Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, Itil, Iso 27002,Iso 27005

S.FARIS
EAS Team, LISER Laboratory,
ENSEM
Casablanca, MOROCCO

S.EL HASNAOUI
EAS Team, LISER Laboratory,
ENSEM
Casablanca, MOROCCO

H.MEDROMI
EAS Team, LISER Laboratory,
ENSEM
Casablanca, MOROCCO

H.IGUER
EAS Team, LISER Laboratory,
ENSEM
Casablanca, MOROCCO

A.SAYOUTI
EAS Team, LISER Laboratory,
ENSEM
Casablanca, MOROCCO

Abstract—**Universities in the public and private sectors depend on information technology and information systems to successfully carry out their missions and business functions. Information systems are subject to serious threats that can have adverse effects on organizational operations and assets, and individuals by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processes, stored or transmitted by those systems. Threats to information systems can include purposeful attacks, environmental disruptions, and human/machine errors, and can result in harm to the integrity of data. Therefore, it is imperative that all the actors at all levels in a university information system understand their responsibilities and are held accountable for managing information security risk- that is the risk associated with the operation and use of information systems that support the missions and business functions of their university.**

The purpose of this paper is to propose an information security toolkit namely URMIS (University Risk Management Information System) based on multi agent systems and integrating with existing information security frameworks and standards, to enhance the security of universities information systems.

Keywords—Information security; information systems; multi agent systems; ITIL V3; ISO 27002; ISO 27005

I. INTRODUCTION

Information systems (ISs) are everywhere. They have a large impact on the everyday lives of universities as well as on individuals. At the heart of information systems, security aspects play a vital role and are thus becoming central issues in those systems' effective usage.

The importance of security technologies and of their enabling technical platforms has been widely recognized and receives continuous attention (e.g., new encryption, algorithms, public key infrastructures, etc.).

For some people, security management issues start with updating an antivirus database, but from a more serious perspective, universities understand that security concerns are the source of important costs, not only in terms of technologies but especially in terms of related management activities.

There are emerging calls for an integrated view of information security, from the technological, human, and organizational aspects, sometimes referred as MTO (Man, Technology, and Organization).

However, there is a lack in the methods for tackling the MTO issues in information security. One of the research focuses on the development of information security checklist and standards in order to capture the best practice.

Another research focuses on risk assessment by identifying the threats and vulnerabilities, and then determining the likelihood and impact for each risk. Risk assessment could either be qualitative, categorizing low, medium and high risks, or be quantitative, calculating the value of "Annualized Loss Expectancy"

This paper is presented as follows: after a brief introduction, in section two; a survey of available information security risk management methods and tools will be presented, and then the standards, ISO 27002, ISO 27005, and the framework ITIL will be described. Then, in the third section the toolkit URMIS will be proposed and the multi agent system will be introduced. The fourth section will propose the architecture, before concluding this paper.

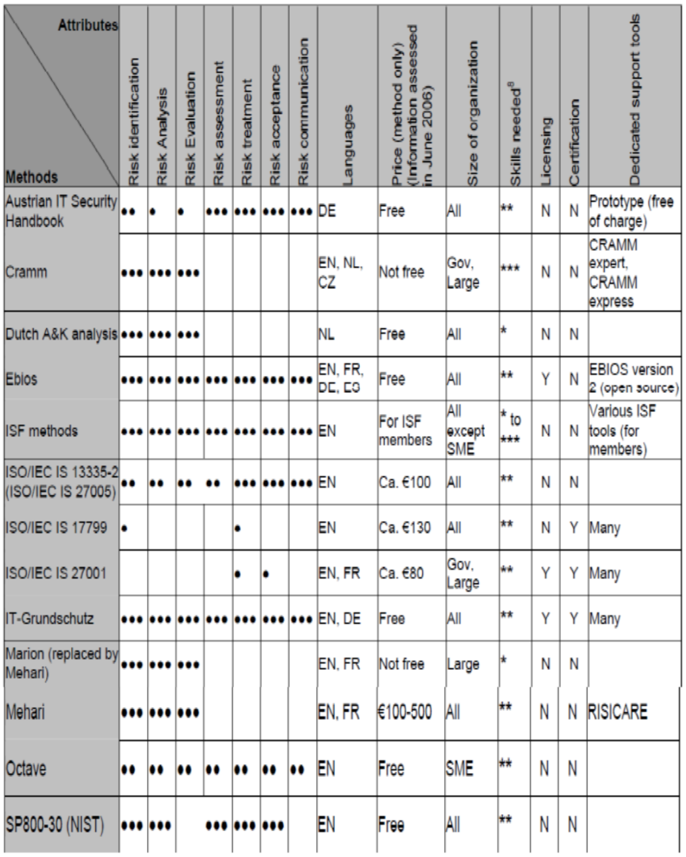
II. State of The Art

A. *Risk Management tools and frameworks*

An organizational risk is the risk to the organization or to individuals associated with the operation of an information system. The management of organizational risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system---the security controls necessary to protect individuals and the operations and assets of the organization.

The common view a Risk Assessment Framework provides helps an organization see which of its systems are at low risk for abuse or attack and which are at high risk. The data an RAF provides is useful for addressing potential threats pro-actively, planning budgets and creating a culture in which the value of data is understood and appreciated.

There are several risk assessment frameworks and risk management methods that are accepted as industry standards that we can list in the figure below.



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	

Fig. 1. Risk Management methods and frameworks

None of these tools implement the multi agent system approach.

Incorporation of the use of information and communication technology in Moroccan universities, involves the need to secure data in information systems.

There is a very little research related to the applications of multi agent systems (MAS) in information system security.

Besides to that, these tools are difficult to use because they require a certain level of knowledge.

Moreover, they don’t provide recommendations or immediate solutions to security issues; they just give guidelines to follow in order to ensure an effective security of the information system.

Based on the methodologies aforementioned, and other works described in [4] [5] [6] [10] [11], we propose an integration of the use of ISO 27002, ISO 27005, ITI, and multi-agent systems to develop an information security risk management tool of universities information systems named URMIS (Universities Risk Management Information System).

B. *ISO 27002*

The ISO 27002 standard is a collection of information security guidelines that are intended to help an organization implement, maintain, and improve its information security management. It is a code of good practices that provides hundreds of potential controls that are designed to be implemented with guidance provided within ISO 27001.

The strengths of ISO 2700 are listed below:

- Optimize the costs of ISS by associating with ISO 27001
- Increased knowledge of risk management
- Does not require a technical solution

Whereas its weaknesses are listed below:

- Optimize the costs of ISS by associating with ISO 27001
- Increased knowledge of risk management
- Does not require a technical solution

In the current version published 2013, ISO 27002:2013 contains 114 controls, as opposed to the 133 documented within the 2005 version. However for additional granularity, these are presented in fourteen sections, rather than the original eleven.

C. *ISO 27005*

ISO 27005 is intended to provide guidelines for information security risk management. It is used either autonomously or as a support for ISO 27001. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. It does not specify or recommend any specific risk analysis method, although it specifies a structured, systematic and rigorous process from analyzing risks to creating the risk treatment plan.

The strengths of ISO 27005 are as follows:

- Flexible and reusable
- Continuous risk management
- Highlighting the human factor: the concept of responsibility
- Whereas its weaknesses are as follows:
- No specific methodology for risk management

The figure below gives an overview of the information security risk management process in ISO 27005.

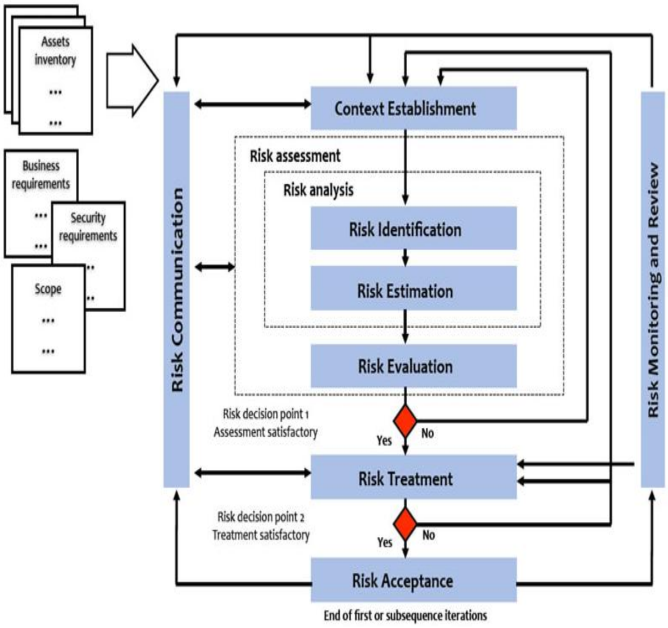


Fig. 2. Information Security Risk Management process

D. ITIL V3

The Information Technology Infrastructure Library (ITIL) is a framework of best practices that promote quality computing services in IT sector.

ITIL is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally.

ITIL presents a broad set of management procedures, which apply to all aspects of IT infrastructure, with which an organization can manage its IT operations (Zegers, 2006, Wegmann, 2008).

The ITIL v3 Core consists of five publications, each providing

guidance on a specific phase in the service management lifecycle.

The ITIL Core publications are as follows:

- **Service strategy**
- **Service design**
- **Service transition**
- **Service operation**
- **Continual service improvement**

ITIL can help companies assess their risks, and put procedures in place to log and respond to incidents. ITIL, and more specifically the ITIL security management process, is widely used for the implementation of information security within an organization. ITIL v3 has placed the information security management process within the Service Design core practice book. The goal of the information security management process is to align IT security with business security and ensure that information security is effectively managed in all services and service management activities (OGC, 2007; Taylor,2008).

E. Information security

Confidentiality, integrity and availability are basic requirements for business information security and provide the maintenance requirements of the business (ITGI, 2009), (Kwok and Longley, 1999), (Fitzgerald, 2007), (Sêmola, 2003), (Dias, 2000), (Moreira, 2001).

- **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, in order to protect it from tampering, whether intentional or accidental;
- **Availability (A)**: All the information generated or acquired by an individual or institution should be available to their users at the time they need them for any purpose;

III. Objectives and Importance of The Research

The major objective of this work is to design and implement an integrated toolkit for improving risk management of a university information system.

This work explores how to promote integration and the establishment of a toolkit that would allow each university to have reliable data on higher education, driving better management and improve their governance and risk management.

Implementing this toolkit involves taking a proactive, strategic and measured approach that is more efficient than the reactive one used in many universities. This can be reached across a strategic integration of appropriate frameworks, models and methods in governance and information security.

Analyzing the relevant frameworks, models and methods, used in the aforementioned domains, and extracting the best practices for implementing them in URMIS, can provide effective security of university IS assets.

A. The proposed toolkit

URMIS (Universities Risk Management Information System) is an information security toolkit that provides guidance policies to achieve an effective information security risk management in universities' information systems.

With the intention of implementing the task of information security risk management, URMIS needs to collect data about the status of information asset, recognize kinds of risk, and perform risk management task based on a good defined risk management process. That means the working environment of URMIS consists of knowledge, data, process and strategies. However, knowledge, data, process and strategies are resources in different formalization, and it is a complex work to design interface for each resource. This work is based on the multi agent systems approach, because of its benefits. It encompasses cooperation, resolution of complex problems, modularity, efficiency, reliability and reusability. All these advantages provided by MAS fit these needs.

B. Agent and Multi agent systems (MAS)

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". Agents have the following main properties and characteristics:

- **Autonomy** : agents encapsulate a state (which is not available to other agents), and make decisions on what to do based on this state, without direct human intervention or other persons;
- **Social ability**: agents interact with other agents (and possibly humans) via some kind of agent communication
- Language, and generally have the opportunity to participate in social activities (such as cooperation for solving problems or negotiating) to achieve their goals.
- **Reactivity**: agents are put in an environment (which may be the physical world, a user via a graphical interface, a collection of other agents, the internet, or perhaps many of these combinations), are able to perceive this environment (through the use of potentially imperfect sensors), and are able to respond to timely changes that occur in it.
- **Proactivity**: Agents do not simply act in response to their environment; they are able to solve a problem by taking the initiative.

A multi-agent system (MAS) is a system composed of several intelligent agents that interact with each other. They can be used to solve problems that are difficult or impossible to solve for an individual agent or monolithic system. Multi-agent systems are open and scalable systems that enable the implementation of autonomous and proactive software components. They are characterized by the local autonomy, social interaction, adaptability, robustness and scalability, and for these reasons, they are a very promising paradigm to address the challenges facing automation and check systems.

IV. URMIS Information Security Architecture

A. Model-View-Controller (MVC)

URMIS is based upon the widely used Model-View-Controller (MVC) architecture common in interactive web based applications.

MVC separates the layers; presentation layer (UI: User Interface), business (BLL: Business Logic Layer) and data access (DAL: Data Access Layer). The goal is to have a minimum length between the different layers of the application; and changes made to any layer of the application do not affect other layers.

B. URMIS architecture

URMIS is composed of five layers: client layer, mediator layer, service layer, risk management layer and resource layer. The system is based on the following multi agent systems: client agents, mediator agent, service agents, risk agents, incident agent and internet agent. The figure 4 below represents the architecture of URMIS

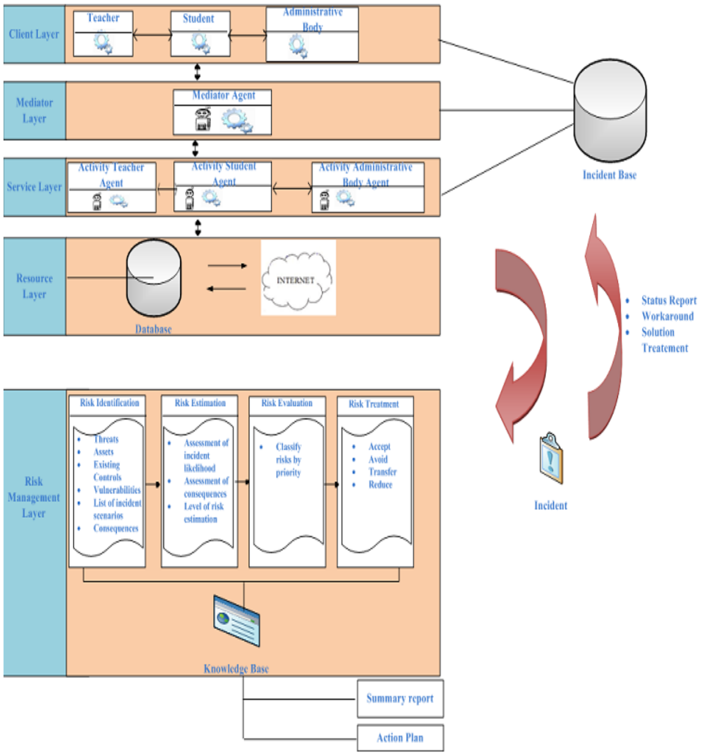


Fig. 3. URMIS architecture

Client agent: They consist of all agents on the client layer, namely agent teacher, agent student, and agent administrative body. They manage the interaction between the users (teachers, students and administrative body) and the system. They allow users to connect to the system by specifying their names, email addresses and id. Every user has a unique id; this field differentiates between the user if it is a teacher, a student or an administrative body.

The id is composed of eight alphanumeric characters; id' teacher starts with the character "t", id's student starts with "s", and id's administrative body starts with "ab". Client agents communicate with the mediator agent by sending users' information of connection.

In case of an incident of connection (password or id forgotten), the user can ask for a solution by sending his request to the risk multi agent system.

Mediator agent: This agent acts like a security checker.

It checks the identities of the users so it can allow them to access to the service layer. It also performs a permission check of the user's access rights and, thereafter, allows him to exploit the service for which he's authorized.

In order to have their needs processed a user requests a service from the mediator agent which then forwards the messages to the destination (service agents) if the access is granted or drops the message and returns a FAILURE message to the sender otherwise. To guarantee a high level of performance several Mediator agents can be triggered to distribute the work among them.

To distinguish between the requesting agents, it is necessary for the mediator agent to link between the user and its category (teacher, student or administrative body). Therefore, the Mediator consults the database which in are stored the users, their corresponding category, and the types of services they can access.

Service agent: These agents communicate with the resource layer to accomplish their tasks.

Risk agents: In the risk management layer we have four agents namely risk identification agent, risk estimation agent, risk evaluation agent and risk treatment agent.

- ✓ ***Risk identification agent:*** It contains in its knowledge base risks that could potentially prevent URMIS to achieve its goals.
  It includes documenting and communicating the users in case of a bad use of URMIS with a list of threats, vulnerabilities and risks that can affect the system.
- ✓ ***Risk estimation agent:*** This agent calculates the likelihood of an incident happening, by applying the risk formula risk=threat * vulnerability * impact.
- ✓ ***Risk evaluation agent:*** It classifies the risk based on the ISO 27005 risk assessment matrix (very low, low, medium, high, very high).
- ✓ ***Risk treatment agent:*** It is in charge of selecting and implementing measures to modify risk. Risk treatment measures can include avoiding, accepting, transferring or reducing risk. The measures (i.e. security measurements) can be selected out of sets of security measurements that are used within the Information Security Management System (ISMS) of the university complying with the standard ISO 27001.

Incident agent: It contains in its knowledge base solutions to similar incidents which occur frequently. This agent stores scenarios of solutions to incidents and make it available for other agents. With this information, other agents are able to take the right decisions in the right moment.

Internet agent: Its role is to store in the knowledge base all the threat and vulnerabilities that it receives from internet.

V. Conclusion and Perspectives

Risk management techniques used before were inappropriate to avoid risks before their occurrence. These approaches were in a reactive perspective. It has therefore become necessary to run into for an integrated approach with a proactive perspective to avoid risks and treat them without compromising the information systems.

In this paper, we describe how information security activities can contribute to the protection of information and infrastructure assets against the risks of loss, bad use or destruction.

In a future work, we will detail the architecture of each agent and the communication between them in URMIS. We will also integrate the processes of the method OCTAVE, in order to quantify risks that can affect URMIS.

References

[1] Y. Rezgui, and A. Marks, "Information security awareness in higher education: An exploratory study," Computers & Security, vol. 27(7-8), pp. 241-253, July 2008.

[2] Defta (Ciobanu) Costinela – Luminita, 2011,Information security in E-learning Platforms, Procedia Social and Behavioral Sciences 15 (2011) 2689–2693

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

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

[5] 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.

[6] A, Kokolakis S, Lambrinoudakis C, Gritzalis S ,"Information Systems Security Management: A Review and a Classification of the ISO Standards". J. Next Generat. Soc. Technol. Leg Issues. 26: 220:35, 2010.

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

[8] Consilium-ICT, ITIL et la gouvernance des systèmes d'informations: vers une e administration agile, Toulouse, Juin 2009.

[9] InTech, April 4, 2011. "Multi-Agent Systems - Modeling, Control, Programming, Simulations and Applications", ISBN 978-953-307-174-9

[10] S.Faris,H. Iguer, H.Medromi and S.Sayouti, "New model multi-agent systems based for the security of information system" Proc. IC2INT'13, 2013.

[11] H. Bahtit, B. Regragui.. "Risk Management for ISO27005 Decision Support", International Journal of Innovative Research in Science, Engineering and Technology,2013

[12] S.Faris,H.Medromi and A.Sayouti, "Modélisation d'une plateforme (SIGRCI) à base des systèmes multi-agents & ITIL", JDTIC,2012.

[13] S.Faris,H.Iguer,H.Medromi and A.Sayouti " Conception d'une Plateforme de gestion des risques basée sur les systèmes multi-agents et ISO 27005", JDTIC,2013.

[14] J.Ferber , " Les systèmes multi-agents, vers une intelligence collective InterEditions", 1995

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

[16] A.Sayouti,F.Qrichi Aniba,H.Medromi, "Remote Control Architecture over Internet Based on Multi agent systems". IRECOS, Vol3,N.6,pp.666-671,Novembre 2008.