ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 3, September 2015

Communication system architecture based on sharing information within an SMA

S.ELHASNAOUI, A.CHAKIR, M.CHERGUI, H.IGUER, S.FARIS And H.MEDROMI
ENSEM- Hassan II University, LISER, EAS, Casablanca, Morocco

***Abstract*— IT GRC deals with issues of IT Governance, IT Risk and IT Compliance. Its processes support the information technology operations of an IT organization. In this paper we will present an autonomous communication system to support a solution which aligns IT GRC requirements. Multi agent system is used to support building a powerful communication system between components of IT GRC solution, which can multiply their capability and effectiveness. The proposed architecture is composed of three sub system which ensures all communication between strategic, decision and processing layers where agents involved in these systems can communicate in a distributed way using sharing information as a communication mode.**

***Index Terms*—IT GRC, governance, risk, compliance, multi agent system, COBIT, ITIL, ISO 27002, EBIOS, MEHARI, ISO 27005,**

I. INTRODUCTION

IT Governance, risk and Compliance, ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options setting direction. This is manifested by prioritization, decision making, and monitoring performance, compliance to achieve business progress [1]. There are several methodologies, standards, frameworks and good practices for IT GRC [2]. Each has its positive aspects and its limitations. It seemed that triggers were so much connected to a punctual event, as lack of strategic alignment, the problems of security…etc.. The diversity of frameworks raises a strategic difficulty for companies to choose the adequate IT GRC frameworks regarding top management choice As a result, IT GRC solution aims to combine IT GRC frameworks in an intelligent manner to take the right IT decision for business directives. It focuses on business objectives and proposes the best solution for an efficient IT management. This paper presents a communication system which provides communication between the layers of the IT GRC solution in a distributed manner. It is based on multi-agent systems that use information sharing as a mode of communication between the different agents. It allows evaluating any specific business goals in real time and in efficient way. The proposed solution takes the advantages of many technical solutions with modularity and autonomy aspects of every sub system. The paper contains the following parts: After the abstract and a brief introduction, we talk about fundamental aspects of IT GRC and its frameworks by discipline; we present next multi agents system. Then we present the proposed solution and detailed every sub system, finally conclusion and perspectives for this work.

II. IT GRC

GRC (governance, risk, and compliance) is an integrated and holistic approach to the organization that ensuring that the organization is ethically correct and consistent with its risk desire, internal policies and external regulations by aligning strategy, processes , technology, and people, improving efficiency and effectiveness[3]. IT GRC is seen as a part of GRC in general. The three IT GRC disciplines are subsets of their corporate complements as illustrated in figure 1 (Fig.1):

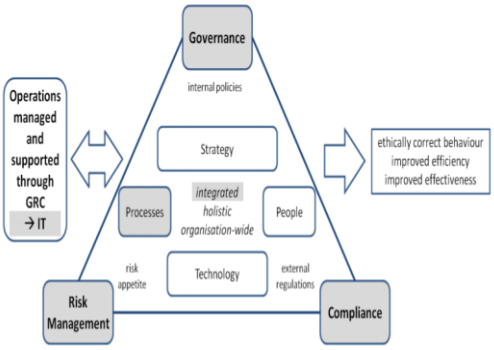


Fig. 1. Scope of GRC approach

A. IT Governance

IT governance corresponds to the implementation of the resources by which stakeholders can ensure the taking into account of their concerns in the operation of the information system (IS) [4]. IT governance aims to define the objectives of the information system to plan, define and implement processes related to the management of the lifecycle of the IS. These activities are based on the control and performance measurement of these processes to the objectives underlying its purpose is to provide business leaders and the shareholders that the IS function is well managed. The famous organization ISACA (Information Systems Audit and Control Association) who pays a lot of interest in the governance of information systems defines five pillars:

- Strategic Alignment
- Value Creation
- Risk Management
- Resource Management
- Performance measurement.

IT department has recourse to good practice guidelines: production with ITIL, COBIT with governance, security with ISO 27000, and project management with PMBOK ... [5].

DOI:10.17605/OSF.IO/ZJQT7

These standards support the diffusion of good practices within the company, the continuous improvement, the homogeneity of the process and contributing to the professionalization of the services delivered.

1) COBIT 5

COBIT (Control Objectives for Information Business year related Technology) is a methodology for evaluating IT services within the company. [6] This approach is based on a repository of 37 processes (best practices collected from experts SI) and on objective indicators (KGI) and (KPIs) to put the process under control in order to provide data for the company to achieve its objectives (alignment of technology on business strategy).

This is a control framework that aims to help the management to manage risks (security, reliability, and compliance) and investment. It does not provide guidance or recommendations to technical (technological choices, consolidation, crisis management ...). In other words, COBIT focuses on what the company needs to do, not how it should do. "

2) ITIL V3

ITIL [7] is an acronym for "Information Technology Infrastructure Library "(IT Infrastructure Library).ITIL Version 3 defines the service as an organization of human resources and IT (hardware and software), whose objective is the delivery of value for the company and the beneficiary of the service.

With ITIL Version 3, five groups of activities have been identified:

- Service Strategy: align IT strategy on business strategy, ensuring that the input value will enable the company to achieve its objectives.
- Service Design: Design Services from requirements collected by the Service Strategy.
- Service Transition: Ensuring the quality of the transition of a new service between studies and operations.
- Service Operation: Operate services effectively and efficiently.
- Continual Service Improvement: Creating conditions for continuous improvement of services.

3) ISO/IEC 27001/27002

ISO / IEC 27001 describe a process approach for establishing an ISMS (Information Security Management System). But if it sets the goal, it does not state specifically how it should achieve [8]. ISO 27002 presents a series of practical recommendations, addressing both technical and organizational aspects.

The standard defines a code of good practice for use by those responsible for implementing or maintaining a management system for information security. The information security is defined as "the preservation of confidentiality, integrity and availability of information". The standard offers 11 major fields of security using 133 security objectives (controls):

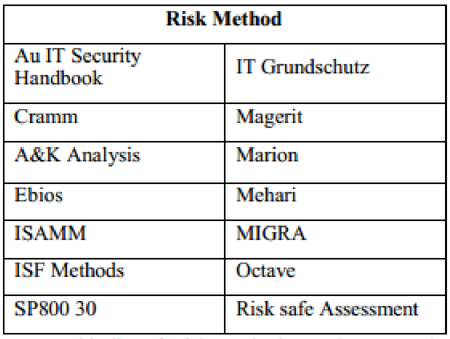
- Security Policy Information
- Organization of information security
- Asset Management
- Security related to human resources
- physical and environmental safeties
- Operation and Communications Management
- Access Control
- Acquisition, development and maintenance of information systems
- Incident Management
- Management Business Continuity
- Compliance.

B. IT Risk

Risk management is a set of coordinated activities to direct and control organization towards the risk [9]. It is generally identifies three goals in the management of risks to SI:

- Improve the security of information systems.
- Justify the budget allocated to the security of the information system.
- Prove the credibility of the information system using the analyzes.

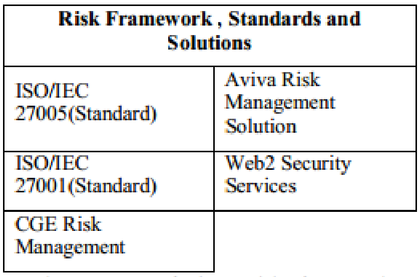
Risk management methods and tools enable the organization to plan and implement programs to maximize their opportunities and to control the impact of potential threats.



Risk Method	
Au IT Security Handbook	IT Grundschutz
Cramm	Magerit
A&K Analysis	Marion
Ebios	Mehari
ISAMM	MIGRA
ISF Methods	Octave
SP800 30	Risk safe Assessment

Table. 1. Risk methods

From this list of Risk Methods shown in the table (Tab.1) , we have tested MEHARI and EBIOS since they are the majorly used. The rest are mostly commercialized tools, only available in free trial with a limit of time. These two methods are proved very detailed and elaborated.



Risk Framework , Standards and Solutions	
ISO/IEC 27005(Standard)	Aviva Risk Management Solution
ISO/IEC 27001(Standard)	Web2 Security Services
CGE Risk Management	

Table. 2. Risks framework, standards and solution

Table 2 (Tab.2) presents some of risk frameworks, standards and solutions used by companies all over the world. For Example CGE Risk Management is an industrial solution that has multiple modules and one of them is dedicated to risk management and which is not available for free. On the other hand ISO 27001 states a set of guidelines that allows ensuring the respect of the limits of risk exposure for your information system [10].

C. IT compliance

IT compliance is a key element of a business' risk management profile and a crucial aspect of good corporate governance [11]. The broader concept of corporate governance captures the need for businesses to identify, understand and comply with the considerable number of laws, regulations and standards which affect how a business operates. The particular regulations concerning IT compliance focus on electronic data processing, networks and IT infrastructure. Becoming compliant requires a business to adopt best practice procedures including internal controls to protect IT systems, processes and ultimately the value of corporate assets. A number of regulations dealing with risk management have been introduced. These include Sarbanes-Oxley and laws on control and transparency in business, corporate governance codes, data protection and telecommunication laws as well as specific IT requirements.

III. SMA

A. What is an agent?

An agent is an entity (physical or abstract), autonomous in decision making, by his knowledge of itself and others, and its ability to act [12]. Experts multi-agent systems have classified agents into three major categories according to essential criteria that is the representation of its environment, and are therefore: Reagent agents, Cognitive agents and Hybrid agents.

B. What is a multi-agent system

A multi-agent system is a distributed system consisting of a independent agents, each with their own thread, specific to fulfill goals, and ways to communicate and negotiate with other to accomplish their goal [13][14]. Multi agents system is composed of the following elements:

- An environment with a metric in general.
- A set of objects, which can associate a position in an environment in a given time. Agents can perceive, create, destroy and modify these objects.
- A set of agents, which represent the active entities of the system,
- A set of relationships between agents between them;
- A set of operators that allow agents to perceive, produce, consume, transform and manipulate objects.

C. Agent communication

Basic communication options used in an SMA are:
-Communication through information sharing
-Communication by sending a message

Our proposed architecture is based on the first option.

IV. COMMUNICATION SYSTEM ARCHITECTURE BASED ON SMA USING SHARING INFORMATION MODE

The proposed model is a modular multi-agents architecture where all components are managed and controlled by different types of agents which are able to cooperate, propose solutions on very dynamic environments and face real problems (Fig.2). This solution helps to enable to establish communication between layers of the IT GRC solution in an intelligent manner, allowing IT organizations to overcome obstacles and achieve its objectives. The proposed architecture is based on the communication by sharing information. Agents of system are not then directly connected, but share a common database where there is knowledge related to resolution that evolve during the execution process. Information sharing mode organizes the resolution of problems through cooperation of all system agents (which are considered sources of knowledge). Each agent has read or writes to the shared database. The common database is shared; its use implies that several agents can be access conflicts during the resolution process. That is why we created a control agent whose mission is to manage the access conflicts between agents, that they cannot read or modify data already being edited. To gain a deeper understanding of the proposed architecture, we describe each sub system of the communication solution.

1) Strategic Layer-com

It manages the incoming IT processes from strategic layer to be managed by Manager Agent. Agents of this sub system accesses to the 1st level of the common database which is devised into 3 sub level.

Data collection Agent: accesses the 1st sub level in which he can write / record requests EAS-preventing strategy and must rank them according to priority / arrival.

Manager Agent constitutes a main component of IT GRC Categorization system: it allows categorizing the processes received according to three disciplines of IT GRC (IT governance: ITIL, ISO/IEC 27002, PMBOK, CMMI…, IT Risk: EBIOS, MEHARI, ISO/IEC 27005…, IT Compliance: SOX or 08:09 laws).

It reads queries classified by the data collection agent and accesses the second sub level as to associate each IT processes belonging to a discipline of IT GRC and later to one or more IT frameworks.

Building Matrix Agent: accesses the second level to retrieve the result of categorization and written in the third sub level in the matrix.

1) DesicionLayer-com

This system provides communication with the Decision making layer. Agents of this sub system accesses to the 2nd level of the common database which is devised into 2 sub levels.

DOI:10.17605/OSF.IO/ZJQT7

Agent DD: Accesses the third sub-level 1 to retrieve the matrix and send it to Decision layer after saving it into the first sub level 2

Agent DD: Enters the second sub level 2 to write the result of the Decision from Decision layer.

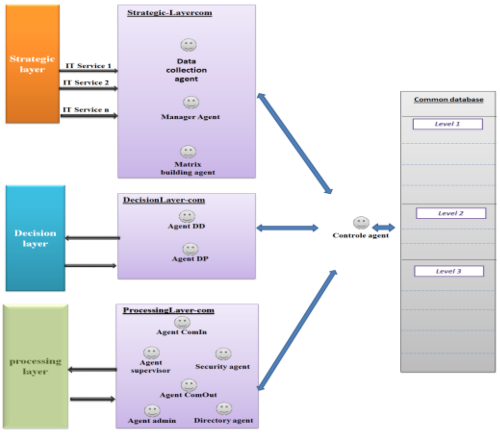


Fig 3.Overview of communication system architecture based on multi agent system and a common database

2) *ProcessingLayer-com*

This system allows managing communications that are related to processing layer. Agents of this sub system accesses to the third level of the common database, which is devised into 5 sub levels.

Agent ComIn: accesses the second level to read the result of the decision and saves it in the first level 3.

Admin Agent: retrieves this result and consults the 2nd sub level 3 to choose processing system that will handle each IT process the matrix.

Agent ComOut: accesses the 3rd sub level 3 to read the result of the decision and send it to adequate processing system.

Directory Agent: receives the result of processing and saves it in the 4th sub level 3.

Supervisor Agent: consult the 3rd and 4th sub level of the 3rd level to calculate the performance of the processing system. The calculation result will be recorded in the five sub level 3.

3) *Control Agent*

This agent acts as a scheduler and a monitor at a time. It selects the next agent to run depending on the overall state of the shared database. To do this, it has an agenda containing executable agents and calculates the priorities associated with each potential activity of each agent of EAS-COM. It fixes the priority activity to execute.

For this, we have established a table showing the access authorized by the control Agent.

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
(1)		🟨								
(2)			🟨							
(3)				🟨						
(4)					🟨					
(5)						🟨				
(6)							🟨			
(7)								🟨		
(8)									🟨	
(9)										🟨
(10)										

(1): **Data collection Agent**	(6) **Agent ComIn**
(2) **Manager Agent**	(7) **Admin Agent**
(3) **Building Matrix Agent**	(8) **Agent ComOut**
(4) **Agent DD**	(9) **Directory Agent**
(5) **Agent DD**	(10) **Supervisor Agent**

🟨 For (i=1, i<11, i++)

Agent (i) accesses to the common database and agent(i+1) cannot access to the common database

V. CONCLUSION AND DISCUSSION

In this paper, we illustrated the design of our architecture which has the objective to establish a powerful communication system between components of IT GRC solution, which can multiply their capability and effectiveness. The proposed architecture is composed of three sub system ensures all communication with strategic, decision and processing layers where agents involved in these systems can communicate in a distributed way thanks sharing information mode. This work is important because of the infinite possibility that it gives to IT GRC solution in order to comply with IT GRC management. In this paper, we discussed the general proposed solution. Then we detailed the each sub system of the architecture and the workflow of procedures from end to end. This particularity of our approach is to use sharing information communication mode that add the uniquely intelligence to our application. The advantage of this communication mode is that little information is lost and there is the opportunity to correct the error very quickly. But the inconvenient of this solution is that there is the risk of accumulation of unnecessary data. In addition, the combination of a several standards, frameworks and methods, internationally recognized, and multi-agents systems provides the ability to achieve the governance of information system and manage risks and compliance activities on an all-encompassing perspective of IT GRC. Future works consists on proposing a communication architecture based on passing message between agents of the system, in order to compare the both proposition and implementing the best proposed model in order to overcomes obstacles and achieve IT organization objectives.

REFERENCES

[1] Nicolas Racz, Edgar Weippl, Andreas Seufert "A process model for integrated IT governance, risk, and compliance management" Databases and Information Systems. Proceedings of the Ninth International Baltic Conference, Baltic DB&IS 2010. Riga: University of Latvia Press, pp. 155-170.

[2] M.N. Kooper, R. Maes, E.E.O. Roos Lindgreen "On the governance of information: Introducing a new concept of governance to support the management of information". International Journal of Information Management: The Journal for Information Professionals, Volume 31 Issue 3, June, 2011, Pages 195-200.

[3] Racz, N., Panitz, J.C., Amberg, M., Weippl, E. & Seufert, A. (2010): Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a survey among large enterprises. In: ACIS 2010 Proceedings, Paper 21. Retrieved 13 December 2010 from: http://aisel.aisnet.org/acis2010/21.

[4] S.Elhasnaoui, H. Medromi, A. Sayouti, Multi-agents modeling solution for IT governance based on ITIL" International Conference on Engineering Education and Research, ICEER 2013.

[5] S.Elhasnaoui, H. Medromi, S. FARIS, H.IGUER, A. Sayouti "Designing a Multi Agent System Architecture for IT Governance Solution" International Journal of Advanced Computer Science and Applications IJACSA Volume 5 Issue 5 May 2014.

[6] Patrick Stachtchenko, « COBIT 5, ses apports pour management et la gouvernance du SI », 25 Janvier 2013.

[7] Delbrayelle, Introduction à ITIL V3 et au cycle de vie des services, juillet 2011. ISO office, "Information technology — Security techniques— Code of practice for information security management", 2005.

[8] ITGI and OGC, "Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit" 2008.

[9] Neeta Shukla, Sachin Kumar, " A comparative study on information security risk analysis practices" on Issues and Challenges in Networking, Intelligence and Computing Technologies – ICNICT 2012, November 2012.

[10] 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» International Symposium on InterCloud and IoT -ICI Symposium 2014.

[11] Racz, N., Weippl, E. & Bonazzi, R. (2011): IT Governance, Risk & Compliance (GRC) Status Quo and Integration. An Explorative Industry Case Study. In: Proceedings of the 1st International Workshop on IT GRC, ITGRC 2011.Washington: IEEE.

[12] A.Sayouti, H. Medromi, Book Chapter in the book "Multi-Agent Systems - Modeling, Control, Programming, Simulations and Applications", ISBN 978-953-307-174-9, InTech, April4, 2011.

[13] Shoham, Y. Agent-oriented programming. Artificial Intelligence, February 1992. Stanford, USA.

[14] J. Ferber, "Les systèmes multi-agents, vers une intelligence collective", InterEditions, 1995, pp. 63-144.