International Journal of Innovation in Science and Mathematics
Volume 5, Issue 2, ISSN (Online): 2347–9051

The Implementation of IT Risk Architecture in IT Governance Context

Hajar IGUER*, Soukaina ELHASNAOUI, Hicham MEDROMI and Adil SAYOUTI
*Corresponding author email id: hajar.iguer@gmail.com

Date of publication (dd/mm/yyyy): 29/04/2017

***Abstract* — The use of technology is useful and indispensable for all companies. In this context, international companies thrive to implement an information system that will help them provide a continuous support to the company's business objectives. Many research papers were written in this domain for the awareness of decision makers to deploy an information system adapted to the size of their structure. In this sight, the awareness shed a light to a specific domain of IT systems which is IT risk management which importance is growing considerably. This also comes in line with the strict regulations that many countries are setting in to protect themselves from these different kinds of risks. Our work is inspired from the several commercial and free standards and frameworks that enterprises feel the immediate need to use in a competing and complex global market. This integrated software is related to Governance, Risk and Compliance (GRC) which is becoming one of the most important business requirements for organizations. In this paper, we propose a business architecture that describes the integration of the main processes for IT Governance, IT Risk Management and IT Compliance (IT GRC), then we emphasize on IT Risk management using ISO 27005 and EBIOS. Plus in order to model this interaction, we used multi-agents and expert system which behavioral and informational structures are valued for an automated system. Finally, we conclude with a simulation developed with JESS which gives results for a good orientation of information system and a quick decision making initiative.**

***Keywords* — EBIOS, GRC, ISO 27005, IT Governance, Risk Management, Security.**

I. INTRODUCTION

Computer science environment find itself embedded in various companies and in different sectors essentially because of the immediate need of a support system to the companies in the marketplace. Indeed, this inclusion comes to highlight the importance of such a system for the improvement of information acquisition, information storage, information treatment, or even information analysis. As a matter of fact, information plays a huge role in all companies because it simply is a support to the company's business objectives. This emphasizes the importance of information system in any business context.

In the ever-changing and evolving business environment, that we live in, push us to develop and enhance all support system to the level that the company need. In fact, companies need to benefit from these changes and advances in technology which is playing a major role in bringing companies reach their business objectives.

II. THEORETICAL BACKGROUND

First, we will state a definition of corporate governance. Second, we propose a causal relationship between IT governance and IT risk management. Third, we propose corporate culture strength as moderator of the relationship between corporate entrepreneurship and IT risk management.[1]–[3]

In this matter, we introduce corporate governance which refers to a system throughout the enterprise direct and control a list of specific tasks and responsibilities between the participants of this environment. Its committee of directors meets on a regular basis in order to shed light on the changes that occur in their companies that is why they need to be delivered a set of dashboards detailing their information system state.[4]

We have also noticed that over the last few decades, many companies went to ruin for the lack of information support systems. Since some of corporate governance components include Policies and procedures and Monitoring and internal control, this situation can show a close relation between corporate governance and IT. The pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT Governance. Indeed, IT governance was created from the fusion of this coalition. Gartner states that ITG has been recognized as a Chief Information Officer (CIO) top-10 issue for more than five years and has risen in priority between 2007 and 2009. In the light of this discovery, other combinations were created from start to finish bringing out different possibilities such as information security governance, IT risk, IT compliance etc[5]. And as it is stated in the IT research literature, corporate entrepreneurship is an antecedent to IT governance, IT risk management, and IT compliance. They all are a must have for companies to contribute to higher returns on assets at a time when businesses are increasing their technology investments. Due to increasingly importance of new requirements, standards and framework, enterprises feel the immediate need to effectively manage the increasing business and operational risks inherent to competing in a complex global market. Responding to this need, organizations created integrated software for Governance, Risk and Compliance (GRC) is becoming one of the most important business requirements for any organization

III. MODELING THE ARCHITECTURE

In this section, we gather and present all scientific resources used throughout this research, stating with determining the context, followed by the models and modelling language used to construct the final artifact. After the discovery of IT governance, we noticed a relatively close relation with IT risk and IT compliance. In view of this closed related, we introduce below these terms:[6], [7]

- IT risk can be considered as set of coordinated activities to direct and control organization towards the risk. IT 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. It generally identifies three goals in the management of risks to the information system:
  - Improve the security of information systems.
  - Justify the budget allocated to the security of the information system.
  - Prove the credibility of the information system using the analysis.
- IT compliance management provides a common framework to manage and monitor compliance with a range of IT regulations and standards such as Sarbanes-Oxley Act, 09-09 Moroccan law.

A. Purpose

The purposes of this publication are to introduce a global architecture including IT GRC concepts then explain specially the IT R component. We emphasize on risk to provide guidance to information security officers for applying risk management to their information system. The study goes through different security levels of an organization information system. Risk management principles main goal is to apply the best practices into an organization wide strategic planning and based on that deliver results in the operational environment.[8]

B. EAS-IT-GRC Architecture

In our laboratory, our objective is to deliver a sustainable support to companies in need of a better information system management. Therefore, our approach is to integrate all companies' essential aspects and fulfil the goal of helping them reach their financial and business outcomes. These aspects that we need to consider could be listed below as the company's:[6], [9], [10]

- Business Objectives
- Security Requirements
- Internal control and audit
- Service management. etc

To achieve this outcome, several researchers gathered and proposed this global architecture, as it is shown in Fig.1. This figure represents the global architecture, EAS-IT GRC, proposed by our laboratory is represented in different layers. They can be presented as follow:

- EAS Strategic Layer
- EAS Decision Layer
- EAS Processing Layer
- EAS Communication Layer
- EAS Updater Layer

Basically, the exchange of information in this architecture is based on message sent. As it illustrated in the figure, the communication starts with the EAS-Strategy layer by sending the results of the business objective analysis. Then, the request is handled by the EAS-Com layer which main role is to deliver the message to the related layer. In fact, there are different forms sent by the DML layer, the strategy layer and the processing layer to the end user to collect answers and match it with data in the knowledge base.

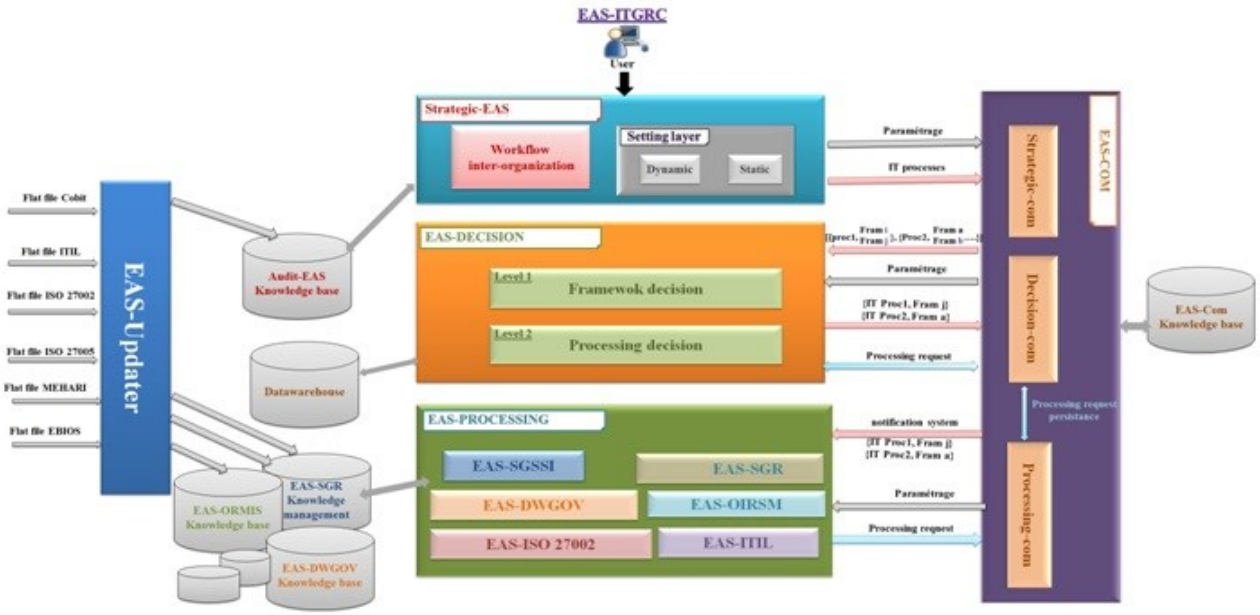

Figure 1 - EAS IT GRC Architecture

C. Multi-agent systems

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 other agents in the same environment working towards the same objective. An agent had different characteristics; he can be cooperative, communicative and
reactive. Multi-agent System (MAS): 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. 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.

D. Expert systems

Experts are supposed to be people with a certain kind of knowledge and expertise in solving problems, while expert system is a branch of artificial intelligence which stimulate human reasoning in some domains. They can be defined are knowledge based system that enables problem solving in different situations. This fundamental function depends on the knowledge quality that is provided. This system can also be defined as a computer program that performs special and difficult task in various fields. The list below presents the different types of expert systems:[11],[12]

- Neural networks
- Blackboard systems
- Case based reasoning
- Belief networks
- Rule based systems

While talking about rule based system, we can distinguish two categories expert system and expert control system. This is a separate distinction between an expert system and an expert control system. Expert control system needs to be on-line because of the immediate requirement of dynamic information in order to achieve real-time control system. However expert system requires a complete consultative function for problems in special domains. Rule based expert system is a type of expert systems that explain and justify solutions in user friendly terms. We chose to use rule based system because of the nature of risk management requests. The problem is stored as data and the reason is based on using IF.. THEN ELSE rules. Then we can deduct from these rules using forward and backward chaining. While using this system, we identify the problem and solution based on the following terms:[12], [13]

- Communication Interface
- Knowledge Base: Representation of facts and rules
- Inference engine
- Interpreter
- Output: a list of recommendations

Inference Engine or the reasoning machine is able to memorize the rules and control strategies that are applied. It plays a major role in coordinating the whole system in a logical manner, draw inference and make the right decision. Inferencing is the reasoning process of AI. It takes place in the brain of an AI process. There are two strategies that are used by the inference engine, these tactics are forward and backward chaining. According to durkin [14], rules can represent a relationship (direct conclusion), suggestion (result: proposing a suggestion), instruction (result: telling you what to do next), strategy (different condition related to each other when the result of the first is a condition of the second) and heuristic. The inference engine which resolves problem facts and rules based goes through a throw process until all rules are satisfied [15].

Knowledge base: It stores two different elements: facts and rules or heuristic rules. Stored facts are outlined as information or data in a certain field. While rules explain procedures of reasoning used to solve certain problems. The other kind of data is stored in a global database. Example of a rule creation: (Type: Instruction).

The communication interface: It is the expert system method to communicate strategies and decisions to the end user. This interaction is written in a problem solving oriented language such as the use of an editor or graphics. The interface mediates the exchange of information between the user and the ES. Throughout the user interface, the interpreter is capable of analyzing and explaining user questions, commands and justifications from both parties as well as request for data. The interpreter: To record and register immediate user's hypotheses and results of ES decision making. This kind of information can also be stored in the global database. While going through the different architecture that exists in the literature not all of them use all of these components but they mainly implement the inference engine and the knowledge base. We will be following these steps in order to achieve the design of the expert system:

- Design of an initial knowledge base
- Development and test for prototype system
- Improvement and induction for the knowledge

Table 1. Example of a rule creation (Instruction)

IF Policy doesn't exist AND the objective is to create an ISMS THEN set a new policy	IF Vulnerability exists THEN apply control measures

These relative steps are determinative of the conception of an expert system. The key element for a successful knowledge base is to start step by step in the introduction of facts and rules. The same rule can be applied for the ES conception.

E. EAS IT risk architecture

We introduce in this subsection our IT Risk Architecture which is part of our global EAS IT GRC architecture. As you can see in the figure below, our architecture is structured as follow:

All the multi-agent systems come in support to our expert system providing it with the necessary information to construct rules and facts. Based on that, it can use its inference engine and come out with a set of recommendations that will be explained in the simulation section. Expert system results can't be effective without the contribution and the requests of the user[16],[17].

With regards to protecting the confidentiality, integrity

and availability of information system and for processed, transmitted and stored information, we categorize these security controls families. These controls can be monitored by someone else than the information owner. It can be a third party official or organization. Applying security control across the organization can result in significant savings to the organization and can be applied to multiple information systems and entities. They can also facilitate accountability for security across the organization.[5], [18]

The Controls Management MAS is composed with four agents which main role is explained below[19]:

- Security Policy Agent: This agent obliges the organization to have a general security policy and a specific one if it is needed.
- Control Agent: It is the agent that is responsible of following the standards that have been chosen.
- Security threats Agent: Collects security threats available in the frameworks knowledge base and adapt them to the environment.
- Laws and Regulation Agent: Its main role is to collect laws and regulations which are applied to the organization in order to prevent serious juridical problems.
- Risk Management MAS: This multi-agent system is constituted of three agents.
- Risk Identification Agent: It oversees the identification of risk parameters.
- Risk Assessment Agent: This agent evaluates threats and vulnerabilities to better understand and measure the risk impact.
- Risk Treatment Agent: It chooses between different measures that were proposed at the main objective to alter risk and their impact on the organization.

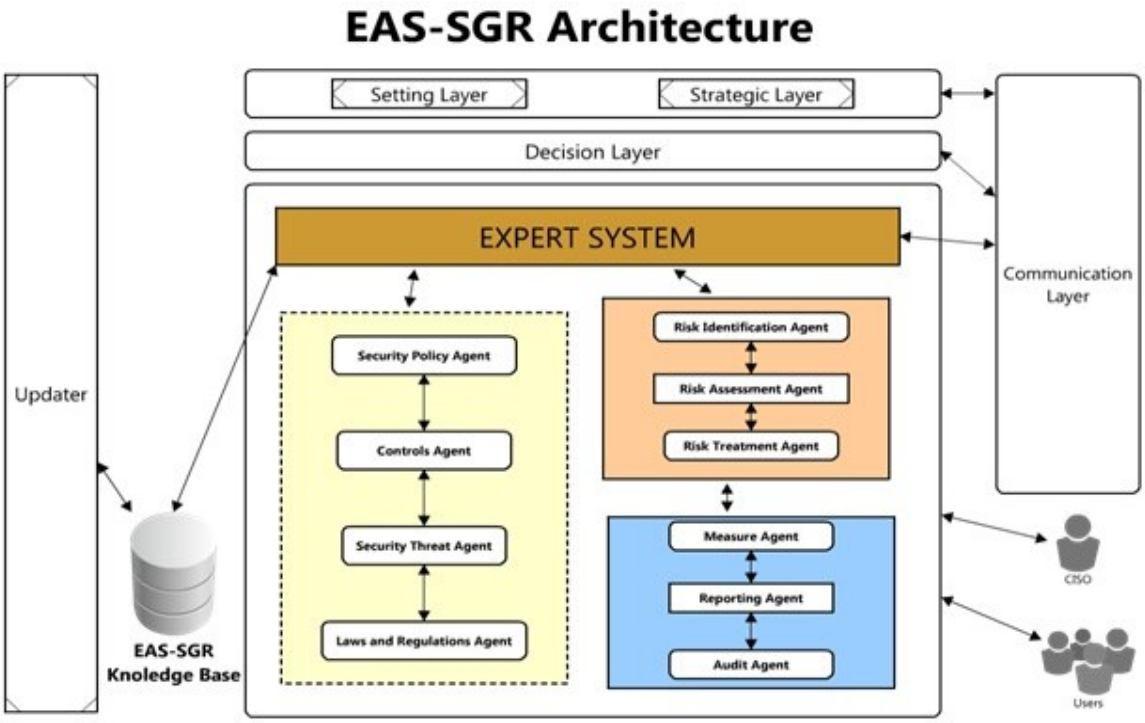

Figure 2 - EAS-SGR Architecture

Measures Management MAS contain also three agents which purpose is explained below.[20]

- Measures Agent: It dictate a plan for the implementation of the chosen measure by the risk treatment agent.
- Reporting Agent: realizes dashboard for the top management.
- Audit Agent: It allows an audit of the information system to check the good application of the measure.

F. Quantification and Calculation of Risks of EAS-SGR

Methods of risk assessment of information security referable are mostly inherited from the traditional ideas of conceptual model proposed by Finne, in which the risks and size of the loss were evaluated from the following areas: the vulnerabilities of information systems, possible attack, and loss of information assets. The following formulation expresses this implementation [21],[22].

$$RA = function(I, V, T) \quad (1)$$

RA delineates the actual loss affected by a potential risk and its value can be expressed as it outlined above. I is the impact of the risk on the business value, T is the probability of threat occurrence in the company's assets. V is the amount of vulnerability reflecting the weak points exploited by some threats which can be quantified by the history of experiences determined by experts. a represents the number of assets impacted by this vulnerability. In a realistic context, we deal with a great number of assets confronting a group of risks. The equation can be written as follows:

$$RAi = \sum_{i=0}^{x} ai * Vi * Ti * Ii \quad (2)$$

IV. Applicability and Simulation Experiment

In this section, we consider a basic enterprise environment to which we are conducting this simulation. In this context, the company owns a small number of assets and employs some people in different department. To emphasize, we realized a JAVA application based on JESS, JAVA Expert System Shell.[23]

A. JESS JAVA Expert Shell System

Jess is an acronym for Java Expert System Shell. It is a rule engine and scripting environment written entirely in Sun's Java language by Ernest Friedman-Hill at Sandia National Laboratories in Livermore, Canada. Jess was originally inspired by the CLIPS expert system shell, but has grown into a complete, distinct Java-influenced environment of its own[24], [25].

With Jess, we can build Java applets and applications that have the capacity to reason using knowledge you supply in the form of declarative rules. Jess is a tool for building a type of intelligent software called expert systems. As it is shown in the figure below, JESS Architecture is based on the architecture of Expert systems. We chose this tool because of different reasons

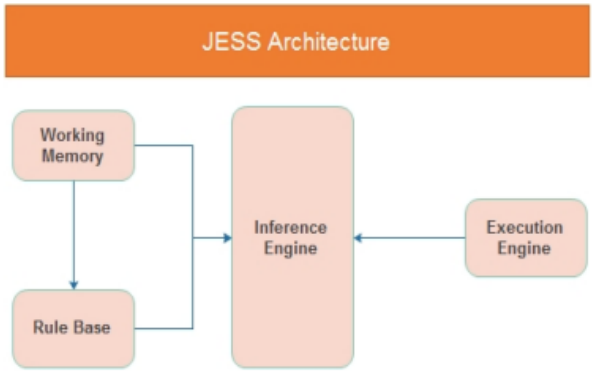

Figure 1 - Jess Architecture

B. The Simulation Experiment

As an example of security controls, we may mention access control which is a technical aspect of introducing controls in information systems. In addition, we mention physical and environment protection which is categorized with the operational class of security controls. That is why in our example; we chose a variation in a software asset.

In order to experiment our designed model, we only included some of our rules and facts to verify the implementation of our EAS-SGR model. According to formula(2), we bear in mind that more the value of the impact is higher; more the asset is sensible and compromised. Here is an example that shows the calculations of the value of Ii

Table 2 Example of impact calculation

Asset Type	Confidentiality	Integrity	Availability
Software	3	3	3

In fact, the calculation of the impact is based on the confidentiality, integrity and availability of the asset. Indeed, we suggested that lower number means a greater impact on the asset and that 3 is the acceptable level.

While using JESS, a rule based system, we interfaced it with a JAVA application and got the following:

- The welcome interface which launch the starting point inference engine of our JAVA application.
- The closing interface displays to the user the recommendation, in a pop-up interface, that he should consider lowering his risk impact.

Admittedly, the simulation has shown that the user communication and interaction is vital to our EAS-SGR proposed model and that it influences the proposed recommendation. Furthermore, our expert system plays a dominant part in the risk system.

This figure shows an example of a question asked tothe end-user.

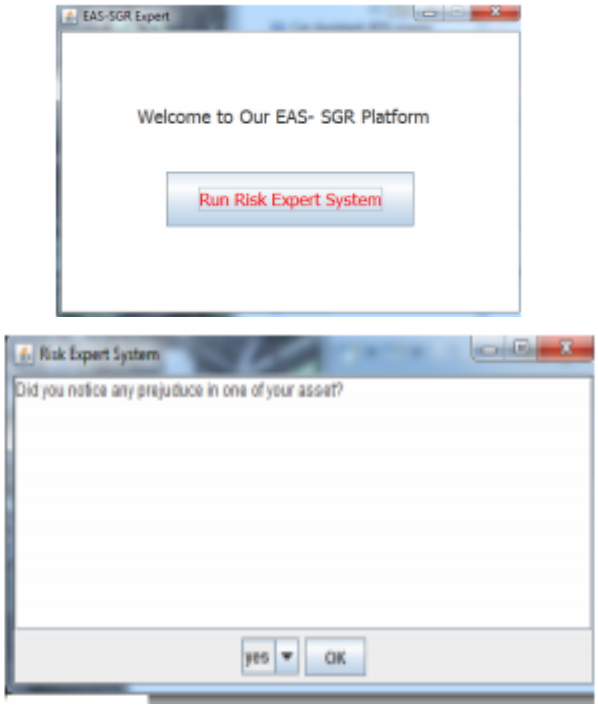

Figure 2 - Simulation Interfaces

a- Welcome Interface
b- Example of a question

V. Conclusion

In this paper, we introduced another version of our architecture EAS -SGR and illustrated the different aspects that were needed into its adaptation. It is flexible, customizable and updated to the original frameworks and methods that already exist in the market. In addition, it is a part of a global architecture EAS IT GRC that was constructed in our laboratory. Our approach was to integrate multi-agents and expert system to accent the deliberate intelligence of these systems. In addition, the combination of the expertise of different IT risk management methods, internationally recognized, attest of quality of our system that represents the image of an organization. Management system of information security can be set up by ways of risk

analysis and decision, as well as the construction of risk control model based on the information system life-cycle. Experiments show that, EAS-SGR and its various calculation methods can effectively help user and chief information security officers to prevent, protect and control the various risks in an ITG process. Not only it can but it can help them but it also can meet requirements and expectations of security objectives in IT management. In future research the next steps will be to complement the simulation with more rules and facts that might be missing, given the high-level nature of the model used. Additionally, the remaining architectural layers will be designed for complete and functional enterprise architecture, namely the updater layer and the reporting system.

ACKNOWLEDGMENT

This research could not have been completed without the support of all joint authors of this paper. H.Iguer would like to thank her mentor and supervisor Pr. Hicham MEDROMI and Pr. Adil SAYOUTI who continue to encourage her to tap deep into scientific research in computer science.

REFERENCES

[1] "grc-resource." [Online]. Available: http://www.grc-resource.com/.
[2] N. Racz, E. Weippl, and A. Seufert, "Governance , Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives," 2004.
[3] Rsa, "RSA GRC Reference Architecture."
[4] A. Belalcázar, J. Díaz, and L. Molinari, "Towards the Strategic Alignment of Corporate Services with IT, applying Strategic Alignment Model (SAM)," vol. 16, no. 1, pp. 52–58, 2016.
[5] W. H. Yuan, H. Wang, J. Zhang, and W. J. Qi, "Research on risk control system ITG-HRCM in IT governance," Proc. 2012 Int. Symp. Inf. Technol. Med. Educ. ITME 2012, vol. 2, pp. 1007–1011, 2012.
[6] H. Iguer, H. Medromi, A. Sayouti, and S. Tallal, "Including EAS-SGR IT Risk framework in an IT GRC global framework."
[7] G. Mangalaraj, a Singh, and a Taneja, "IT Governance Frameworks and COBIT-A Literature Review," Twent. Am. Conf. Inf. Syst., pp. 1–10, 2014.
[8] A. E. Brown and G. G. Grant, "Framing the Frameworks : a Review of It Governance Research," vol. 15, pp. 696–712, 2005.
[9] H. Iguer, H. Medromi, and A. Sayouti, "The Impact of the 4th Wave on the Governance of Information Systems : IT Risk Architecture- EAS – SGR- Based on Multi-Agents Systems," vol. 6, no. 5, 2014.
[10] S. Elhasnaoui, A. Chakir, M. Chergui, H. Iguer, S. Faris, and H. Medromi, "Building an integrated IT GRC platform based on multi agent system," vol. 4, no. 8, 2015.
[11] "Introduction to Artificial Intelligence & Expert Systems.pdf." .
[12] R. The, "Steps to Create an Expert System," 2015. .
[13] J. C. Ross, "Developing Expert Systems from Examples and Explanations," 1987.
[14] J. Durkin, Expert Systems- Design and Development, 1st Editio.
[15] P. Tripathi, S. N. Islam, J. Ranjan, and T. Pandeya, "Developing computational intelligence method for competence assessment through expert system: An institutional development approach," 2010 IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC 2010, pp. 146–151, 2010.
[16] C. Zhang, D. Tang, Y. Liu, and J. You, "A Multi-Agent Architecture for Knowledge Management System," no. 1, pp. 433–437, 2008.
[17] J. Ferber, O. Gutknecht, and F. Michel, "From Agents to Organizations: an Organizational View of Multi-Agent Systems," Lncs, vol. 2935, pp. 214–230, 2003.
[18] H. Iguer, H. Medromi, A. Sayouti, and S. Tallal, "A new architecture multi-agents based combining EBIOS and ISO 27001 in IT risk management," no. July 2013, pp. 1–8.
[19] S. Foley, "Security Risk Management using Internal Controls," pp. 59–63, 2009.
[20] J. R. Getter, "Enterprise architecture and IT governance a risk-based approach," Proc. Annu. Hawaii Int. Conf. Syst. Sci., pp. 1–11, 2007.
[21] D. Ionita, P. Hartel, W. Pieters, and R. Wieringa, "Current Established Risk Assessment Methodologies and Tools," Univ. Twente, Cent. Telemat. Inf. Technol., no. September, 2013.
[22] N. Racz, E. Weippl, and A. Seufert, "A process model for integrated IT governance , risk , and compliance management," Ninth Balt. Conf. Databases Inf. Syst., pp. 155–170, 2010.
[23] E. Friedman-Hill, Under the hood: how Jess works. 2003.
[24] M. Menken, "Jess Tutorial," 2002.
[25] "Java Expert System Shell (JESS)." [Online]. Available: http://herzberg.ca.sandia.gov/jess/.

AUTHOR'S PROFILE

H. Iguer was born in Casablanca in the 25th of January in the year of 1989. The author graduated as an engineer in computer science from the National School of Electricity and Mechanics, Casablanca, Morocco in 2011.

Before her graduation, she has been in four companies doing internships; the first job was in 2010 for the implementation of a package for sales management in sugarcrm then in the same year she joined disway for the administration of networks and systems. Finally, she did her end of study project at highTech payment system with the topic of the design and implementation of a business intelligence platform for the management of performance indicators in dashboards. For her first job, she joined the International University of Casablanca in the beginning of the year 2012 where she occupied the job of a PERMANENT PROFESSOR. She also has published two national and two international communications among them JDTIC 2012, ICEER 2013 IC2INT 2013 and JDTIC 2013. Her current research interest is in IT risk within the governance of information systems.

Ms. Iguer is certified ITIL® V3 Foundation (IT Infrastructure Library) and ISO/IEC 27002 Foundation (International Organization for Standardization).

Soukaina EL Hasnaoui graduated from ENSEM engineering school in 2011 in the field of computer science. With her work experience in multiple companies, she converted to do scientific research in the same platform.

She participated in several national and international conferences with high impact in the same domain. She also published with collaboration with other researcher's articles in well renown journal like Thomson Reuters, IEEE and Springer.

Hicham Medromi received the PhD in engineering science from the Sophia Antipolis University in 1996, Nice, France. He is director of the National Higher School of electricity and mechanics(ENSEM) Hassan II University, Morocco. His actual main research interest concern Control Architecture of Mobile Systems Based on Multi Agents Systems.

Adil Sayouti received the PhD in computer science from the ENSEM, Hassan II University in July 2009, Morocco. In 2003 he obtained the Microsoft Certified Systems Engineer (MCSE). . His actual main research interests concern Remote Control over Internet Based on Multi agents Systems.