The Impact of the 4th Wave on the Governance of Information Systems: IT Risk Architecture- EAS –SGR- Based on Multi-Agents Systems

Hajar Iguer, Hicham Medromi, and Adil Sayouti

***Abstract*—The increasing demand of the protection of an enterprise information system has become one of the major priority and commitment of the executive committee and the board of directors. Risk management aligned with IT resources consists of a strong result which is called Information Security Governance (ISG) or the 4th wave. This article will present a multi-agent system which automates the ISG process on the behalf of the top management. The originality consists on using multi-agents systems including the 4th wave which has never been done before in other scientific works. It would result on the assessment of a new model merging the development of ISG, compliance and risk management in one framework which demonstrates the pivotal role of handling security risks in a company. In this context, we must address security with highly precautions; we should not only focus on the technical problems of security but also to their decisional part which involves the board and top management. Following the PDCA approach, we will demonstrate how our model can use international standards and methods to support organization's information systems.**

***Index Terms*—4th wave, information security governance, multi-agents systems, plan do check act.**

I. Introduction

It is common these days to accept that information security has changed its aspect of technicality and moved to a strategic approach. The mainly objective is to protect the data that circles in the organization from the employees to the managers and the top board. In order to secure the organization IT systems, IT must be involved within the organization daily operations and take part of the improvement of all the processes [1].

The importance of risk management in the IT department is increasing knowing the sensibility of the information. In fact, IT should be embedded in the company security activities and should be aligned within the organization business objectives. Achieving these objectives is a result of good corporate governance. Top management and boards of Directors are accountable for their IT systems.

Manuscript received December 10, 2013; revised February 8, 2014.

The authors are with the National School of Electricity and Mechanics , Hassan II University and Permanent Professor at the International University of Casablanca, Casablanca, Morocco (e-mail: hajar.iguer@gmail.com, hmedromi@yahoo.fr, sayouti@gmail.com).

II. State of the Art

A. Information Security and Corporate Governance Differences and Backgrounds

The fourth wave of the information security is defined as a new approach to the Information security governance. This wave is closely related to the Corporate Governance. Several documents has related to the Corporate Governance in the last decade establishing its importance in an international level. Corporate Governance refers to the system by which corporations are directed and controlled with a specific distribution of duties and responsibilities among different participants in the corporation. As an example, whereas handling their responsibilities, the board of directors may be accountable for aspects like risk management and still ensuring the integrity of their IT systems. In order to fulfill their responsibilities, the board needs to have access to timely available information [2].

Several legal and regulatory enhancements related to corporate governance have focused on the role and responsibility of the Board, including the law of Sarbanes - Oxley (SOX, 2002) which also requires setting up a system control related to operational risks that often result in the establishment of measures to manage risks related to security of information systems [3].

As a result of using the Sox act (Sarbanes- Oxley); top management must certify the accuracy of information contained in annual reports, which concerns CEOs and CFOs. That's why the security of this kind of information needs more attention from us - Information Security practitioners. Therefore the Information Security Governance has a wide impact on enterprises, so is the impact of risks on the organization's activity [4].

Recently, decision makers tend to consider information security as a part of the IT governance process which makes their security program accurate and aligned with their business objectives.

It is clear that Information Security Governance is more than just Information Security Management. It shows the importance of the role of top management in the way of managing their company.

As a result, Information Security Governance is a whole part of Corporate Governance which consists of an organizational structure for applying a good information security whereas implementing the right policies, procedures, process, technologies and compliance enforcement mechanisms. It also makes sure of the full awareness and commitment of the board and top

DOI: 10.7763/IJCTE.2014.V6.904

management to maintain the confidentiality, the integrity and the availability of the company's assets.

B. The 4th Wave or Information Security Governance

Information Security Governance or the 4th wave is based on a "closed" loop which consists of six parts as showed in the figure below:

Fig. 1. Processes of information security governance.

This figure illustrates the importance of the involvement of the top management into security matters. Because not only the business should consider material risks but also human defects. People who work for companies tend to misuse the business information leading a bad manipulation of the companies IT resources. The risks of committing frauds and misusing financial resources became prominent in any organization. Therefore, the companies had to protect their business information from such maneuver [5].

Top management started to integrate Information security into their strategic approach of good corporate governance. These risks can appear in different forms from scams, financial theft, and espionage to social engineering, but the most common in the IT industry is social engineering i.e. when people use psychological manipulation into divulging confidential information which seems to be rising recently.

Through IT devices, employees have opportunities to commit fraud that's why; Laws and regulations have been set to protect senior management.

Now that decision makers realized that Information security should be part of their strategic governance. In many companies, Information security technical practitioners started to take high responsibility in corporate boardrooms. We realize that Information Security Governance is not a technical problem but depends on compliance and operational management which should be followed by formal reports to be sent to top management.

We must use this development to ensure an optimal state of Information Security systems.

From another perspective, following the PDCA approach is also a way of implementing Information Security Governance. When a company commits to a certain project, they put all of their efforts into making achieving the results. Sometimes reaching these goals can be vigorously rough and the consequences more significant. In fact, it would be better to produce a conduct for this project to make sure that your resources aren't misemployed. A process has been created to satisfy these purposes which are referred as PDCA, the Deming cycle or even the Deming wheel.

In order to explain the Deming cycle, we need to view in details the Plan, Do, Check, Act phases.

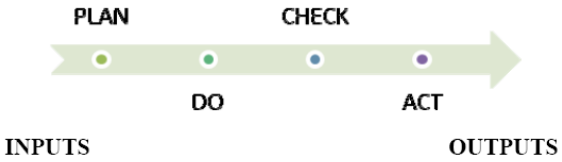

Fig. 2. PDCA cycle.

A traditional process has required inputs and obligatory outputs. The same manner applies to the Deming cycle; in each phase we find incomes, process and outcomes. In the process, we detail the set of procedures and policies to address. There can be as much repetition of these phases into refining the results.

The Deming cycle applied to Information Security governance can be resumed on the following steps:

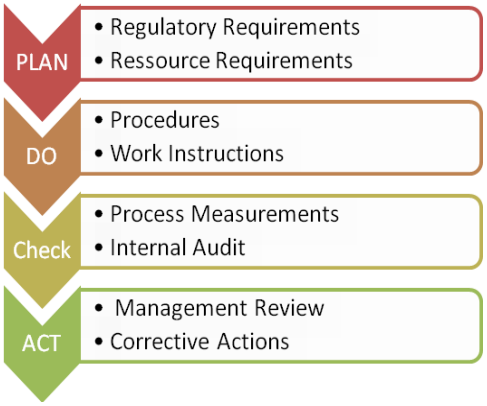

Fig. 3. PDCA Cycle applied to ISG.

C. IT Risk Methods and Frameworks

During the exchange of this information, it must be protected from a number of threats that can affect its quality. To preserve the quality of this information should be taken into account three parameters confidentiality, integrity and availability that can be defined as follows:

- Confidentiality: The information must be protected against unauthorized interception or publication.
- Integrity: The accuracy and completeness of the information must be guaranteed.
- Availability: The information must be available when needed.

The information security is provided by the establishment of a set of measures which may be company's policies, procedures, practices, organization or software features.

As a matter of fact, there are several standards, methods or frameworks that help companies improve risk management in their system.

Different comparative studies (Table I, Table II) have been conducted by researchers and software vendors for methods or frameworks [6].

TABLE I: COMPARATIVE STUDY ON RISK ANALYSIS METHODOLOGIES

Criteria	Qualitative			Quantitative		
Method/Tools	OCTAVE Method/Tools	CORAS Tools	CRAMM Method/Tools	ISRAM Method/Tools	CORA Tools	IS Method/Tools
Method/Tool Name	Octave v2.0 Octave –S v1.0	Coras Editor v1.1	CCTA Risk Analysis and Management Method	ISRAM	CORA 5.0	IS Risk Analysis based on a Business Model
Vendor Name	Carnegie Mellon University, SEI(Software Engineering Institute)	European Commission	Insight Consulting	National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology	International Security Technology, Inc	Korea Advanced Institute of science and Technology
Country of Origin	USA	Intracom(Greece) Solinet(Germany) Telenor(Norway)	United Kingdom	Turkey	New York	Seoul, Korea
Date Of First Release	Version 0.9.1999	January 2001	1985	December 2003	1978	2002
Languages	English	English	English, Dutch, Czech	English	English	English
Price	Free	Free	Unknown	Free	$ 7000 - $85000	Free
Compliance to IT standards	N/A	ISO 31000 ISO/IEC17799 AS/NZS4360	ISO/IEC17799	NIST SP 800 - 30 ISO/IEC17799 ISO/IEC13335	N/A	N/A
Skills Needed	Standard	Standard	Specialist	Standard	Standard	Standard
Availability	Trail Version available, registration required	Trail Version available, registration required	Registration Required	Open	Licensing organization without limit	Open
Tools Supporting the method	Commercial Tools Licensed materials Trainings	An XML Markup for exchange of risk assessment data A UML based specification language targeting security risk assessment	Commercial Tools CRAMM Expert(Insight) CRAMM Express (Insight)	Key Risk Management Tool for information	N/A	N/A

TABLE II: COMPARATIVE STUDY ON RISK ANALYSIS METHODOLOGIES

Attributes / Methods	Risk identification	Risk Analysis	Risk Evaluation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only) (Information assessed in June 2006)	Size of organization	Skills needed[8]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	•••	•••	•••	•••	DE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	EN, FR, DE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•				•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001					•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	EN, DE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE
Octave	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••		EN	Free	All	**	N	N	

We note that in terms of methods of managing risk, EBIOS method and IT-Grundschutz are the most effective and widely used. These methods are similar in terms of attributes.

* basic level, ** standard level, *** Specialist [6].

The symbols (•, ••, •••) Used in the table vary between 0 and 3. They specify the degree of fulfillment of the phase by the method chosen.

Between all of these methods, some of them are considered very helpful and legitimate from theirs users, It managers or researchers are confronted with the frightening task of choosing one. The proposed architecture will help them use only the processes that they need in their organizations.

D. Multi-Agents Systems

Multi-agents systems came to relieve the pressure on software applications that were build in response to real problems. The use of agents and artificial intelligence, computers has become more than just tools but actors in their environment.

The objective of the Multi-Agent System (MAS) is to use methods for the creation of highly distributed control agents.

Agents work is supported by fast auto-determination decision process. This behavior operates well in response to critical environments, where the intelligent agents expect synchronous responses, as opposed to pure MAS, where asynchronous communication is the core mechanism. In this work, the agents operate in both domains, asynchronous and synchronous. The MAS architecture is organized according to the following and major features [7]:

- Autonomy. Each intelligent agent makes its own decisions and is responsible for carrying out its decisions toward successful completion.
- Cooperation. Intelligent agents combine their capabilities into collaboration groups (clusters) to adapt and respond to diverse events and mission goals.
- Communication. Intelligent agents share a common language for cooperation
- Fault tolerance. Intelligent agents possess the capability to detect equipment failures and to isolate failures from propagating. This has special value in the detection of water leakage in CWS systems
- Pro-action. Intelligent agents periodically or asynchronously propose strategies to enhance the system performance or to prevent the system from harmful states [8].

Agent planning is carried out in three main phases: creation, commitment, and execution. During creation, an intelligent agent initiates a collaborative decision making

process. The intelligent agents offer a solution for a specific part of the request. Then, the intelligent agents commit their resources to achieve the task in the future. Finally, the intelligent agents carry out the execution of the plans.

The purpose of using multi-agents systems in our architecture is to help the IT manager should the right processes for his information Systems [9].

III. Proposed Architecture

Our aim is 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. Fig. 4 is presented in the following manner:

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 [1].

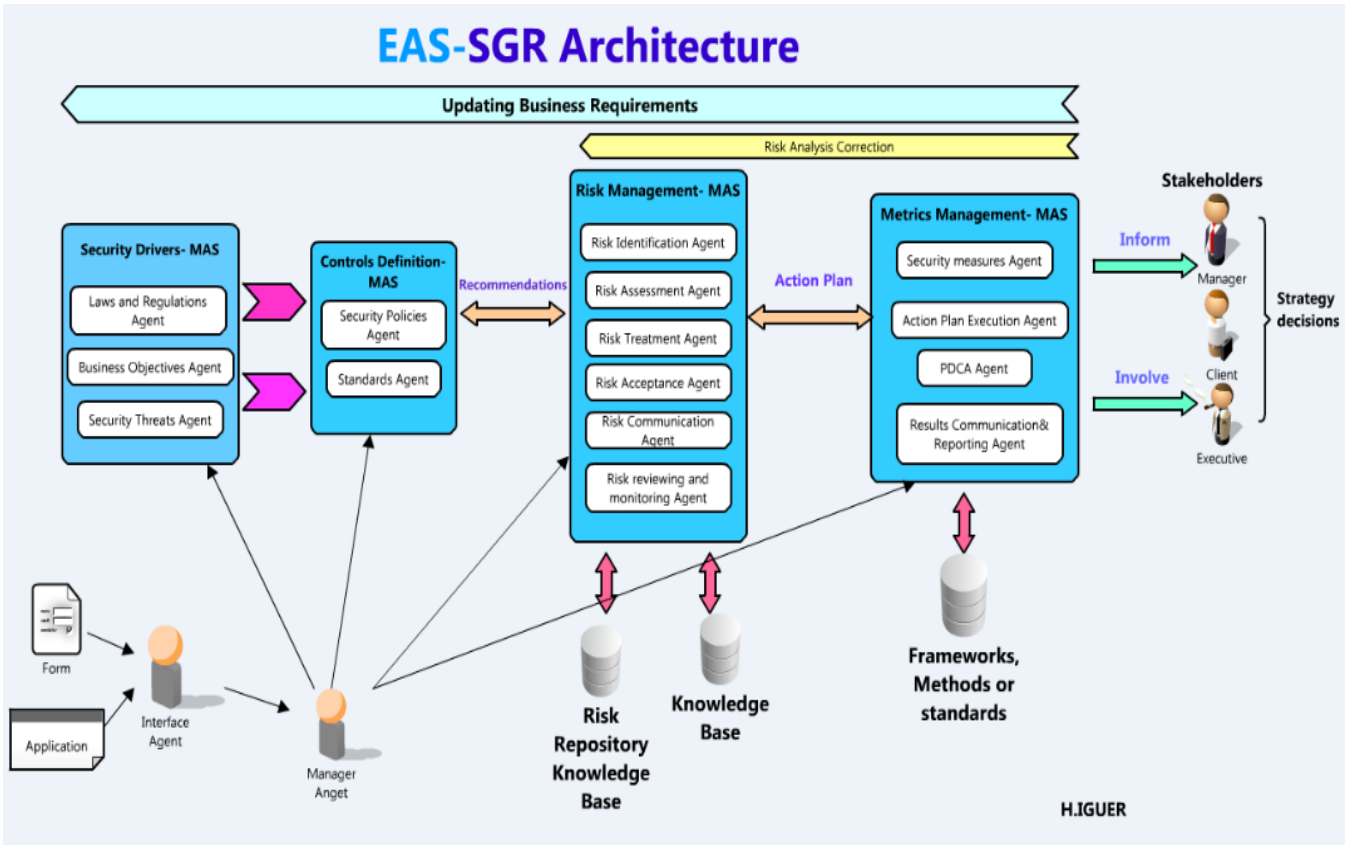

Fig. 4. Proposed architecture EAS-SGR (Equipe d'Architecture des Systèmes – Système de gestion de Risque).

EAS-SGR is made of four essential MAS; security drivers, controls, risk management and metrics management. Each part is a multi-agent system. The security professionals exist to help the company achieve its business objectives. Consequently, it should follow certain rules and regulations to avoid facing legal actions. It also has to be aware of the externals threats in order to manage them throughout the process.

Once all drivers are set, the company needs to set a series of policies, standards aligned with the drivers, to be followed by the security professionals. Every security solution should be put in a security repository to achieve steady security. Thus, these recommendations need to be considered for risk management MAS. Thereby an action plan is sent to apply metrics management for this risk.

Accordingly, we try to improve the metrics management MAS and correct the risk management if there is any improvement. The final step after the implementation is to inform all stakeholders and decision making managers with the final results. As a result, the stakeholders must ensure that the results meet their expectations if this isn't the case they need to update their business goals to the security drivers MAS [9].

A. Security Driver-MAS

Without any drivers, they would be no security at all that's why we intended to add the security drivers MAS. This multi-agent system is composed with three agents.

1) LR agent (Law and Regulations)

This agent collects law and regulations that the company must comply with in order to avoid facing legal action. An example of a law is the data protection law.

2) BO agent (Business Objective)

This agent is responsible for gathering the company business objectives. Security supports these objectives by offering a full protection for their systems and for information used in the business process.Its aim is to keep the system running and protect it from attacks.

3) ST agent (Security Threats)

This agent is in charge of conducting information security to respond to threats.

B. Controls Definition-MAS

Control Definition –MAS is held controls which are a set of policies, standards and guidelines that describe how the company addresses information security drivers. There are also International standards which can be available to be implemented. This multi-agent system is composed with two agents [10].

1) SP agent (Security Policies)

This agent describes security controls objectives including the alignment of policies with the business objectives and drivers.

2) S agent (Standard)

This agent ensures that security controls follow an international catalogue of controls. It also has to detail all the security controls that should be applied to support policies.

C. Risk management-MAS

The third part is the MAS Risk Management where we go through the analysis of risks as details in EBIOS processes. This multi-agent system is composed with six agents.

1) RI agent (Risk Identification)

RI has to define the scope of the risk

2) RAS agent (Risk Assessment)

The agent has to evaluate threats and vulnerabilities to understand and measure the impact of the risk involved.

3) RT agent (Risk Treatment)

RT agent has to select between different measures to modify risks that have been assessed.

4) RAC agent (Risk Acceptance)

RAC agent makes decisions in order to accept a risk by the organization management. Risk acceptance depends on risk criteria defined within the RI agent (risk identification).

5) RC agent (Risk Communication)

This agent is accountable for the exchange and share of information about risk between the decision-maker and other stakeholders inside and outside an organization.

6) RRM agent (Risk Reviewing and Monitoring)

RRM agent is under obligation to review and monitor the risk analysis management.

D. Metrics Management-MAS

The fourth part is the MAS Metrics Management where we apply risk measurement. This multi-agent system is composed with four agents

1) SM agent (Security Measures)

This agent is in control of aligning policies statement with business objectives

2) APE agent (Action Plan Execution)

This agent has to execute the action plan from the risk management MAS.

3) PDCA agent (The Deming Cycle)

This agent has to make sure that there is a continual improvement of the metrics management.

4) RCR agent (Results Communication & Reporting)

This agent carries the authority to communicate results to managers, stakeholders and executives and to achieve some reports.

Now that we've presented our multi –agents systems, let see what kind of agent are handling the communication and the interaction between these MAS. There are two major agents: Interface Agent and Manager Agent.

When the employees are logged into the application through forms they need to fill out or web interface or even when the administrator is logged for approving processes, the interface Agent manages the layout of all of the interfaces presenting all the processes handles by the all of the agents [11].

The Manager Agent is a cognitive agent having to dispatch the requests of the application's user in which are stored all the processes. When the user connects to the web interface, it specifies the goal that the company wants to achieve, it is displayed by the interface agent and translated by the manager agent that identifies and makes it understandable to the platform so that the agent knows what MAS that will be used.

On one hand and as you can see on Fig. 4, the Risk Management- MAS is connected directly with two databases: Risk Repository Knowledge Base and the General knowledge Base. The Risk Repository Knowledge will be accessed when the risk encountered was already treated and corrected while the general knowledge base will be accessed the risk identified is new to the processes and all of the parameters needs to be calculated [12].

A risk is defined by the relation below:

$$\text{Risque} = \text{Likelihood} \times \text{Impact}$$

The impact of a risk is calculated based on the DIC (Disponibility, Integrity and Confidentiality) parameters. Every parameter is given a number following the classification table of ISO 27005, which is the ISO standard for risk management [13].

The probability is defined as follow:

$$\text{Likelihood} = ((\text{Exposure} + \text{Frequency})/2) \times (\text{Control Inverse})$$

The control: is a value that must induce the results of the audit done before in the definition section of the context.

Exposure and frequency are proportional to the likelihood. Against the Reverse Control is inversely proportional to the probability, the greater the control over the probability is much reduced. Hence in formula is multiplied by the inverse of the value of the control.

On the other hand, the Metrics Management- MAS is also connected to another knowledge base which is Frameworks, Methods or standards. Agent of Metrics Management can access it to choose only the processes that the company need for securing their systems [14].

These results are useful in supporting decision making processes and raising critical dependencies between risk projects. EAS- SGR reduces the complexity of IT risk management by aligning IT operations management with corporate business initiatives, strategy, and regulatory requirements and by selecting the processes that the

organizations need.

IV. Conclusion

We started our paper with a state of art of the all the methods and standards that exists in this domain. Then we introduced multi-agents systems which are the key element of our research and finally in this paper we proposed a new generic model in IT risk management based on multi-agents systems and Information Security Governance EAS-SGR (RSIS) in order to control and manage the security of their systems. In fact, the use of multi-agents systems in the governance of information system is considered an innovation in researches in the domain of artificial intelligence. Indeed, 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. In future articles, we will detail the role and functioning of each agent which support our EAS- SGR architecture whereas we will study further the applicability of our model for e-learning systems.

In our future work, we will be able to describe in details the job and all the scenarios that involve the participation of every agents and multi-agent 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. This work was supported in part by the National School of Electricity and Mechanics and the International University of Casablanca.

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, pp. 126.

[2] B. V. Solmsa and R. V. Solms, "From information security to.business security?" *Computers and Security*, vol. 24, pp. 271-e273, 2005.

[3] N. Y. Kim, R. J. Robles, S. E. Cho, Y. S. Lee, and T. H. Kim," Sox act and IT security governance," in *Proc. International Symposium on Ubiquitous Multimedia Computing*, 2008.

[4] R. V. Solmsa and S. H. B. V. Solms, "Information security governance: A model based on the direct–control cycle on computers and security," *Computers and Security*, vol. 25, pp. 408 – 412, 2006.

[5] B. V. Solms, "Information security – the fourth wave," *Computers and Security*, vol. 25, pp. 165 –168, 2006.

[6] N. Shukla and S. Kumar, "A comparative study on information security risk analysis practices," in *Proc. ICNICT 2012, Issues and Challenges in Networking, Intelligence and Computing Technologies*, November 2012.

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

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

[9] F. Q. Aniba, H. Medromi *et al.*, "Remote control architecture over internet based on multi agents systems," *International Review on Computers and Software (I.R.E.CO.S)*, vol. 3, no. 6, pp. 666–671, November 2008.

[10] S. J. Russell and P. Norvig, *Artificial Intelligence: A modern Approach*, Prentice Hall, 3rd ed. 2009.

[11] M. Wooldridge, *An Introduction to Multiagent Systems*, Chichester, UK: John Wiley & Sons, 2002.

[12] Y. B. Khoo1, M. Zhou, B. Kayis, S. Savci, A. Ahmed, R. Kusumo, and H. Bokhari, "An agent based risk management tool for concurrent engineering projects," *Complexity International*, vol. 12, 2005.

[13] *Multi-Agent Systems – Modeling Control, Programming, Simulations and Applications*, InTech, April 4, 2011.

[14] N. Otan, "Risk analysis tools," *Improving Common Security Risk Analysis*, ch. 5, 2008.

H. Iguer was born in Casablanca on January 25, 1989. She 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).