International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12 – No. 7, October 2017 – www.ijais.org

Design and Implementation of a Comprehensive Information Security Risk Management Tool based on Multi-agents Systems

Mohamed Ghazouani
ENSEM
Casablanca, MAROC

Hicham Medromi
ENSEM
Casablanca, MAROC

Laila Moussaid
ENSEM
Casablanca, MAROC

ABSTRACT
While there are many framework that help users in Governance, Risk, and Compliance (GRC), we know of none which actually try to automate the process by using multi agent systems. The Team of Systems' Architecture proposes an integrated IT GRC architecture for a high level IT GRC management. This article focuses on IT Risk topic and presents a new approach for a multi-agent expert system, where managers of IT GRC can in an intelligent manner specify the IT needs following the strategic directives through a questionnaire about specific business goals. The key element that differentiates this research from the previous ones is that none of them are based on multi-agents system. The system was verified on concrete example. Future works consists on realizing a practical example of the proposed subsystem on real company systems that are involved in the research in order to overcomes obstacles and achieve IT organization objectives.

General Terms
Security risk assessment, risk management system, information system

Keywords
IT GRC; ISO27005; ISO27001; MEHARI; Multi-agent system (MAS)

1. INTRODUCTION
Risk management has long ago been incorporated businesses of all kinds. Now that computers came into the business, IT risk should be taken into consideration. Furthermore, the computer is now in charge of several critical operations, so the IT risk becomes one of the main risks of the company of today.

Risk assessment is the determination of value of risk related to a concrete situation and a recognized threat depending on two factors, the probability and impact. The level of risk is the product of the two risk factors. IT risk assessment can be performed by a qualitative or quantitative approach. When the impact is assessed in dollars, we are talking about quantitative analysis; otherwise we speak of qualitative analysis. Our subsystem addresses the qualitative risk.

This paper is presented as follows: in the section 2 we will give an overview of the common architecture: EAS-ITGRC, in section 3 we will provide a survey of available information security risk management methods and tools, in the section 4 and 5 we will present a description of ISO27005 and Mehari, in the section 6 we will introduce the multi agent system, in section 7 we will propose the approach and in the section 8 we will propose the architecture for EAS-SGRSSI Tool.

2. OVERVIEW OF THE COMMON ARCHITECTURE
We present an overview of the proposed solution that provides a high level model for integrated IT Governance, IT Risk and IT Compliance processes (Fig.1). Each member of the Systems Architecture Team (EAS) works on a subsystem individually.

To gain a deeper understanding of the proposed architecture, we give a brief description of each layer of the EAS-ITGRC platform.

Strategic layer: it is an ITG Platform based on COBIT framework; ensuring permanent alignment of IT and business with stakeholder's participation. It contains an interactive level in an intelligent way to specify the IT needs following the strategic directives through a questionnaire about specific business goals.

Communication layer: it is responsible for all communications between layers of the IT GRC platform.

Decision making layer: the Decision Making Layer allows us to propose the best reference to perform for each request.

Processing layer: this layer contains different subsystems, which can be implemented, responding to communication layer's notification.

The purpose of the paper, when accepted, is to present EAS-SGRSSI, one of these subsystems, its features and a mathematical formulation of risk by using a lower level of granularity of its elements: threat, probability, criteria used to determine an asset's value, exposure, frequency and existing countermeasure.

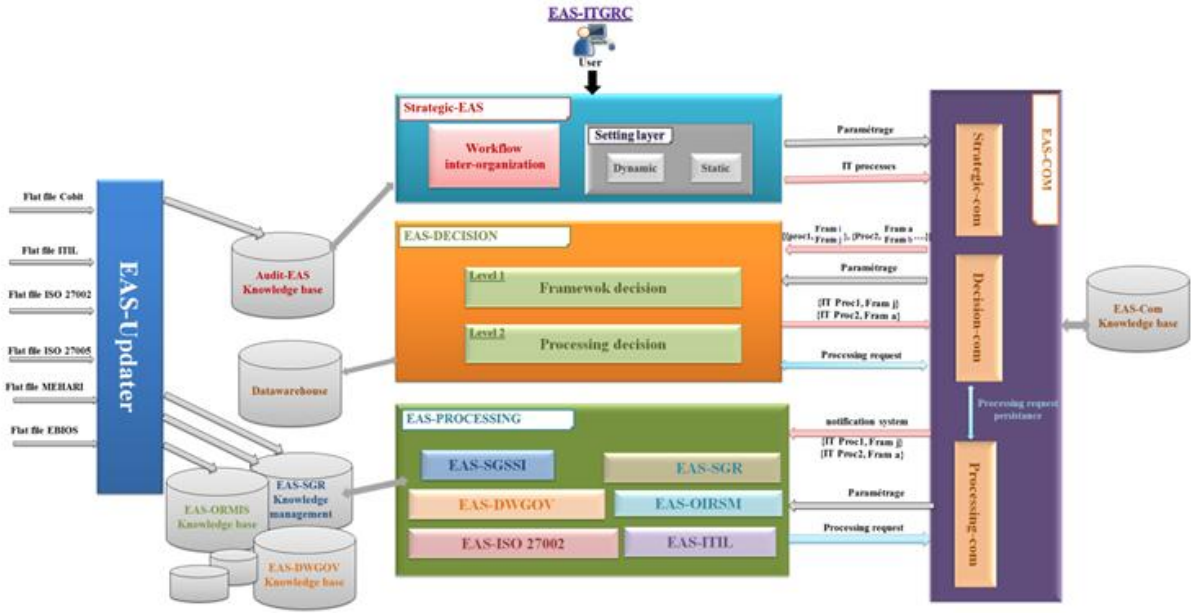

Fig 1: EAS-ITGRC Architecture

3. AVAILABLE RISK MANAGEMENT METHODS AND TOOLS

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

3.1 Methods

Table (1) lists the main well-known methods.

Table 1. Risk Management Methods

Au IT Security Handbook	Cramm	A&K Analysis	Ebios
ISAMM	ISF Methods	SP800 30	ISO/IEC 2005
ISO/IEC 27001	IT Grundschutz	Magerit	Marion
Mehari	MIGRA	Octave	Risksafe Assesment

3.2 Tools

Table (2) presents related tools.

Table 2. Risk Management Tools

Countermeasures	Cramm	EAR/Pilar	Ebios
Gstool	GxSGSI	ISAMM	Mehari
Callio	Casis	CCS Risk Manager	Cobra
MIGRA Tool	Modulo Risk Manager	Proteus	Octave
Ra2	Real ISMS	Resolver*Ballot	Resolver*Risk
Risicare	Riskwatch	RM Studio	SISMS
TRICK light	Acuity Stream		

- Most of these tools are Commercials.
- None of the tools implement Multi agent system.
- There is no tool developed in Morocco. Usability of the tools used by Moroccan organizations and contribute to help Moroccan organizations in the information security field are important for us.
- There is very little research related to the applications of multi agent systems (MAS) in Audit Information System Security.
- Do not provide recommendations or immediate solution to security problems.
- Difficulty of use, it's requires a certain level of expertise.
- Do not explain their calculation methods.
- Require a lot of time to implement.
- Based on the above methodologies, researches and others work described in [1] [2] [3] this work propose an integrated use of ISO27005, Mehari and multi-agents system to develop an Information Security Risk Management Tool (ISRMT).

Based on the above methodologies, researches and others work described in [8] [9] [10] we propose an integrated use of ISO27005, Mehari and multi-agents system to develop an Information Security Risk Management Framework (EAS-SGRSSI).

4. ISO 27005

The purpose of ISO 27005 is to provide guidelines for information security risk management. 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 [1]. It does not specify, recommend or even name any specific risk analysis method, although it specifies a structured, systematic and rigorous process from analyzing risks to creating the risk treatment plan [2].

ISO 27005 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

5. MEHARI

MEHARI is a risk analysis and management method developed by CLUSIF and supported by software managed by the company Risicare1 (http://www.risicare.fr). MEHARI, originally developed in 1996, aims at assisting the executives (operating managers, CISO, CIO, risk manager, auditor) in their efforts to manage the security of Information and IT resources and to reduce the associated risks. MEHARI is compliant to ISO 13335 risk management standard and is suitable for the ISMS process described by ISO 27001. It allows the stakeholder to develop security plans, based on a list of vulnerability control points and an accurate monitoring process to achieve a continual improvement cycle [3].

6. MULTI AGENT SYSTEM

Multi-agents systems (MAS) are based on the idea that a cooperative working environment comprising synergistic software components can cope with problems which are hard to solve using the traditional centralized approach to computation. Smaller software entities – software agents – with special capabilities (autonomous, reactive, pro-active and social) are used instead to interact in a flexible and dynamic way to solve problems more efficiently. Agents model each other's goals and actions; they may also interact directly (communicate) [8].

6.1 Agent

Agents are software entities that have a very specific task and that decide for themselves what they need to do in order to satisfy their design objectives. They perceive their environment through sensors and acts on that environment through effectors [9]:

A characteristic is an intrinsic or physical property of an agent. The following are some common agent characteristics (Morreale, 1998; Wooldridge & Jennings, 1995):

- Autonomy: An agent can act on another's behalf without much guidance.
- Communication: An agent can communicate with other agents on a common topic of discourse by exchanging a sequence of messages in a speech-act-based language that others understand. The domain of discourse is described by its ontology.
- Mobility: An agent can migrate from one system to another in a pre-determined fashion or at its own discretion. Accordingly, agents can be static or mobile.
- Learning: An agent can have the ability to learn new information about the environment in which it is deployed and dynamically improve upon its own behavior.
- Cooperation: An agent can collaborate and cooperate with other agents or its user during its execution to minimize redundancy and to solve a common problem.

6.2 Potential of Multi-Agent Systems

The use of agent-orientation in the modeling, design, and implementation of an Information Security Risk Management provides at least the following benefits:

- **Flexible**. Agent architectures are more flexible, modular and robust than, for example, object-oriented ones. They tend to be open and dynamic as their components can be added, modified or removed at any time (Yu, 1997).
- **Pro-activeness**. [10] Intelegent agents are able to exhibit goal-directed behavior by taking the initiative in order to satisfy their design objectives :
    - **Goal-directed behavior**. [11] If agents are a level of abstraction between a user and a set of low-level tasks, an agent must be able to create a mapping between the high-level goal and the available tools such that it can use the tools effectively to achieve the goal. In other words, the agent must be able to plan. In this project, a RSSI may task an Audit agent to make an Information Systems Security Audit.

The ability of an agent to exhibit goal-directed behavior typically comes from incorporating AI planning techniques into the agent code.

- **Cognizant Failure**. An important (but often neglected) component of goal driven behavior is cognizant failure. Cognizant failure is the idea that once tasked, the agent either completes the task and returns, or recognizes that it cannot complete the task and reports a failure.

- **Reactivity**. Agents are crucial when operating in an unpredictable environment containing a large number of data sources scattered over multiples sources. If an agent queries an information source and finds no answers to its query, it would then try alternate sources of information until it could come up with a reasonable number of answers.
- **Learning**. Another important characteristic of autonomous behavior is the ability to enhance future performance as a result of past experiences. Machine learning techniques allow an agent to learn new methods or refine existing ones to meet specific needs.
- **Communication and cooperation**. Intelligent agents are capable of interacting with other agents (and humans) in order to o achieve a common goal.
- **Temporal continuity**. Persistence of identity and state over long periods of time.
- **Information gathering and filtering**. Is another useful example of using agents for user assistance. Using questionnaires and survey can be very time-consuming. But rather than do this work on our own, agents can do this work for us. In addition, automating data collection ensures that risk assessment is thorough and complete.

7. PROPOSED APPROACH

EAS-SGRSSI is a qualitative tool for assessing information security risks; it utilizes concepts defined in ISO27005 and Mehari. The tool provides an easy-to-apply information security risk analysis spanning the enterprise. With EAS-SGRSSI the threats and vulnerabilities can be identified, the probability that a threat will occur and the impact if the threat does occur can be assessed, the risk levels can be established,

[1] www.risicare.fr, accessed July 2017

mitigating controls and safeguards are identified and implementation action plan can be developed.

Our approach proposes a qualitative risk analysis for information asset. In the qualitative method we evaluate, based on judgment, experience, and situational awareness:

The exposure of the asset and frequency of the threats are two of three parameters to get the probability value.

Control is the percentage of measurements they are implementing for each asset. It's the main parameter used in calculating the probability.

Probability = (exposure + frequency) / 2 * 1 / Control

The confidentiality, integrity and availability of information to get the impact value. These metrics are selected according to Ebios, NIST 800-30 and SP which are based on these criteria to estimate the impact value.

Approaches that can be used for qualitative analysis include, but are not limited to, internal interviews, internal surveys, internal questionnaires, storyboarding and internal Focus groups. For our case we select internal surveys and internal questionnaires, because surveys and questionnaires are usually the best mechanism to accomplish data collection when you have to query a large group of individuals [4].

8. PROPOSED ARCHITECTURE

The proposed MAS is actually composed from several sub-MAS to support the whole decision making process. The tool is designed as web application connected to a database system. The application implements an input questionnaire, which is used for asset impact evaluation. Then the threats are assigned according to assets type using set of rules IF-THEN. Based on the selected threats, risk values are calculated and based on threats, assets and risks, appropriate measures are proposed by the system. These measures are viewed in a friendly way, with attributes describing their effectiveness and their cost of implementation. On the basis on these attributes, the manager can decide to implement them or not. At the end, the system generates a study summary report and an action plan suggesting the manager countermeasures to implement. All deliverables are transmitted to the communication layer through web services. Figure 2 graphically illustrates the global view of the EAS-SGRSSI Tool. This section discusses its components.

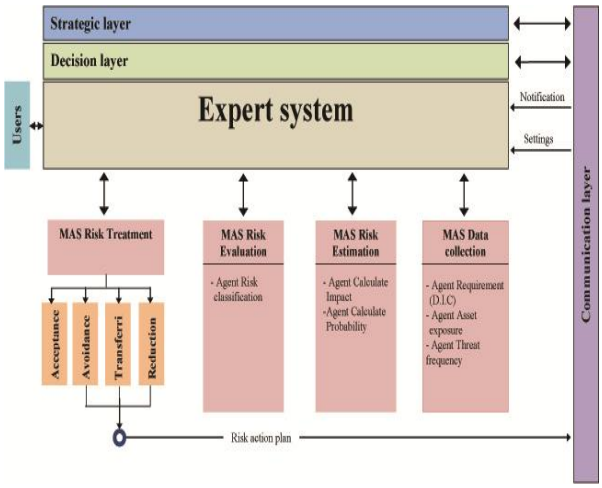

Fig 2: Global view of EAS-SGRSSI

8.1 Expert system

An expert system is a tool capable of reproducing the cognitive mechanisms of an expert in a particular field and, more precisely, is software capable of answering questions, performing reasoning from known facts and IF-THEN rules [21]. An expert system is divided into two sub-systems: the inference engine and the knowledge base. The knowledge base represents facts and rules. The inference engine applies the rules to the known facts to deduce new facts. Inference engines can also include explanation and debugging capabilities [22].

The Expert system is in charge of handling all communication with the manager, the MAS Data collection, MAS Risk Estimation, MAS Risk Evaluation, MAS Risk Treatment and asset owner in order to manage the planning and execution.

An Expert system who has done multiple assessments within an organization would probably already have some expectations on what the results will be and could easily identify inconsistencies in the results based on these expectations.

Potential expert systems are foreseen at many levels:

- The need to store the expertise for future use and potentially cloned or multiplied.
- More than one experts' knowledge has to be grouped at one platform.
- detect possible errors in measurement and avoid issues of data insertion errors leading to the under-performance of the risk management;
- An active planner and organizer of risk management activities.
- helps to identify and prioritize specific tasks to improve security and achieve compliance;

8.2 Data collection

In the first step, it is necessary to receive all assets about the scope of risk management from communication layer through web services. Afterward, MAS Data collection has the role of sending input questionnaires to users or collaborators and ensures respect duration, retransmit, make a first consolidation and detect anomalies in respondent answer. It's also in charge of assessment of level of compliance for a given level and derives a control score that was described in section 7.

The questionnaire is shown in the following figure 3:

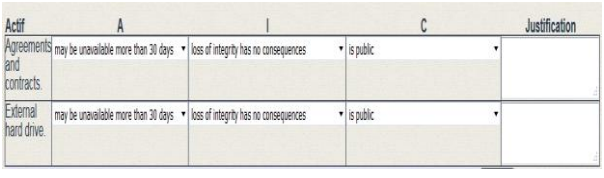

Fig. 3: Asset impact evaluation by the asset's owner

In the questionnaires, the criteria are represented as fuzzy linguistic variables, because the user is often not able to quantify the content of these items exactly. Thus, the application is suggesting linguistic values, which are closer to the human cogitation.

The asset owner should indicate a value, from 1 to 5, for each

criteria where required and these values must be validated by his/her direct superior. These three—the loss of confidentiality, integrity, and availability—are ranked as the top business liabilities by organizations [4]. The user must enter a justification for the values.

- Confidentiality (C) concerns the protection of sensitive information from unauthorized disclosure.
- Integrity (I) relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- Availability (A) relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities [3].

Availability (A) should be from 1 to 5:

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

Integrity (I) should be from 1 to 5:

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.

Confidentiality (C) should be from 1 to 5:

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.

The greatest value of these three criteria is the value of the impact.

Then there is the exposure of the assets: the manager must consider certain factors to give this value: accessibility to assets, location, data flow, number of users, etc. The following table (3) indicates detailed information of frequency value:

Table 3: Exposure Determination Matrix

Score	Description	Criteria
5	very likely	Weaknesses for the system have been noted.
4	likely	System is Internet accessible.
3	moderate	System is remotely accessible (e.g. Site-to-Site or Client-to-Site VPN)
2	unlikely	System is accessible only through the internal network
1	very unlikely	Anything that does not fall into the LOW criteria.

Based on marked assets and a filled-in questionnaire, the threats will be listed (see figure 4 below) using set of rules IF-THEN and utilization of the database of threats (Mehari). When selecting a relevant threat, vulnerabilities are automatically loaded.

Change number of columns: Select the "Columns" icon from the MS Word Standard toolbar and then select "1 Column" from the selection palette.

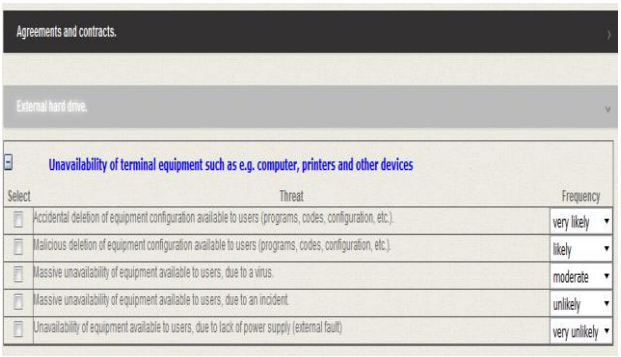

Fig 4: List of threats for each asset

The manager should select the threats and indicate its frequency. The frequency of the threat is never exact, the manager should be based on some information like: number of attacks and incidents detected in relation to the threat faced by the organization. Using these parameters, the manager can provide a rough estimate of the frequency of a particular threat in the context of the organization. The following table (4) presents detailed information of frequency value:

Table 4. Frequency Determination Matrix

Score	Description	Criteria
5	very likely	Could happen more than 100 times per year
4	likely	Could happen between 10 and 100 times per year
3	moderate	Could happen between 1 and 10 times per year
2	unlikely	Could happen within 1 year
1	very unlikely	Could happen within 5 years

8.3 Risk Estimation

MAS Risk Estimation handles the execution of the impact and the probability calculation. (See figure 5 below).

External hard drive.				
Risk code	Description	Impact	Probability	Risk level
S03-D01	Accidental deletion of equipment configuration available to users (programs, codes, configuration, etc.).	5	5	25
S03-D02	Malicious deletion of equipment configuration available to users (programs, codes, configuration, etc.).	5	5	25
S03-D03	Massive unavailability of equipment available to users, due to a virus.	5	5	25
S03-D04	Massive unavailability of equipment available to users, due to an incident.	5	5	25
S03-D05	Unavailability of equipment available to users, due to lack of power supply (external fault)	5	5	25

Fig 5: Risk estimation

8.4 Risk Evaluation

MAS Risk Evaluation has the role of classifying the risk based on the ISO27005 risk assessment matrix. (See figure 6 below).

This part is to classify risk levels according to different levels of gravity. In other words, we will put these results into three classes, high, medium and low.

The knowledge base is filled with IF-THEN rules containing expert knowledge. Examples of used IF-THEN rules for risk evaluation:

IF F== high AND E == high AND C==low AND Impact == high THEN risk= high

IF F== medium AND E == medium AND C== high AND Impact == high THEN risk=medium

IF F== low AND E == low AND C==low AND Impact == low THEN risk= low

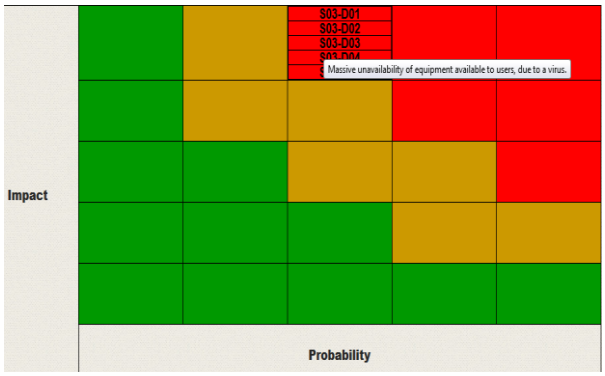

Fig 6: Risk classification

Using this matrix, the manager have an on-screen overview of all risks and there classifications. By hovering the mouse over the risk code the manager can see what risk description.

8.5 Risk Treatment

MAS Risk Treatment presents all the threats to each asset. Each line must indicate the threat, level of risk, its classification and a dropdown menu offering the following options: mitigate, transfer, accept and avoid. (See figure 7 below).

External hard drive.				
Risk code	Description	Risk level	Classification	treatment
S03-D01	Accidental deletion of equipment configuration available to users (programs, codes, configuration, etc.).	15	High	Reduce / Accept / Transfer / Avoid, OK
S03-D02	Malicious deletion of equipment configuration available to users (programs, codes, configuration, etc.).	15	High	Reduce, OK
S03-D03	Massive unavailability of equipment available to users, due to a virus.	15	High	Reduce, OK
S03-D04	Massive unavailability of equipment available to users, due to an incident.	15	High	Reduce, OK
S03-D05	Unavailability of equipment available to users, due to lack of power supply (external fault)	15	High	Reduce, OK

Fig 7: Risk treatment

8.5.1 Risk mitigation

If the manager chose to mitigate the risk, the system suggests administrative controls, technical or physical to be applied within the information system according to their effectiveness and cost of implementation.

Examples of possible countermeasures and their attributes are listed in following table (5):

Table 4. An Example of Countermeasures

Countermeasure	Cost	Efficiency
Develop a security policy and recommendations for the work outside the company premises. The recommendations and guidelines should address precautions both at home and on the move or in public transport and cover the protection of laptops, the use of an updated firewalls and antivirus, connections to public networks or third party, precautions to take regarding written documents, instant messaging and phone conversations.	low	big
Develop a security policy and recommendations related to telework. The recommendations and guidelines should address precautions to cover the security of connections to the corporate network (strong authentication, VPN, etc.), the exact terms of possible restriction of access, precautions regarding the use of the personal computers by persons others than the owner (family, friends, etc.), etc.	low	big
The security policy should formally prohibit taking outside the company document being classified as important or document of probative value.	low	medium
People likely to work outside the premises of the company and must receive awareness training on the measures to be used to protect documents, systems and the data they contain. These safeguards concern the physical and logical security against	high	big

theft but also indiscretions or unauthorized access by the family as much in public.		
The configuration of IT resources used for work outside the company premises (laptops, etc.) should be regularly checked.	med ium	medium

The expert system knowledge base is filled with rules containing expert knowledge on the field. Based on these rules, the cost and efficiency of measures and input data obtained from the manager and the end users through questionnaires, the system displays the most relevant countermeasures for the marked assets. Based on this information, the manager can select the most appropriate countermeasures according to its financial resources and its requirements in terms of efficiency in order to reduce risk. (See figure 8 below).

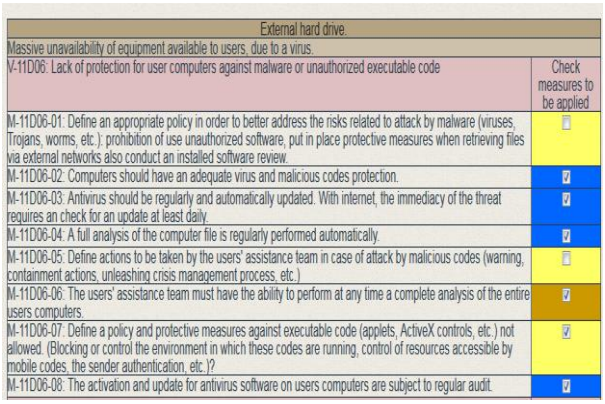

Fig 8: Risk mitigation

The colors represent the countermeasure effectiveness, where:

- Yellow – small efficiency
- Orange – medium efficiency
- Blue – big efficiency

Once the manager chose the countermeasure to correct the vulnerability, the system recalculates the level of risk. (See figure 9 below).

Fig 9: Risk Classification after Mitigation

8.5.2 Risk transfer

If the manager selects to transfer risk, mainly by insurance, the system offers a list of companies that supports this type of threat; otherwise the system proposes to add one.

8.5.3 Risk acceptance

Accept the risk as it is.

8.5.4 Risk avoidance

Decide to avoid the risk by eliminating the risk situation by structural or organizational measures.

9. CONCLUSIONS

In general, the safety of SI has several objectives. Safety, then, must protect information such as company assets against data loss, disclosure or alteration to ensure continuity of business operations. In this paper, we discussed the general proposed solution then we detailed the EAS-SGRSSI subsystem components and its architecture. This particularity of our approach is that the architecture is an integrated use of ISO27005, Mehari and multi-agents system in order to design a comprehensive Information Security Risk Management Tool.

The system was verified on concrete example. Future works consists on realizing a practical example of the proposed subsystem on real company systems that are involved in the research in order to overcomes obstacles and achieve IT organization objectives.

10. ACKNOWLEDGMENTS

I would like to thank to my advisor Ms. H. Medromi, PhD. And Laila Moussaid, PhD for their invaluable guidance and many useful suggestions during my work on this paper. I would also like to express my gratitude to all those who gave me the possibility to complete this paper.

11. REFERENCES

[1] Information-Technology—Security techniques—Information security risk management. INTERNATIONAL STANDARD ISO/IEC 27005 First edition 2008.

[2] KOUNS, Jake and MINOLI, Daniel. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams. John Wiley & Sons, 2011.

[3] TALABIS, Mark et MARTIN, Jason. Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis. Newnes, 2012.

[4] DOUSH, Iyad Abu. MULTI-AGENT SYSTEMS MODELING, CONTROL, PROGRAMMING, SIMULATIONS AND APPLICATIONS. 2011.

[5] RUSSELL, Stuart J. et NORVIG, Peter. Artificial intelligence: a modern approach. 2009.

[6] WOOLDRIDGE, Michael et JENNINGS, Nicholas R. Intelligent agents: Theory and practice. The knowledge engineering review, 1995, vol. 10, no 02, p. 115-152.

[7] BURKEY, Roxanne and BREAKFIELD, Charles V. (ed.). Designing a Total Data Solution: Technology, Implementation, and Deployment. CRC Press, 2000.

[8] CARDOSO, Rui Costa et FREIRE, Mário Marques. SAPA: software agents for prevention and auditing of security faults in networked systems. In: Information Networking. Convergence in Broadband and Mobile Networking. Springer Berlin Heidelberg, 2005. p. 80-88.

[9] MORADIAN, Esmiralda et HÅKANSSON, Anne. Approach to solving security problems using meta-agents in multi agent system. In: Agent and Multi-Agent Systems: Technologies and Applications. Springer Berlin Heidelberg, 2008. p. 122-131.

[10] PRUSIEWICZ, Agnieszka. A multi-agent system for computer network security monitoring. In: Agent and Multi-Agent Systems: Technologies and Applications. Springer Berlin Heidelberg, 2008. p. 842-849.

[11] Automating System Security Audits. ISACA Journal, volume 1, 2004.

[12] http://msdn.microsoft.com/en-us/library/ff648641.aspx Improving Web Application Security: Threats and Countermeasures. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. Microsoft Corporation

[13] SAYOUTI, Adil, MEDROMI, Hicham, et MOUTAOUAKIL, Fouad. Autonomous and Intelligent Mobile Systems based on Multi-Agent Systems. In: International Conference on Computing and Control Applications (CCCA). 2011. p. 452-467.

[14] VASUDEVAN, Vinod. Application Security in the ISO27001 Environment. IT Governance Ltd, 2008.

[15] SAYOUTI, Adil, MEDROMI, Hicham. Book Chapter in the book MULTI-AGENT SYSTEMS MODELING, CONTROL, PROGRAMMING, SIMULATIONS AND APPLICATIONS. 2011

[16] MORADIAN, Esmiralda et HÅKANSSON, Anne. Approach to solving security problems using meta-agents in multi agent system. In: Agent and Multi-Agent Systems: Technologies and Applications. Springer Berlin Heidelberg, 2008. p. 122-131.

[17] CALDER, Alan and WATKINS, Steve G. Information Security Risk Management for ISO27001/ISO27002. It Governance Ltd, 2010.

[18] Mohamed GHAZOUANI, Hicham MEDROMI, Brahim BOULAFDOUR and Adil SAYOUTI, "A model for an Information security management system (ISMS Tool) based multi agent system."International Conference on Intelligent Information and Network Technology (IC2INT'13)

[19] GHAZOUANI, Mohamed, MEDROMI, Hicham, SAYOUTI, Adil, et al. Article: An Integrated use of ISO27005, Mehari and Multi-Agents System in order to Design a Comprehensive Information Security Risk Management Tool}. International Journal of Applied, vol. 7, p. 10-15.

[20] GHAZOUANI, Mohamed, FARIS, Sophia, MEDROMI, Hicham, et al. Information Security Risk Assessment--A Practical Approach with a Mathematical Formulation of Risk. International Journal of Computer Applications, 2014, vol. 103, no 8.

[21] https://en.wikipedia.org/wiki/Expert_system last retrieved: December 13th 2015.

[22] NWIGBO STELLA, N. et CHUKS, Agbo Okechuku. Expert System: A Catalyst in Educational Development in Nigeria. 2011.