, performance objectives and security policy of the database acquired are sometimes not clearly defined. It will be necessary to be attentive independently of the database acquirement price.

Another solution is the purchase of the software, hardware not included. This solution is rather close to intermediary 1, with the only difference that the selected database will not be installed in local, but on a rented machine, in hosting. It is a person from outside the company, who will administrate and manage the database server. The company will accede remotely and be able to execute only elementary commands.

This solution is much protected than the exploitation mode intermediary 1, because the rented server will have a security level much more specialized and better administrated: moisture and smoke detector, bi-electric feeding systems, dedicated firewall material, duplication of data...

We can conclude that the exploitation mode, which seems most suitable, is the fully external.

3.3 Application Server

The application servers are based on "Business Component " which must be programmed for the company. SME does not have, in general, internal competences to make this programming, nor to manage the application server. The exploitations modes are thus the following: intermediary 1 or fully external.

Intermediary 1

The same as for the web server and database, to install an internal application server requires a particular infrastructure. The security management can require much energy for only one machine, and thus to be very expensive.

Fully external

The exploitation mode fully external corresponds to rent a server in "Hosting" and to deploy the application server. This solution is much protected than the preceding one, because the infrastructure around the server is especially arranged for that use.

Normally, an application server can be almost free, even if there is proprietary, whose price relates to the performance level. However a company will not choose to deploy an application server whereas it does not need, because its installation and its management are much heavier than those of a web engine. What will be expensive is not the application server itself, but well it's programming.

While this component is analyzed, we will make the same for the web engine, which is rather close of the application server.

3.4 Web Engine

The differences between the web engine and the application server relate to functionalities, but the work completed by the one and the other is the same: data processing.

All annotations on security and exploitation mode of the application sever are exactly the same ones for the web engine. The choice between the deployment of a web engine or an application server will be made on a design level, which is out of scope of our actual research.

3.5 Access Control

In a dynamic environment, the problem is how the access control will know to which resources a customer have access. If the access control relates to a table field, then it will be difficult for the supplier of the access control to make a control if he is not directly connected to the persistence data system of the company.

There are overall three methods to control the access to files or folders: a control based on the hostname and user IP address, control via username and password, and finally the "strong" control using certificates.

The first two solutions are weak authentication solutions and can be installed internal. The third possible solution is the installation of a PKI. This one allows to the customers to be connected, to be authenticated on a server through their navigator and to reach resources. These resources can be executable code; therefore the company can completely delegate its access control to a third party.

3.6 Encryption

Whatever the required security level or the required functionalities, encryption component will have to be located at the same place as the web server and the access control, and the administration could not be made by SME.

Then we need external competences for the management of this component, because even if one or the other operation can be carried out by SME, the configuration of this component requires a high level of expertise to reach an irreproachable security level.

We have just characterized each component of the architecture most independently possible of the others. We saw that the two possible secure exploitation modes for almost all the components are fully internal and intermediary1. We have the tool to make the analysis of all architecture according to these two exploitation modes.

4 Conclusion

As a conclusion, we can note that among the four identified exploitation modes, only two are possible: it is intermediary 1 and the fully external.

For confidentiality, it is preferable to have an internal architecture. If this option is not possible, the company can be provided with necessary legal and contractual tools and maintain a level of confidentiality sufficient by deploying its architecture into external. The problem of availability cannot be considered with the same manner. To invest in an expensive infrastructure is the only manner of ensuring the availability, but such an investment remains difficult for the majority of SME. Face to this statement, we can conclude regarding to security, the most adequate exploitation mode for e-business architectures which we defined for SME is the fully external.

This conclusion must however be moderate. If we think that it applies in many cases, there are big sizes companies that do not have competences in data processing and which, for reasons of confidentiality, do not want to externalize their persistence data system. Thus, we could consider for example the case of a hospital, which could precisely have the means of acquiring this protected infrastructure in internal.

5 References:

[1] T. Dierks, C. Allen, The TLS Protocol version 1.0, Internet Engineering Task Force, January 1999.

[2] A. Dulaunoy, T. Fruru et S. Stormacq, OpenSST Message Format, Internet Drafts, December 2002.

[3] Feltus, Christophe, Djamel Khadraoui, and Filipe COSTA Pinto. "OpenSST based clearing mechanism for e-business." In Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on, pp. 89-90. IEEE, 2004.

[5] Ph. Oechslin, Quelques notions de cryptographie, http://lasecwww.eppfl.ch/securitereseaux/files/s1_07.pdf

[6] M. Pablos Martin, T. Pinxteren, P. Robert, Sécurité du commerce électronique, http://www.tele.ucl.ac.be/ELEC2920/2000/E-Commerce/secu_et_e-commerce.html

[7] D. O'Mahony, M. Peirce, H. Tewari, Electronic Payment Systems for E-Commerce, second edition, Artech House, 2001.

[8] http://www.opensst.org/

[9] Alexandre Dulaunoy, Sébastien Stormacq - OpenSST : Open Simple Secure Transaction, Une approche de réduction de la complexité pour les transactions électroniques. SAR 2003, 30 juin – juillet 2003. Marrakech, Maroc.

[10] Feltus, C., Ouedraogo, M. and Khadraoui, D., 2014, March. Towards cyber-security protection of critical infrastructures by generating security policy for SCADA systems. In Information and Communication Technologies for Disaster Management (ICT-DM), 2014 1st International Conference on (pp. 1-8). IEEE.

[11] http://atilf.inalf.fr/Dendien/scripts/tlfiv5/showp.exe?63;s=3375760125;p=combi.htm

[12] http://www.cetrel.lu

[13] http://www.iso.ch

[14] International Standard for Corporate Governance of IT (IT Governance) - ISO/IEC