Expert Systems and Multi Agent Systems for Information Security Risk Management and Audit

Sophia FARIS, Hicham MEDROMI, Adil SAYOUTI

***Abstract*— Governing the security of information became an increasingly important challenge for all executive levels of every organization.**

It is extremely important that security has to be addressed through the whole system development process, not in a late stage i.e. development or maintenance.

An effective risk management can protect organizations and maintain their ability to carry out their missions and activities against threats as well helping them to implement relevant controls to their information systems.

Our work is part of a project resulting from the collaboration of the systems architecture' team (EAS) that proposes an IT GRC (Governance, risk and compliance) architecture for a high level of IT GRC management.

Our solution focuses on IT risks and proposes a new approach of security and audit which aims to provide security managers recommendations to justify their information security management decisions.

The EAS-OISRMA (Organization Information Security Risk Management and Audit) solution proposed in this paper is based on multi-agent systems and expert systems.

These two concepts provide significant advantages in information security and audit areas.

This paper discusses the conception of EAS-OISRMA which is a web-based application module that serves as a tool for handling with security issues.

EAS-OISRMA is a tool dedicated to auditors, information system security managers (ISSM) and business decision makers to help them manage the security incidents through their information systems, and take the best decisions in an intelligent way in order to mitigate risk in their platforms to achieve business goals.

Index Terms— **audit, expert systems, information security risk management, information systems, multi agent systems.**

I. Introduction

Nowadays, information systems have become necessary for all organizations; they respond to a multitude of their needs and allow them to manage their customers, purchases, production, accounting, etc.

Over the last few decades, the relationship of dependence between the organizations and the information system had become more complex with the spread of the Internet.

These systems can cause serious damages if they are not working properly or if they are insufficiently protected.

The information system has become very important and has a very high value; the security of this system has become an important strategic issue.

Users and administrators of computer networks have realized this and are aware of the need of protecting the system.

Information is a strategic resource used in all decision-making processes, it is essential to ensure its availability, integrity and confidentiality.

The issue of security is difficult to manage because organizations share information not only with their collaborators but also to external networks.

It is therefore necessary to take into account significant risk factors such as: changes (legislation, environment, technical and technological progress), the globalization of markets and mergers, acquisitions and the multiplication of partnerships.

The lack of information security within the organization significantly impacts the continuity and credibility of its business.

The information systems are permanently exposed to a large range of threats, which threaten to compromise the confidentiality, the integrity and the availability of the information. Within the organizations, the security of information system is more and more handled using approaches based on risk's management solutions. Several organizations lay and implement security policies, sometimes formalized, sometimes empirical. Some go until obtaining Information Security Management System (ISMS); security managers of information systems have the obligation to control technological risks, but also to contribute in the improvement of the performance of the business processes.

So a governance of the information security is essential and mandatory for all organizations.

Threats to information systems are various; they involve a number of components and are grouped into categories.

The major categories of threats are: software, hardware, data, network, physical, personnel, and administration.

Both external and internal threats present security issues for organizations.

Moreover, regular audits of information security should be conducted in the organizations in order to ensure a good level of security.

Automating the audit process will reduce costs, speed up the audit process and improve the quality by complying with international security standards.

In this paper, we propose an architecture for an intelligent system for information security risk management and auditing (EAS-OISRMA) which supports the security and audit processes within an organization.

The system supports knowledge acquisition to assist the human user in the problem solving of information security and security audit domains.

This paper is presented as follows: the next section gives the state of the art in information security risk management and

Sophia FARIS, Department of computer sciences, Team of Systems' Architecture, Laboratory of engineering research, National and High School of Electricity and Mechanics (ENSEM), Hassan II University, Casablanca, Morocco

Hicham MEDROMI, Department of computer sciences, Team of Systems' Architecture, Laboratory of engineering research, National and High School of Electricity and Mechanics (ENSEM), Hassan II University, Casablanca, Morocco

Adil SAYOUTI, Professor at Royal Naval School (ERN), HASSAN II University ,Casablanca, Morocco

information security audit, then in the third section we present an overview of the IT GRC architecture developed by our team.

The fourth section discusses our proposed architecture EAS-OISRMA.

The fifth and sixth sections describe the multi agent systems of our proposed architecture. The seventh section presents our expert system proposed before concluding this paper.

II. State of the Art

Information is one of the most important assets in the organizations, it increases their value; that is why it must be protected properly.

It is a common misconception that information security deals specifically with computer security. But in fact, it addresses the need and desire to protect information from a wide range of threats in order to ensure business continuity, minimize business risks and maximize return on investments and business opportunities.

According to the international standard of good practices in information security ISO 27002, information security is the preservation of the confidentiality, integrity and availability of information. More other properties such as authenticity, responsibility, non-repudiation and reliability may also be involved.

- **Confidentiality** (C): All information must be protected according to the degree of privacy of their content, aimed at limiting its access and used only by the people for whom they are intended;
- **Integrity** (I): All information must be kept in the same condition in which it was released by its owners,
- **Availability** (A): All the information generated or acquired by an individual or institution should be available to their users at the time they need it,

A. *Concepts of ISSRM*

The purpose of ISSRM (Information System Security Risk Management) is to protect assets of an organization, by using a risk management approach.

It is inspired by, and compliant with the existing security standards.

The concepts of ISSRM are:

- ✓ **Assets:** An asset is anything that has value to the organization and is necessary for achieving its objectives. A business asset describes information, processes, capabilities and skills inherent to the business of the organization, and that has value for it. An IS asset is a component of the IS supporting business assets.
- ✓ **Security criterion**: It characterizes a property or constraint on business assets. They are most often confidentiality, integrity and availability, but sometimes, depending on the context, other specific criteria might be added, like non-repudiation or accountability.
- ✓ **Risks:** A risk is the combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. An impact describes the potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or the cause of a risk) is accomplished. The event, in the frame of IS security, is the combination of a threat and one or more vulnerabilities.
- ✓ **Vulnerability**: A vulnerability describes a characteristic of an IS asset or group of IS assets, that constitutes a weakness or a flaw in terms of IS security.
- ✓ **Threat**: A threat characterizes a potential attack or incident, which targets one or more IS assets that may lead to a harm for the assets. A threat agent is an agent that can potentially cause harm to IS assets. An attack method is a standard means by which a threat agent carries out a threat.
- ✓ **Risk treatment:** describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. A risk treatment is the decision of how to treat an identified risk. A security requirement is the refinement of a risk treatment decision to mitigate the risk.
- ✓ **Controls**: Controls (or countermeasures) are means designed to improve security, specified by a security requirement, and implemented to comply with it.

B. *Security Risks analysis methods*

Today a number of methods are available to Chief Information Security Officers (CISO's) in organizations for performing risk analysis of security issues and identifying solutions that are the most adequate in the context of the alignment of the business with an IS solution.

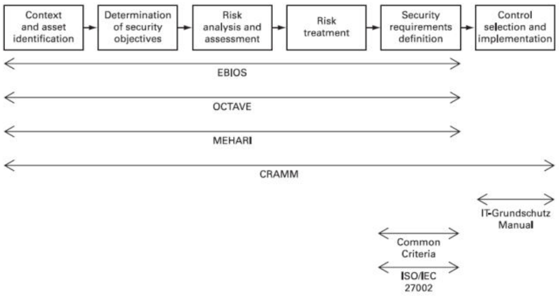

Context and asset identification
Determination of security objectives
Risk analysis and assessment
Risk treatment
Security requirements definition
Control selection and implementation
EBIOS
OCTAVE
MEHARI
CRAMM
IT-Grundschutz Manual
Common Criteria
ISO/IEC 27002

Fig.1 Classification of some risk management methods

Risk management is a major component of information security management.

Risk management methods and tools give the organizations the ability to plan and implement programs to control impact of potential threats.

A large number of methods are available on the market, their main difference is the importance given to the risk management activities as shown in figure 1 above.

Some of them are only providing best practices and propose a set of security requirements to implement for example the standard ISO 27002 which we choose to work with in order to guarantee a good level of security in an organization's information system.

Although these existing methods cover the activities of risk management, they present some disadvantages such as a lack of well-defined concepts, detailed analysis and a systematic approach.

The work presented in this paper is motivated by the lack of integrated solutions of information security and audit developed in the Moroccan research laboratories.

Our proposed solution has the objective of providing a better support in the formalization of information and knowledge of information security risk management.

It is based on an intelligent system as a software system to ensure effective information security controls over information resources.

C. Information Security Auditing

The information security audit of an information system is a complex activity covering all the components of the IS and consists of evaluating the level of security and proposing the appropriate means of correction.
This evaluation covers the following areas:

- **Organizational and physical audit**: It allows making a complete inventory of the security of the IS and identify the dysfunctions and the potential risks.
  During this audit the following elements can be addresses: information security policies, information security organization, human resources security, asset management , access control, cryptography, physical and environmental security, security related operation, communications security, IS development and maintenance acquisition, supplier relations, information security aspects of managing business activity continuity, and compliance.

In our case, the organizational and physical allows the possibility to verify the compliance and the relevance of the measures deployed in relation to the organization's security policy and to the ISO 27002 good practices framework.
Our proposed multi-agents auditing system performs this first level audit using questions and answers.
This phase is bases on the use of questionnaires adapted to the context of the audited organization, the interviews and the analysis of the resources and documents provided.

- **Technical security auditing**: This is an evaluation that enables the in-depth analysis of the IS (active systems, applications, components and equipment of the network infrastructure, internal access networks, interconnection networks, etc), in order to identify potential technical vulnerabilities.

III. OVERVIEW OF THE GLOBAL IT GRC ARCHITECTURE

The Architecture Systems Team (EAS: *Equipe Architecture des Systèmes*) focused on Governance, Risk management and Compliance of information systems (IT GRC) by proposing a global EAS-IT GRC architecture that provides a high level of IT management.
There is no IT GRC platform developed in the Moroccan research laboratories; that is the reason that motivates the work of the team.
EAS-IT GRC allows the integration of several frameworks of good practices within the same platform, enabling decision-makers and managers to choose from a wide range of frameworks that are the most adapted to the context of their organizations, and helping them achieve their business objectives in an efficient manner.
In this section, we give an overview of the common architecture EAS-IT GRC which provides a high level model for integrated IT Governance, IT Risk and IT Compliance processes (Figure 2).
In order to understand deeply the common architecture, we describe below each layer of the EAS-IT GRC platform.

- **Strategic Layer**: EAS-Audit is an IT Governance (ITG) platform based on COBIT framework; ensuring permanent alignment of IT and Business with stakeholders' participation.
- **Decision making layer**: This layer allows us to propose the best reference to perform for each request
- **Communication layer**: This layer ensures communications between all the layers of the IT GRC platform.
- **Processing layer**: This layer contains different systems, which can be implemented, responding to communication layer's alert. Our system OISRM is included in this layer. We will present it in detail in the next section.

The figure below illustrates the global architecture proposed by the EAS team.

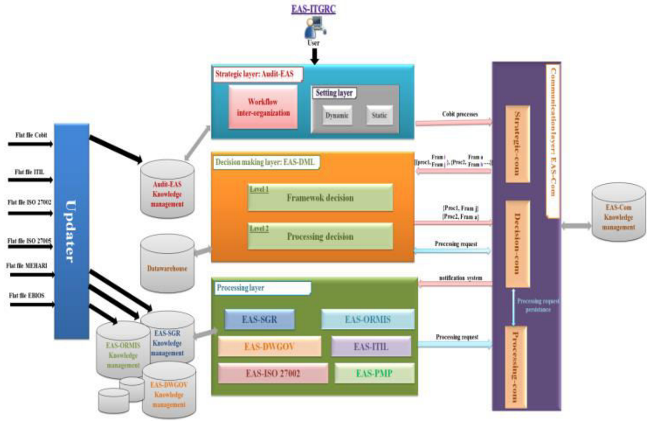


Fig.2 EAS-IT GRC architecture

IV. PROPOSED ARCHITECTURE EAS-OISRMA

The aim of this paper is to contribute to the domain of information security by proposing a solution whose objective is the management of information security risks and audit.
To achieve this goal, we equip the EAS- IT GRC global platform with an information and audit security risk management solution EAS-OISRMA based on multi-agents systems, using an expert system and complying with the standard ISO 27002.
Unlike the other solutions that exist in the IT market, the solution we propose in this paper is generic, distributed based on the multi-agents systems, and can integrate a lot of frameworks of good practices.
EAS-OISRMA is an ergonomic and easy-use toolkit that can be used by any user regardless of his level of expertise in the field on information security.
It is intended to the organizations in order to adopt the standard ISO 27002, automate the activities required for risk management, and perform a compliance audit to identify the gaps between the organizations' practices and those recommended by the standard.
This solution will enable organizations to assess the state of the security within their information systems, effectively manage their risks, conduct compliance audits and provide recommendations for the evolution of their IS.
The main qualities and properties of our proposed architecture are:

- **Intelligence**: Under this word are gathered various groups of events and activities such as the adaptation of the means for the realization of a goal, the use of real or abstract tools for an action, the construction of representations of external of internal phenomena which then are used for the preparation of future actions.

In our case, intelligence will be used to collect, standardize and analyze in real time data generated by users, applications, and infrastructure that impact IT security.
Its goal is to provide an actionable and comprehensive overview that reduces risk and operational effort for any organization size.

- **Autonomy**: It is the ability to resist to external perturbations by using its internal resources.
  It is a relative and not an absolute faculty. For an information system, it is linked to its capacities of decision and action, strength, energy resources, perceptive sense, the characteristics of the environment in which it is plunged and its variations, and the tasks it must performs.
  The essential advantage of autonomy is the capacity of an autonomous system to explore possibilities for action and to decide what to do next with little or no human involvement and to do so in unstructured situations that may have great uncertainty.
- **Adaptation**: It consists of the ability to maintain performance when facing the variations in the environment, tasks to be performed or its own capabilities.
  For an information system, it is the ability to adapt quickly to market changes, new standards, regulations and laws.
- **Learning**: It is a process of knowledge acquisition. For an information system, this knowledge can relate to its environment, the relationships between its actions and perceptions, and the relationships between its behaviors, goals and achievement.
  This is usually a long process and requires relatively favorable conditions in order to be carried out. The system generally uses a learning base which must be representative of the phenomena to be learned and of the conditions in which they are encountered. Some knowledge needs to be provided to the system such as knowledge that is too high or unattainable to acquire.

Our proposed solution is modular, integrates the various capacities previously mentioned and is based on multi-agents systems.
A multi-agents system is a set of agents that possess a certain degree of autonomy, a certain degree of artificial intelligence, a representation of their environment; they interact with it, they are able to take the initiative, and they can adapt to different situations.
The need for these concepts at different levels of our proposed architecture indicates the need of autonomy and intelligence, and validates our choice of MAS approach.
Jennings and Wooldridge [Jennings & Wooldridge 1998] have defined an agent as "a computer system located in certain environment which is able to act autonomously in this environment, in order to meet its design goals".
In the architecture EAS-OISRMA we propose, agents are able to monitor and extract the security information, using the domain knowledge provided in the form of practicable rules, and can reason in order to achieve the established security goals.
The figure 3 below illustrates our proposed architecture.

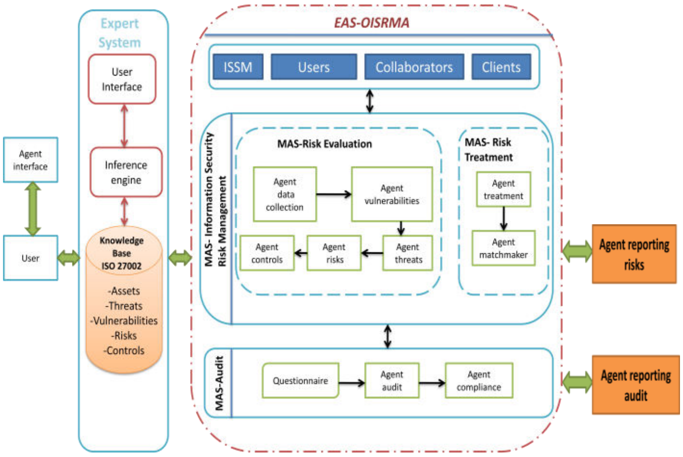


Fig.3 EAS-OISRMA architecture

The objective of EAS-OISRMA is to offer Information System Security Managers a toolkit in order to adopt ISO 27002 to automate information security management and information security audit processes.
Two integrated multi agent systems constitutes the EAS-OISRMA toolkit: "MAS-Information security risk management" and "MAS-security audit".
Our system of ensuring security in information systems involves the following steps:

- ✓ **Asset identification**: Identify assets to be secured and their value to the organization.
- ✓ **Vulnerability assessment**: Identify potential security vulnerabilities that could be exploited by threats.
- ✓ **Threat assessment**: Identify threats against assets and evaluate their potential to happen.
- ✓ **Recommendations**: Identify and evaluate threat mitigation options.

Our system asks the user a set of questions of various forms, analyzes the answers to questions using its knowledge base, and calculates security risks together with giving recommendations for improving security level.
Our architecture is composed of two multi agents systems which we will detail in the next sections.

V. MAS- Information Security Risk Management

The aim of this MAS is to collect the necessary elements for managing information security risks, so that it can be implemented in good conditions, adapted to the context of the organization, and provide relevant results that are usable by the stakeholders.
It is composed of two MAS namely: MAS-risk evaluation and MAS risk treatment.

A. *MAS-Risk Evaluation*

The purpose of the risk assessment is to define and evaluate risks based on the results of asset evaluation, vulnerability evaluation and threats evaluation.
The risk calculation process is explained below.
The output data from this process is to identify appropriate controls to reduce or eliminate the risks during the risk mitigation process.

It is composed of several agents that are describes below:

- **Agent data collection:** This agent is responsible of gathering all the data about the assets and the organizations communicated by the users in the questionnaire.
  After that, it has the role of displaying to the user the criteria (C,I,A) of security in order to evaluate the assets. Then, it calculates the value of the assets with this formula: VA= max(C,I,A), and sends all these information to the agent vulnerability. In order to evaluate the assets, we use the following variables:

Value	Description
1	The asset is public
2	The asset must be accessible to the staff and partners
3	The asset must be accessible only internal staff.
4	The asset must be accessible only internal staff involved
5	The asset should be accessible to identified persons and having need to know

TABLE.1 CONFIDENTIALITY PARAMETER

Value	Description
1	The asset may be unavailable more than 30 days
2	The asset may be unavailable more than 72 hours
3	The asset must be available within 72 hours
4	The asset must be available within 24 hours
5	The asset must be available within 4 hours

TABLE.2 AVAILABILITY PARAMETER

Value	Description
1	loss of integrity has no consequences
2	loss of integrity has insignificant consequences
3	loss of integrity has consequences
4	loss of integrity has significant consequences
5	loss of integrity has big consequences

TABLE.3 INTEGRITY PARAMETER

- **Agent vulnerabilities:** Its goal is to associate vulnerabilities to the assets identified earlier. It evaluates the vulnerabilities from 1 to 5 according to the table below.

Value	Description
1	Very important
2	Important
3	Moderate
4	Unlikely
5	Very unlikely

TABLE .5 VALUES OF VULNERABILITIES

- **Agent threats**: Its goal is to associate threats to the assets identified earlier . It evaluates threats from 1 to 5 according to the table below.

Value	Description
1	Very important
2	Important
3	Moderate
4	Unlikely
5	Very unlikely

TABLE.6 VALUES OF THREATS

- **Agent risks**: It associates the risks to the assets identified earlier and calculates the impact of this risks on the assets with the formula:

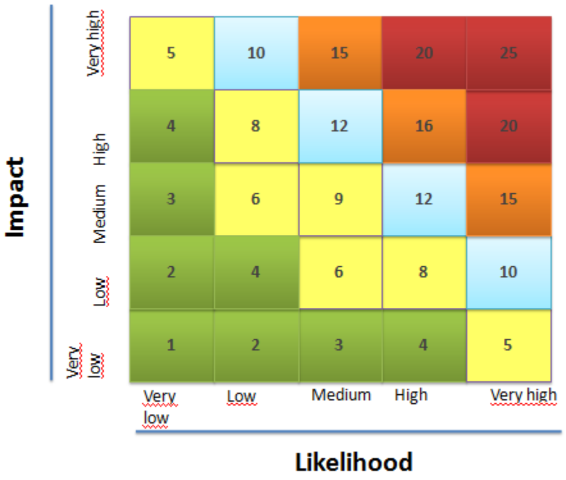
Value of risk= Value of the asset x Value of the threat x Value of the vulnerability

Value	Description
1	Very important
2	Important
3	Moderate
4	Unlikely
5	Very unlikely

TABLE. 7 VALUES OF RISKS

Its objective is to systematically highlight and assess the risks to the information system.

After calculating the level of the risk, the system displays the matrix of risks levels as illustrated in the figure below.



Impact	Very low	Low	Medium	High	Very high
Very high	5	10	15	20	25
High	4	8	12	16	20
Medium	3	6	9	12	15
Low	2	4	6	8	10
Very low	1	2	3	4	5

Fig. 4. Matrix of risk level

Using this matrix, the manager have an on-screen overview of all risks and there classifications.

The green area is for acceptable risks.

The yellow area is for risks that can be accepted or transferred.

The blue area is for risks that must be monitored.

The orange area is for risks that must be treated.

The red area is for risks that should be treated and reduced, because they have a significant impact on the assets.

- **Agent controls**: It associates controls to assets identifies earlier.

- **Agent reporting risks**: Its role is to generate reports from the study of information security and audit containing the dates of the study, the persons who conducted the study, a summary of risks affecting the assets, and the action plans that have been taken in order to improve security in the information system.

B. *MAS-Risk Treatment*

There are four basic ways to deal with risks:

- **Transfer**: transfer the risk to an insurance company
- **Reject**: ignore the risk and eliminates the risk situation
- **Reduce**: the organization suggests controls to be implemented in the information system according to their effectiveness and cost of implementation
- **Accept**: the organization accepts the risk and doesn't implement countermeasures.

This MAS is composed of the agents below:

- **Agent treatment**: After the risk evaluation, the user chooses to treat the risk.
- **Agent matchmaker**: In case of reducing the risk, this agent proposes according to ISO 27002 a set of relevant controls assigned to each risk.

A security control should be cost effective and should be decided based on some cost/benefit analysis.

In this step of selecting appropriate countermeasures to reduce the risk, the decision is based on the cost/efficiency measures.

For example:

Control: The existence of an information security policy document published, approved by the managers, communicated to all employees and reviewed.

Cost: Low

Efficiency: Medium

VI. MAS- Audit

The major goal of this multi agent system is to identify gaps between certain security standards (ISO 27002 in our case) and existing organization's security practices.

To achieve this goal, the user has to answer an audit questionnaire, which is based on the set of issues defined by the company employees.

The main criterion for development of questions is an approach audit and security compliance with ISO27002.

Thus, auditing process can be seen as a process of asking questions and making conclusions from answers.

The security audit part of our platform is responsible of producing reports concerning the evaluation of the security of the company's information system by measuring how well it conforms to a set of established criteria.

Our system asks provides number of audit questions regarding the standard ISO 27002 guidelines.

The questions are stated in yes-no-exclude form, and in case of no answers the system points security practices that need to be implemented and actions that should be taken.

Exclude as an answer means that the control of this domain is not relevant in the context of the organization.

These questions cover all the domains of ISO 27002, and the user is prompted to enter values as an answer to the control of each domain.

The user must enter a value from 0 to 5 based on one of the elements of answer below. Note that these values are from the Capability Maturity Model[2] (CMM).

0Non-existent: Total lack of identifiable process. The company has not even realized it was a problem to be studied.(This value is entered by the user in case of a no answer).

1 Initial: Processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.

2 Repeatable: Basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.

3 Defined: An organization has developed its own standard software process through greater attention to documentation, standardization, and integration.

4 Managed: An organization monitors and controls its own processes through data collection and analysis.

5 Optimizing: Processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

As and when the values are entered, a rosette is created, giving a photography of the current state of the security point of view for the subject area.

VII. EXPERT SYSTEM

Four main characteristics distinguish an expert system from a conventional program. They are listed as follow:

- **Expertise**: Expert systems use a large amount of knowledge about a particular domain, this knowledge is often subjective, possibly incomplete and subject to change.
  However, expert systems must have the skill to use this knowledge efficiently in order to solve complex problems quickly.
- **Symbolic reasoning**: In an expert system, the knowledge is explicitly represented in symbolic form, in a structure called the knowledge base.
  The inference engine manipulate this knowledge using a set of heuristic rules appropriate to the given domain.
- **Depth**: Expert systems operate in a narrow domain, dealing with hard and challenging problems. They have to use complex rules.
- **Self-knowledge**: An expert system has the feature of explanation capability. It should be able to explain how it has arrived at a particular conclusion.

Besides to that, an expert system can advise, modifies, update, expand and deals with uncertain and irrelevant data.

Our expert system is based on the data collection and analysis of the environment by the agents.
Its knowledge base contains the best practices of ISO27002.
Data collection is carried out by agents by means of questionnaires, and the answers are recorded, and analyzed by the expert system of our architecture.
The answers to the questionnaire should give a general picture of conditions to maintain information security in the company.
The expert system is the driver of our architecture: it collaborates with the three multi-agents systems in order to manage risks effectively.
The knowledge base of the expert system is filled with documents containing specialized knowledge in the field of information security.
The most commonly formalism used to represent the knowledge base is the production of rules.
Our system is based on rules base.
On the basis of these rules, the system displays the most appropriate controls to the assets based on their cost and effectiveness. Therefore, the user can select the controls which are adapted to its financial resources and its requirements in terms of effectiveness in reducing the risks.
The expert system we propose consists of the following steps:

- Identification of the assets (based on the questionnaire completed by the user);
- Assignment of the appropriate threats based on the type and value of the asset;
- Propose controls to cover the identified threats that impact identified assets;
- Selection of the most appropriate controls to reduce the risk to an acceptable level taking into account their cost and effectiveness;

VIII. CONCLUSION

The traditional information security risk management methods are lack of clear expression and granular analysis.
In this article, we proposed a new approach for handling security incidents and security audit which is based on an expert system compliant with the standard ISO27002, that gives the organizations an overview of the threats and vulnerabilities occurring in their information systems.
In a future work, we will verify the results provided by our system in a real organization in order to ensure a good level of security and achieve their business goals.
The main advantage of our proposed system is that it combines expert systems and multi agent system, in order to design a comprehensive information security risk management and audit tool and to add value to organizations by enhancing security.
The status of security of information system can be highlighted by using this tool.

ACKNOWLEDGMENT

I would like to thank my advisors Mr. H. Medromi and Mr. A. Sayouti for the efforts they made to review this paper and for the many useful suggestions they gave me during the work on this paper.
I would also express my gratitude to every person that has contributed to the achievement of this works.

REFERENCES

[1] S.FARIS, H.MEDROMI, A. SAYOUTI, "Multi Agent Systems Applications", International Journal of Engineering and Innovative Technology (IJEIT) 2017 Volume 6, Issue 7, January 2017

[2] H.IGUER, H.MEDROMI, A.SAYOUTI, S.EL HASNAOUI, S.FARIS, "Towards a multi-agents systems application based on the eas-sgr framework", Journal of Theoretical and Applied Information Technology (JATIT),Vol.71 No.1, January 2015

[3] S.FARIS, H.MEDROMI, S.EL HASNAOUI, H.IGUER, A.SAYOUTI. "Toward an effective information security risk management of universities' information systems using multi agent systems, ITIL, ISO 27002,ISO 27005". Digital Object Identifier (DOI) : 10.14569/IJACSA.2014.050617 -International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No. 6, June 2014

[4] S. EL HASNAOUI, H.MEDROMI, S. FARIS, H.IGUER, A.SAYOUTI, "Designing a Multi Agent System Architecture for IT Governance Platform", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 5, No.5, May 2014

[5] M.GHAZOUANI, S.FARIS, H.MEDROMI, A.SAYOUTI, "Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk", International Journal of Computer Applications (IJCA), October 2014

[6] S.FARIS, H.IGUER, H.MEDROMI, A.SAYOUTI. "New model multi-agent systems based for the security of information system". International Conference on Intelligent Information and Network Technology (IC2INT'13), Settat, Morocco, 13-14 Novembre 2013

[7] S.FARIS, H.MEDROMI, A.SAYOUTI. "A new information security risk management and audit framework based on multi agent systems and expert systems". International Conference of High Innovation in Computer Science (ICHICS'16), Kénitra, Morocco, 01-03 June 2016

[8] A.TOUNSI, S.FARIS, H.MEDROMI, A.SAYOUTI. "Multi-agents systems: Application to the governance of information systems", International Conference on Engineering Education and Research (ICEER'13), Marrakech, Morocco, June 2013

[9] A. CHAKIR, S.FARIS, S.EL HASNAOUI, H.MEDROMI, A. SAYOUTI. "Using multi agent system to make decisional chain reliable and benefic", International Workshop on Software Engineering and Systems Architecture, (SESA 2014), Tetouan, Morocco,13 Decembre 2014

[10] Adil SAYOUTI, Hicham MEDROMI, Sophia FARIS. "Multi-agents Systems : Application to Distance Education", International Conference on Engineering Education and Research (ICEER'13), Marrakech, Morocco, June 2013

[11] H.IGUER, H. MEDROMI, S. ELHASNAOUI, S. FARIS, A. SAYOUTI «The Impact of Cyber Security Issues on Businesses and Governments- A framework for implementing a Cyber Security Plan».

DOI: 10.1109/FiCloud.2014.56, IEEE International Symposium on InterCloud and IoT -ICI Symposium, 2014

[12] S.FARIS, H.MEDROMI, A.SAYOUTI," Expert systems and multi agent systems for information security and auditing", Journées Doctorales des Sciences de l'Ingénieur (JDSI'16), Casablanca, Morocco, Decembre 2016

[13] S.FARIS, H.IGUER, H.MEDROMI, A.SAYOUTI. "Conception d'une Plateforme de gestion des risques basée sur les systèmes multi-agents et ISO 27005". Journées Doctorales dans les Technologies de l'Information (JDTIC'13), Kénitra, Novembre 2013

[14] S.FARIS,H.MEDROMI,A.SAYOUTI. "Modélisation d'une plateforme (SIGRCI) à base des systèmes mutli-agents and ITIL". Journées Doctorales dans les Technologies de l'Information (JDTIC'12), Casablanca, Maroc, Novembre 2012

[15] N.Mayer, P.Heymans, and R.Matulevicius. Design of a modelling Language for Information System Security Risk Management. In Proceedings of the 1st International Conference on Research Challenges in Information Science (RCIS 2007), pages 121-131-,2007.

[16] W. Boehmer, *Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001*, *Proc. Second Int. Conf. Emerging Security Information, Sys. & Technologies. pp: 224-231,2008.*

[17] N.Mayer, *Model-Based Management of Information System Security Risk*, Ph.D. Thesis, Dept. Computer Science, Namur, Belgium, 2009.

[18] A.Sayouti & H. Medromi, *intechopen,2011*,(Autonomous and Intelligent Mobile Systems based on Multi-agent, Book Chapter in the book, Multi-agent Systems – Modeling Control , Programming, Simulations and Applications) ,.

[19] Clarke, J. et al., (*Consumerization of IT: Top Risks and Opportunities*), European Network and Information Security Agency ENISA, Heraklion, 2012

[20] *ISO/IEC Guide 73:2002*, *Risk management – Vocabulary* – Guidelines for use in standards.

[21] J. Ferber, (*Les systèmes multi-agents, vers une intelligence collective*) InterEditions, 1995, pp. 63-144.

[22] M. Wooldridge. Agents and software engineering. In *AI*IA Notizie XI(3), 1998 ,pages 31-37.*

[23] E.Humphreys ,Information security management standards: Compliance, governance and risk management".*J. Info. Secur. Tech*, Rep. 13(4), 247-255,2008.

Sophia FARIS is a PhD student in the National High School of Electricity and Mechanics (ENSEM), HASSAN II University, Casablanca, Morocco.
She is an engineer in computer sciences from ENSEM since 2011.
In 2013, she got certificates of ITIL V3 and ISO 27002 foundation.
Her actual main research interest concerns Information Security Risk Management and Security Auditing in Information Systems.

Hicham MEDROMI received the PhD in engineering science from the Sophia Antipolis University in 1996, Nice, France.
He is responsible of the system architecture team of the ENSEM HASSAN II University, Casablanca, Morocco.
His actual main research interest concerns Control Architecture of Mobile Systems Based on Multi Agents Systems.
Since 2003, he is a full professor for automatic productic and computer sciences at the ENSEM.

Adil SAYOUTI received the PhD in computer sciences from the ENSEM, HASSAN II University in July 2009, Casablanca, Morocco. In 2003, he obtained the Microsoft Certified Systems Engineer (MCSE). In 2005, he joined the system architecture team of the ENSEM. His actual main research interests concerns Remote Control over Internet Based on Multi agents Systems.