Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TOWARDS A MULTI-AGENTS SYSTEMS APPLICATION BASED ON THE EAS-SGR FRAMEWORK

[1]HAJAR IGUER, [2]HICHAM MEDROMI, [3]ADIL SAYOUTI, [4]SOUKAINA ELHASNAOUI, [5]SOPHIA FARIS

[1] ENSEM- Hassan II University, LISER , EAS, Casablanca, Morocco

E-mail: [1]hajar.iguer@gmail.com , [2] hmedromi@yahoo.fr, [3] sayouti@gmail.com , [4]soukaina.elhasnaoui@gmail.com, [5]sophiafaris1989@gmail.com

ABSTRACT

Information has always been in the heart of every organization. During its exchange this information can be altered or modified. It is also considered as a key element for the development of many businesses. In this context, we have the obligation to protect it and secure it. In fact, it can't be protected without the use of frameworks and effective tools for risk management. Many industrial companies have chosen to put out in the market solutions that feed the need of IT managers. Our proposed framework EAS-SGR (Équipe Architecture des Systèmes- Systèmes de Gestion de Risque) was created to use the advantages of the panel of solutions that exists in the marketplace and designs a new system by using multi-agents system which will bring the intelligence to our application and to address risks from different angles and in different departments of the organization.

Keywords: *Multi-agent system, EAS-SGR Model, Risk Management, IT Governance, ISO 27005.*

1 INTRODUCTION

The organizations face a world of constant evolutions in the governance of their systems which directly affects their business in information governance. Obviously it is highly considered and vital for their systems especially information systems.

Because of organizational failures of the last decade, the statutory legislations and authorities created a complex set of laws and regulations aiming at forcing an improvement regarding the governance of an organization, the security, the control and the transparency. Due to its importance, the access to reliable information became a mandatory component for the business continuity.

Lately, the security was focused on the protection of the computer systems which treat and store the majority of information, rather than on information itself [1].

Facing the creation of new laws and regulations, we need a new approach of information security governance to protect the most critical credits from the organization.

Risk management issues need to be addressed with an infinitive care and requires leaders to review the organization decision making and the level of their information system's governance.

There is now a global consensus to consider that is no longer reasonable to assign responsibility only to IT security information held, produced or processed by the company. Information security, as well as managing all the critical resources of the company, is not only a technical problem, it became a trade issue that must be managed at the highest level of an organization. Effective security requires the active participation of executive's managers and the board to assess emerging threats and response to it. This work is motivated by the need of a model to address multiple risk possibilities that may harm your information system. Until now and in the IT governance domain, there isn't a solution that able the user to parameter different processes for one information system while using multi-agent systems.

The paper is organized as follows: after a brief introduction of the existing solutions, we will discuss in the second section a state of the art of information security governance and the solution EAS-SGR proposed by our team. Then, we will detail the functionality of our application that will implement our framework and give the best solution for security issues in organizations.

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2 PRELIMINARIES

2.1 Existing Solutions

In the business world, there is a multitude of solution that gives guidance to information security managers in order to help to protect their systems. Before starting to introduce the existing solutions, let's analyze the different frameworks and methods that exist for helping IT managers to step up a methodology or procedures to follow in their risk issues.

Risk management methods and tools enable the organization to plan and implement programs to maximize their opportunities and to control the impact of potential threats. This section provides an overview of available security risk analysis frameworks, methods and tools [2].

Put simply risk management is about looking at the risks that arise in the workplace and then putting in place sensible health and safety measures to control them.

You could view a risk's workplace as 'an incident waiting to happen'. Effective risk management means understanding what these risks are and preventing these accidents from ever materializing. The workplace can be defined as both within your premises or any employees you may have on the road.

Whether your business is large or small, effective risk management should not be ignored. Managing risk today means fewer surprises and unexpected consequences in the future.

2.1.1 Risk frameworks, Standard and Solutions

We present in this section an exhaustive list of framework and solution that are offered by international organizations [3].

TABLE 1. Risk Framework, Standard And Solutions

Risk Framework , Standards and Solutions	
ISO/IEC 27005(Standard)	Aviva Risk Management Solution
ISO/IEC 27001(Standard)	Web2 Security Services
CGE Risk Management	

From these some of these risk frameworks, standards and solutions are used by companies all over the world. For Example CGE Risk Management is an industrial solution that has multiple module and one of them is dedicated to risk management and which is not available for free. On the other hand ISO 27001 states a set of guidelines that allows to ensure the respect of the limits of risk exposure for your information system.

2.1.2 Risk Methods

We present in this section, the list of methods that exists in the IT marketplace, most of them are commercials or either they have paid modules.

TABLE 2. Risk Methods

Risk Method	
Au IT Security Handbook	IT Grundschutz
Cramm	Magerit
A&K Analysis	Marion
Ebios	Mehari
ISAMM	MIGRA
ISF Methods	Octave
SP800 30	Risk safe Assessment

From this list of Risk Methods, we have tested MEHARI and EBIOS since they are the majorly used. The rest are mostly commercialized tools, only available in free trial with a limit of time. These two methods are proved very detailed and elaborated. We inspire our work from these tools with the different steps that it shows but it is involving too many users and different actors.

2.1.3 Risk Tools

We present in this section, we present the available tools in the security management marketplace.

TABLE 3. Risk Management tools

Risk Tool	
Countermeasures	Octave
Cramm	Ra2
EAR/Pilar	Real ISMS
Ebios	Resolver*Ballot
Gstool	Resolver*Risk
GxSGSI	Risicare
ISAMM	Riskwatch

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Mehari	RM Studio
Callio	SISMS
Casis	TRICK light
CCS Risk Manager	Acuity Stream
Cobra	Modulo Risk Manager
MIGRA Tool	Proteus

We notice that there is a multitude of solutions, frameworks, methods and tools that only play a role for mitigating risks. Despite of all the available solutions, IT managers still get confused in front of these solutions. That's why our measure is to help decisions makers to make the right decisions and to do them right by accounting responsible for each of their services.

As a matter of fact, these are the mainly used solutions for risk management .Our solution's main objectives are to use multi-agent's system that will give it the autonomy and flexibility which are not important characteristics in the free available solutions. In addition, we tried to limit the interaction with the users in order to make the solution more intuitive. And, we will propose the upcoming application to be available for free.

2.1.4 EAS-SGR solution

Our aim was to create a new hybrid architecture that will allow flexibility to managers. In order to implement risks processes, it is necessary to define their tasks and workflows, which will ensure a consistent and accurate visibility of the relations between them. Figure 1 is presented in the following manner [4]:

There are several types of agents which include communicative agent, reactive agent, cognitive agent and intentional agent.

The multi-agent system reinforces the achievement of the same objectives of our hybrid architecture SGR. In particular, we will show how a flexible and extensible architecture of agents is constructed to form an intelligent risk mapping and assessment system. Figure 1 below describes the interoperability of our agents in the new framework that we proposed.

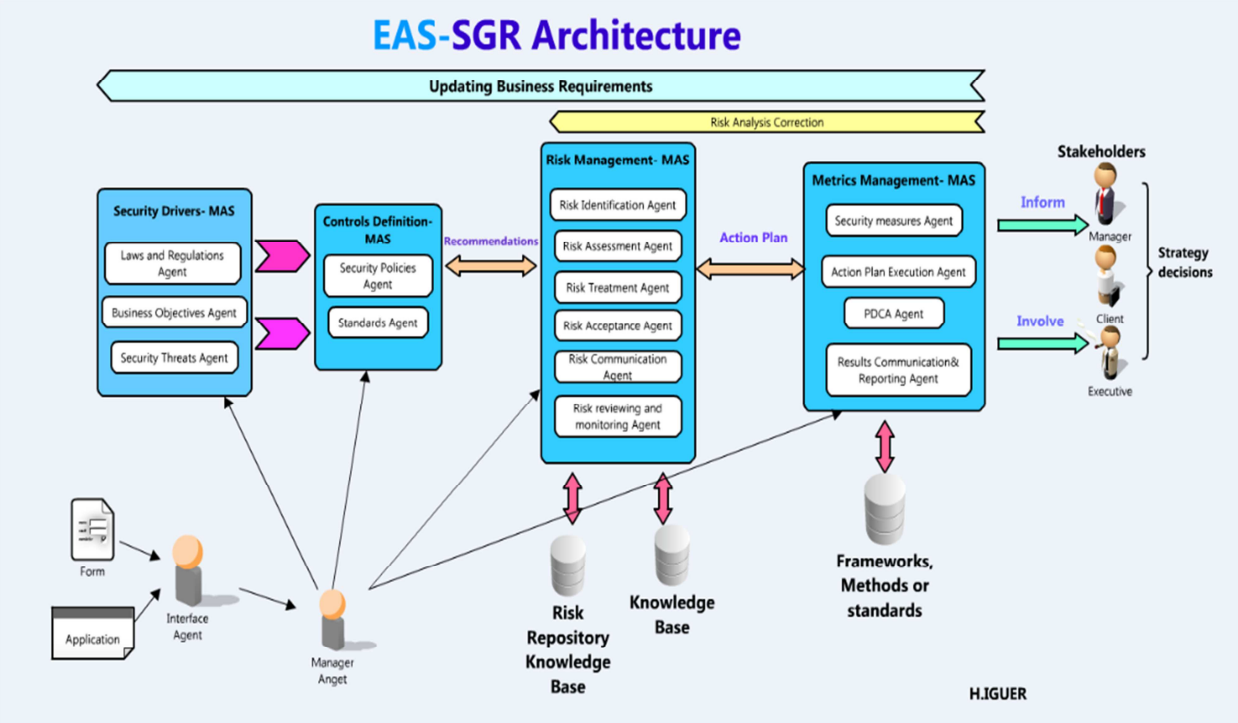

Figure 1. EAS-SGR Architecture

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3 EAS-SGR APPLICATION

For the creation of an application that will satisfy the need of IT managers, we implemented multi-agents system(MAS) that will give to our application the intelligence it needs to create a different approach with a cooperation between the different MAS [5].

The changing approach agent based, creates almost the same needs of the object-oriented but gives a dimension of a methodological approach to agent that will permit better control of risk attacks.

3.1 Multi-agents

Our application would not have the intelligence and autonomy without our multi-agents systems. In fact, we are going to define an agent and a multi-agent system.

Agent: is a virtual or physical entity that cooperates with others agents in the same environment working towards the same objective. An agent had different characteristics; he can be cooperative, communicative, reactive,

Multi-agent System: is an organized set of agents. It consists of one or more organizations which structure rules cohabitation and teamwork between agents. In the same system, an agent can belong to several organizations [6].

The inter-agent communication is fundamental to the realization of the agent paradigm, as is the development of human language was the key to the development of human intelligence and societies. To share information and knowledge, agents use ACL (Agent Communication Language).

The multi-agent System introduces a new approach to the implementation of several systems including independent and autonomous elements. This field of research is one of the most innovative; it shows many applications in several fields. Its wealth is a benefit derived by several companies or institutions which use multi-agent systems. However due to their efficiency, multi-agent systems are determined by several agent models and find with some complexity in their implementation. The use of these systems is often considered difficult [7].

3.2 Description of EAS-SGR functionality

The application will consist of a customizable hybrid platform according to the specific needs of IT managers. Concerning information security management within a company and covering the features necessary for their governance of all the processes of information security management will be detailed further on. For the first version of this solution, we are going to limit ourselves on the analysis of the risks of the software applications in the organization.

We aligned ourselves, to present our new approach as described in the standard ISO27005 for risk management. The different steps of our application "Risk Governance's Module" have for objective the [8]:

- Collection of the necessary data for the analysis of the risks
- Appreciation of the risk
- Determination Risk treatment
- Application of Risk management
- Application of Metrics management

In the rest of the document, update means the actions of addition, modification and suppression.
We aligned ourselves, to present our approach based on the description in the standard ISO 27005 and represented in the figure below:

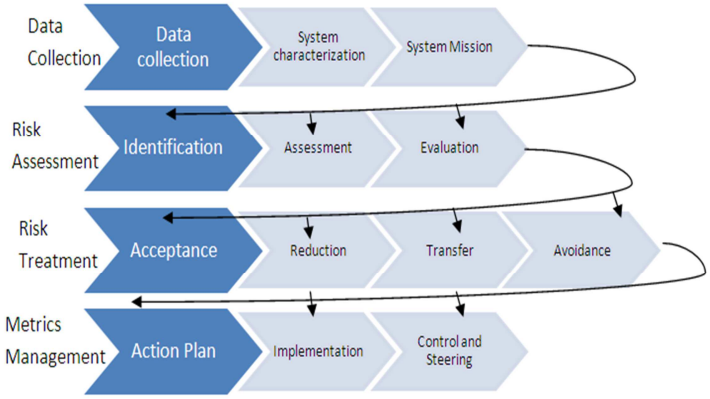

Figure 2. Major Steps in our IT Risk Governance

Journal of Theoretical and Applied Information Technology
10th January 2015. Vol.71 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Concerning the user interface of our application, the system will have to be accessible from any Web browser. It should be easy to use by limiting as much as possible the number of clicking. The navigation on the site will have to be simple and intuitive. A file for the user's assistance, presenting the interface and the features will be within the reach of the user. A login page will allow to different profiles of users to access the application. Then, the user will have access to the welcome page that displays the general information of the projects of each user. Indeed, it gives a general summary of the study in question because the system has to be to parameter according to every project. In fact, it will have a menu with tabs; a tab for each step of our risk governance framework [9].

- Data collection Tab
- Risk assessment Tab
- Risk treatment Tab
- Metrics management Tab
- Help Tab

Let's explain the functionality of each tab and detail the use of our framework in this methodology.

3.2.1 Data collection

Through this menu the user has several possibilities: Creation and update of the scale of criteria of information security criteria (CIAA: Availability, Integrity, Confidentiality and Accountability).

Examples:

- Availability: A from 1 to 5. 1= unavailability of 30 days unbearable / 4=unavailability of 4 hours is bearable.
- Integrity: I from 1 to 5. 1=the loss of integrity has no significant consequences for the project)

The display of the table of estimation of the levels of risk resulting from the association impact and probability (5*5).This part consists in classifying the levels of risk according to various levels of the gravity. In other words, we are going to put these results in three classes, high, middle and weak. We are going to adopt the table of classification used by ISO 27005 as indicated in the following table [10]:

TABLE 4. Table Of Risk Classification

Likelihood					
Impact	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

We also need to specify adequate levels to define specific risk classification which can vary from a project to another project and from a company to another.

TABLE 5. Table Of Interval And Risk Classification

Zone	Interval	Classification
Dark Green	1-4	Weak
Light Green	5-14	Middle
Red	15-25	High

In Table IV, the user has the possibility to change these intervals according to his needs and the degree of likelihood that a risk may occur.

In this page we can also find information about the company (name, number of employees, address, etc.), the systems business objective and the company's characterization [11].

In another section, we have the possibility to add questionnaire to identify risk and vulnerabilities that the users encounter in their everyday life. The management of the questionnaire is presented as a multiple choice questionnaire. It is divided into several modules according to the types of the questions. It allows the administrator of the application to manage users.

In order to manage questionnaires, the user has the choice to create several types of questionnaires:

- Questionnaires for the identification of the used applications in the organization. The questions have to draw the list of the most important applications in his department and at those in the organization. For example the name of the application, the operating system, the seller, the owner, the technical support, the number of recording and the database. It is necessary to pay attention; sometimes the user gives the name of a module of an application. There

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are applications which have several modules, such as the finance, RH and the stock.

- Questionnaire of audit of the organization with regard to compare with the domain analyzed according to Mehari's database of 14 questionnaires. For our system, we are only going to be interested in the "Security application ". The user has the ability of transmitting one or several questions in a technical contact if he doesn't manage to answer all of it.
- The questionnaire of the audit must be realized after that of the identification of assets.
- Import questionnaires in CSV format
- Send the questionnaires to qualified employees to provide answers. The user has the possibility to send the questions by blocks or individually (for every question we affect and indicate the person who will answer and the time slot allowed to that)
- Consolidation of the answers into reports.

3.2.2 Risk Assessment

This section will handle the creation and update of the assets in support by category or class of assets. Indeed, we start by identify risk and then we pass one to assess its degree of impact and at the end we evaluate this risk by using a formula which is described below as [12]:

Risk= Impact * Likelihood*(1/Countermeasure)

Where Likelihood = (Exposition+ frequency)/2 * 1/Control

And Severity = Risk / Time

In this tab the interface will allow the user to assess the sensitivity of core assets according to their security needs. Each asset will be judged on three criteria CIA. The user can change the values according to the scales he indicated as it is shown in Table IV.

The user will receive a form with all applications which are relates and within the scope of the study. The user must specify a value for each criterion. A description and explanation of the security criteria scale is mentioned in the data collection tab. The greatest value of these three criteria becomes the value of the impact.

Another page will estimate the value of the probability of the threats that have been identified in the case study. The user can choose the threat and see the list of vulnerabilities that are associated to it.

The calculation of the probability requires three components for the calculation:

- The frequency of the threat: While never being accurate; the auditor must base its conclusions on some information such as: number of detected attacks, antivirus statistics, current research and trends, anti - virus companies, etc.
- Exposure of the application: the auditor should consider certain factors to give this value: the accessibility of the application, location, data flows, number of users, previous incidents, etc.
- The control: is a value that must induce audit results previously achieved in the definition section of the context.

The values of these three elements must be between 1 and 5. Since the formula for calculating the probability is:

Probability = ((Exposure + Frequency) / 2) x (reversed Control)

While Exposure and frequency are proportional to the likelihood, the Reverse Control is inversely proportional to the probability; the greater the control over the probability is much reduced.

Concerning the evaluation of risks, another interface presents all threats to each application:

a. Each line must indicate the threat, impact, probability, the level of risk and its classification. For each application, the total levels of risk of all threats. The user can choose each line to give details on the threat:

3.2.3 Risk Treatment

By analyzing our formula results, we conduct a final assessment to know which method of treatment will be used for each risk depending on the results it gets upon all the calculations [13].

This page will provide an interface that presents all threats to each application. For each application, we must indicate the threat level of risk classification and a menu as a drop down list with the following options: reduce, transfer, maintain or avoid.

Once the user selected one of these treatments, the system gives it the ability to click on the line of threat for details to continue its operation. The user can choose from the different treatments that are proposed:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Risk Reduction:

The system must provide the description of the threat and the vulnerabilities associated with the asset. In fact, vulnerability for each system offers a number of measures that will reduce the risk, once the user choose to treat the vulnerability, the system recalculates the level of risk.

As a matter of fact, vulnerability can be treated with one or more safety measures and a security measure can handle one or more vulnerabilities [14].

- Risk Transfer

If the user chooses to transfer risk, the system is taken to a company that supports this type of threat or the user can propose the name of another company.

- Risk Maintain

When the user considers that the risk can be bearable after its correction and that the system is no more vulnerable then he may choose to maintain the risk within its level of acceptance.

- Risk Avoidance

If the user decides to avoid the risqué then he will be deleting the risk situation by using organizational or structural measures.

3.2.4 Metrics Management

After choosing the right treatment for the risk that we are encountering, now it is the time to implement the countermeasure by using an action plan in order to obtain the right security management for the organization [15].

3.2.5 Help

The help tab will provide assistance to the user and administrator to go through all the functionality provided by our application.

4 CONCLUSION

In this paper, we illustrated the use of our framework EAS-SGR in the design of our application which has the objective to help IT managers to choose the right processes to comply with their information systems. This work is important because of the infinite possibility that it gives to IT managers in order to comply with risk management procedures.

In this paper, we discussed the operability of our framework. Then we detailed the functionality of our application going through our risk governance processes from end to end. This particularity of our approach is to use multi agents systems that add the uniquely intelligence to our application. In addition, the combination of a method of risk management with ISO, internationally recognized, other frameworks and multi-agents systems provides the ability to secure and protect a system that represents the image of an organization. If the system is misused by the dramatic attempts of accessing restricted information by employees, it can harm its interests and the achievement of its business objectives.

This study is now limited to risk management in an organizational company. In our future work, we will start the audit of an information system. Then, we will detail the modeling, the realization of the application based on our framework. At the end, we will proceed for the test of the application on a case of study that includes an e-learning application.

REFERENCES:

[1] H. Iguer, H.Medromi.and A.Sayouti,"A new architecture multi-agents based combining EBIOS and ISO 27001 in IT risk management," in *Proc. ICEER'13*, 2013, paper 126.

[2] Basie von Solmsa,, Rossouw von Solms " From information security to.business security? » Computers & Security (2005) 24, 271e273.

[3] Na-yun Kim, Rosslin John Robles, Sung-Eon Cho, Yang-Seon Lee , Tai-hoon Kim,"Sox act and IT security governance", International Symposium on Ubiquitous Multimedia Computing 2008

[4] Rossouw von Solmsa, , S.H. (Basie) von Solms « Information security governance: as model based on the direct–control cycle on computers & security 25 (2006) 408 – 412.

[5] Basie von Solms, " Information security – the fourth wave" on Computers & Security 25 (2006) 165 –168.

[6] Neeta Shukla, Sachin Kumar, " A comparative study on information security risk analysis practices" on Issues and Challenges in Networking, Intelligence and Computing Technologies – ICNICT 2012, November 2012

[7] H.Iguer,S.Faris, H.Medromi and A.Sayouti," Conception d'une plateforme de gestion des risques basée sur les systèmes multi-agents et ISO 27005.

[8] J. Ferber, "Les systèmes multi-agents, vers une intelligence collective", InterEditions, 1995, pp. 63-144.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] Sayouti,F.Qrichi Aniba,H.Medromi. "Remote control architecture over internet based on multi agents systems".International Review on Computers and Software (I.R.E.CO.S), Vol 3,N.6,pp. 666 – 671,November 2008

[10] Hajar Iguer, Hicham Medromi, and Adil Sayouti, "The Impact of the 4th Wave on the Governance of Information Systems: IT Risk Architecture- EAS –SGRBased on Multi-Agents Systems," International Journal of Computer Theory and Engineering vol. 6, no. 5, pp. 432-437, 2014.

[11] Stuart J. Russell and Peter Norvig, "Artificial intelligence: a modern approach". Prentice Hall; 3 edition, 2009.

[12] Wooldridge, M. (2002). An introduction to multiagent systems. Chichester, UK: John Wiley & Sons.

[13] Y. B. Khoo1, M. Zhou1, B. Kayis2, S. Savci3, A. Ahmed 2, and R. Kusumo1S, .H. Bokhari, "An agent based risk management tool for concurrent engineering projects", Complexity International, Vol. 12, 2005.

[14] April4, 2011 Book Chapter in the book "Multi-agent systems – modeling control, Programming, Simulations and Applications", ISBN 978-953-307-174-9, InTech,

[15] Nato Otan, "Risk Analysis Tools", Improving common security risk analysis ,2008, Chapter 5.