The Compliance of Information Technology based on Multiagents Systems and the SOX Law

Wafaâ Bouab Bennani
TIC Team, LSI, ESTEM
Research Center
Casablanca, Morocco

Pierre Nlend
TIC Team, LSI, ESTEM
Research Center
Casablanca, Morocco

Adil Sayouti
Team Architecture of Systems
LISER - Laboratory
ENSEM, Hassan II University

ABSTRACT

The governance of information system contributes, among other things, to ensure the governance of compliance for the benefit of corporate governance. The multiplicity and diversity of laws in the field of IT governance place information systems managers of SMEs-SMIs before a problematic of compliance obligation especially that the laws, which are now of international and national order, are subject to change, and sometimes may be antagonistic.

The objective of this work is to study the various options for an exhaustive integration of all the laws that deal with governance compliance whether national or international into a comprehensive, cognitive and evolutionary platform.

In this paper, we propose the integration of a modular and scalable multi-agent system that allows the laws to evolve within the governance platform.

Keywords

Governance, IT Governance, CRM, Compliance, Multi-Agent Systems.

1. INTRODUCTION

Governance refers to the set of measures, rules, decision-making bodies, and information and monitoring that ensure proper operation and control of a state, institution or organization, whether public or private, regional, national or international.

In the highest political circles, one speaks of "Good Governance" as a national necessity seeking efficiency in the effective management of the state.

The concept of governance originated in reports issued by national organizations such as the UN organization, particularly in such instances as the United Nations Development Program (UNDP). This program is the global UN development network, advocating change and connecting countries to knowledge, experience and information resources to help their people to improve their lives.

We can define good governance in six points:

- Accountability

Public authorities should be able to show how their actions and decisions are consistent with the specific objectives agreed on.

- Transparency:

Actions, decisions, government decision-making should, to some extent, remain open to verification by other government sectors, the Parliament, civil society and sometimes by institutions and external authorities.

- Efficiency and Effectiveness

Public authorities should be dedicated to quality production—particularly in the services provided to citizens—and ensure that their effective performance meet the intended objectives set by public action operators.

- Responsiveness

Public authorities should have the sought-for means and flexibility to respond quickly to changes in society; they must take into account the expectations of civil society with regard to serving public interest, and should be ready to examine critically the role of the state.

- Foresight

Public authorities should anticipate problems that arise from the data available and the trends observed, and develop policies that take account changing costs and the predictable changes (demographic, economic, environmental, etc.).

- The rule of law

Public authorities need to enforce the laws, regulations and codes in all fairness and transparency.

2. IT GOVERNANCE

Initially used to describe how a government exercises its economic, political and administrative authority and how it manages a country's resources for development purposes, the concept of "governance" has been extended to corporate management**.** In a narrower sense, corporate governance is the relationship between the shareholders and company management, more particularly the operations of the Board of Directors, of the Management Board, or of the Supervisory Board. According to the IT Governance Institute, corporate governance "aims to provide strategic direction in order to ascertain that objectives are achieved, the risks managed, and the resources used responsibly." Its priority concern is to respect the interests of the "beneficiaries" (citizens, public authorities, partners, shareholders ...) and to ensure that their voices are heard in the running of the business affairs.

The governance of information systems or IT Governance [1] is meant therefore to define, describe, implement, monitor and continuously improve the management processes, operational processes and organization to enable information systems to meet the needs of the business and provide efficiently value while holding in check potential risks.

Information system governance contributes by:

- Ensuring compliance governance for the benefit of corporate governance, and
- Optimizing governance performance for corporate governance.

3. THE REFERENCE FRAMES OF GOVERNANCE

Most reference frames are specific to a particular area such as ISO 27001 and 27002 for IT security, and PMBoK for project management. There is a large number of reference frames for an organization that can be classified into four categories:

- The standards describing good practice guides
- The criteria used to obtain additional certifications
- Reference frames detailing some technical points related to safety
- The standards imposed by regulatory requirements

For good practice guides, these are typically COBIT, ITIL, CMMI, and ISO 27002. They can cover all areas related to Information Technology.

3.1 COBIT

COBIT (Control Objectives for Information and related Technology) is a set of the best practices designed to help optimize IT investments, ensure service delivery, and provide the metrics to refer to for assessing dysfunctions. COBIT [2] is an internationally framework conceived in terms of the best global practices in auditing and IS control. COBIT is oriented process. It defines IT activities in a generic process model that can be divided into four areas. These domains are Plan and Organize, Acquire and Implement, Deliver and Support, Monitor and Evaluate.

With respect to the COBIT framework, these domains are especially cut out to:

- Plan and Organize (PO): to provide guidance in problem-solving (AI) and service delivery (SD) (10 processes).
- Acquire and Implement (AI): to provide solutions and submit them in order to turn them into services (7 processes).
- Distribution and Support (DS): to receive the solutions and make them usable for end-users (13 processes).
- Monitor and Evaluate (ME): to monitor all processes to ensure that guidance is respected (4 processes).

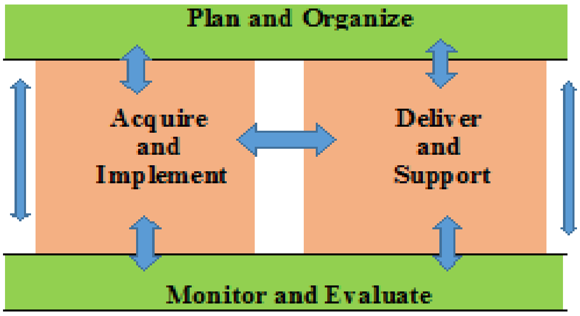

Fig 1 COBIT Process

3.2 ITIL

ITIL (Information Technology Infrastructure Library) is a set made of the best practices for operating an information system [3]. ITIL philosophy is based on four fundamental concepts:

- The first of these is the inclusion of customer expectations in the implementation of IT services that English speakers call Customer Focus.
- The second principle stands for the life cycle of IT projects that integrate from the outset different aspects of management of IT services.
- The third founding concept recommends the implementation of interdependent ITIL processes to ensure the quality of services.
- The fourth and last principle is the implementation of a quality approach to the services installed, and of a measure of this quality taken from the users' perspective. With respect to ITIL, service quality is based on a structuring of activities in interrelated, measurable and repeatable processes. A large number of companies now recognize this management approach to by-process activities as the most effective. ITIL has adopted this solution by cutting IT-service management into ten processes. This partition is recommended and can be adapted to each company's needs.

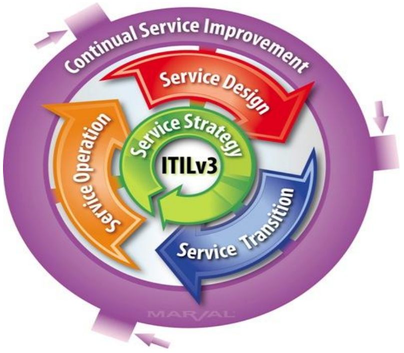

Fig 2: ITIL Process

3.3 PMBoK

The Project Management Body of Knowledge (PMBoK) is the Project Management Institute's Guide defining the fields of knowledge covering project management, and identifying good professional practices. As such, it serves as a reference base for establishing course contents on project management and for developing certification examinations. The PMBoK (Fourth Edition) is an ANSI* official standard, internationally recognized (IEEE Std 1490-2003), which documents the best practices and the fundamentals of project management. [4] It is general in scope and applies to projects in many sectors, such as construction, software, engineering and industry, etc.

This version, published in 2009, lays particular emphasis on a better management at the level of stakeholders while harmonizing, removing and repositioning certain actions within areas of knowledge.

The PMBoK defines the five process groups of project management as follows: Initiating, Planning, Executing and controlling, and Closing.

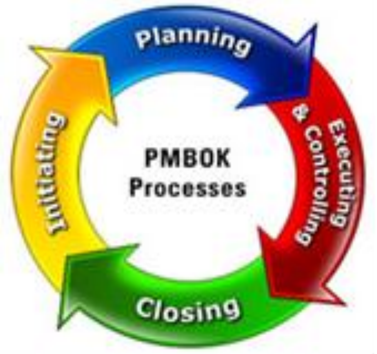

Fig 3: PMBOK Process

PMBOK covers nine areas of project management skills, namely:

Integration management

Content management (perimeter)

* American National Standards Institute

Time management

Cost management

Quality management

Human Resources management

Communications management

Risk management

Supplies management

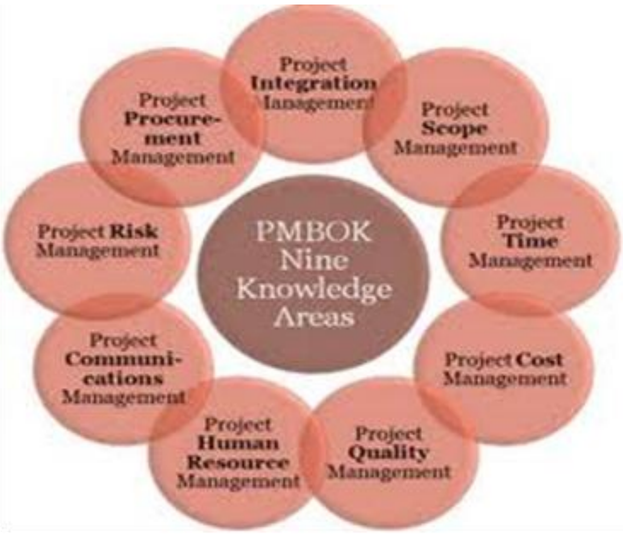
Project Integration Management
Project Scope Management
Project Time Management
Project Cost Management
Project Quality Management
Project Human Resource Management
Project Communi-cations Management
Project Risk Management
Project Procure-ment Management
PMBOK Nine Knowledge Areas

Figure 4. PMBoK Areas of competence

PMBoK distributes 42 processes in total in these process groups and knowledge areas.

3.4 ISO 2700 X

The international standard ISO 27001 specifies a management system of information systems (SGSSI) [5]. SGSSI is structured in four recurring steps (plan, implement, verify, improve) to comply with the principle of the Deming wheel, emanating from the matrix of quality. This concept helps to draw a parallel with the standards of quality management systems (ISO 9001) and of the environment (ISO 14001).

To operate this SGSSI, the ISO 27001 standard recommends the use of its Annex A or ISO 17799 to identify the security measures that need to be implement during the planning stage.

The international standard ISO 17799 is a guide of good practice containing 39 security objectives, subdivided into 133 security measures, and relating to 11 areas (security policy, personnel security, access control ...). The security objectives set the goal to reach, while the security measures present the activities whereby to achieve such a goal, explaining the actions to perform in order to implement these measures.

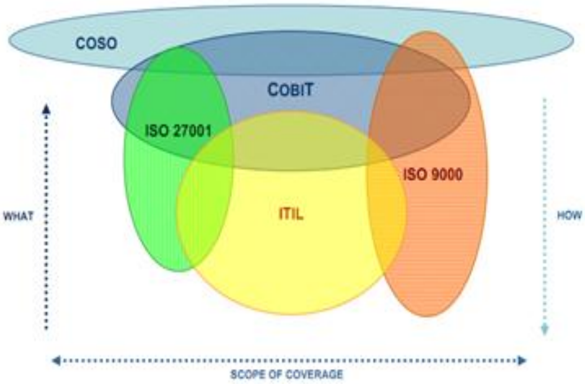

Fig 5: ISO 27001 Reference Frame

We often consider the implementation of an IS reference frame more as an obligation of compliance than as investment. Indeed, many companies justify their implementing of reference frames on legal grounds, or for reasons of compliance or quality. The best-known regulatory frameworks are SoX, Basel, SAS 70 and LSF. The implementation of guidelines for good practice and standards helps to comply with the regulatory requirements defined by these standards.

4. LAWS

In making their choice of the particular process to set up, information systems managers are faced with the problem of the diversity of laws as well as that of the exhaustiveness of the laws to abide by.

The CIO must comply not only with US laws (SOX), French (LSF) but also with Moroccan laws: 09-08 personal data laws; Consumer Protection law, and the law of industrial property.

4.1 SOX

The Sarbanes Oxley law, an acronym made of the respective names of the two Senators Paul Sarbanes and Michael G. Oxley (on his initiative), was adopted by the US Congress in July 2002. This law, also known as the Public Company Accounting Reform and Investor Protection Act of 2002 or more simply SOX or Sarbox, is the answer to many accounting and financial scandals: Enron, WorldCom, Tyco International, occurring in some countries in the early 2000s.

In the US the 2002 law, on the reform of accounting for listed companies and of investor protection, is a federal law imposing new rules on accounting and financial transparency.

4.1.1 The Requirements of the Sarbanes Oxley Act

The Sarbanes Oxley law provides an even more severe framework for the production of accounting and financial documents. The penalties for the falsification of balance sheets can reach 20 years imprisonment. The promulgation of this framework law is accompanied by the creation of an independent regulatory agency, the Public Company Accounting Oversight Board, or PCAOB. Among other functions, the PCAOB is responsible for the supervision of accounting audits.

Quite comprehensive in scope, the Sarbanes Oxley law has many obligations whose origins do not lie far off. These include the prohibition of an audit company to combine consulting and auditing services for the same client, the obligation of CEOs and CFOs to sign the financial accounts and reports, and the necessity to supervise the financial benefits (loans) granted by the company to its executives.

This extra-territorial legislation applies to all US companies listed or unlisted on the New York Stock Exchange.

4.1.2 *New obligations*

The law of 31 July 2002 (Pub. L. No. 107-204, 116 Stat 745), called the Sarbanes-Oxley Act, introduced:

- • The obligation of the presidents and CFOs to personally certify the accounts;
- • The obligation to appoint independent directors to the audit committee of the board of directors;
- • The supervision of the particular benefits granted to managers (loss of incentives in case of the dissemination of inaccurate information, the prohibition of loans taken from the company, the possibility accorded to the SEC (Securities and Exchange Commission as the regulator of US stock markets) to ban all social mandate for leaders suspected of fraud).

4.1.3 *Extra-Territoriality*

Because a number of non-US companies are listed on the New York Stock Exchange, the largest global stock exchange, and are therefore subject to this law, SOX has repercussions beyond the US borders. This is why we talk about extraterritoriality with regard to the impact of the SOX law.

Issuers are required to disclose publicly, on an urgent basis, information on important changes in their financial position or operations. This information should be presented in easily understandable terms; or else, through supportive trends and graphic qualitative information.

4.2 *The LSF Financial Security Law in France*

The French Parliament adopted the Financial Security Law (LSF), also called the Mer Law on behalf of the French Finance Minister on duty Francis Mer, on 17 July 2003 in order to strengthen the legal provisions relating to corporate governance. LSF is published in OJ n° 177 of 2 August 2003 (No. 2003-706 of 1 August 2003).

This new law applies to all public companies and to companies using public savings; these provisions are applicable for the accounting periods beginning on 1 January 2003.
Like the US Sarbanes-Oxley, the Financial Security Law is based primarily on:

- • Increased management liability
- • A strengthening of internal control
- • A reduction of the sources of conflicts of interest.

4.3 *Moroccan Laws*

Henceforth, ISDs must also concord with Moroccan legislation and particularly:

- • The Moroccan Law 08-09: for the protection of individuals with regard to the processing of personal data
- • Consumer Protection Law
- • Industrial Property Law

4.3.1 *The 08-09 law for the protection of personal data has just been promulgated*

Moroccan law n° 08-09—promulgated by Dahir n° 1-09-15 of 22 Safar 1430 (18 February 2009) on the protection of individuals with regard to the processing of personal data—addresses the question of the actors involved in personal data processing.

Long awaited, the 08-09 law on the protection of personal data has just been provided, together with its implementation decree. One first step of reform, openness and modernization undertaken by Morocco. Nevertheless, the road is still long for its extension to the different socio-economic spheres of the country.

For legislature, the objective of the 08-09 law is to provide the Moroccan legal arsenal with a lawful instrument to protect individuals against abuses in the use of data that may infringe upon their privacy, and to harmonize the national system of personal data protection with its partners as defined by the European authorities.

Thus, the law defines, inter alia and with accuracy, the right of access to databases containing personal data, to counter certain treatments, to request correction of erroneous data or to delete outdated data or those whose objective is already achieved. In addition, the law has set the conditions of transfer of personal data to foreign states by requiring that these states have a level of protection of personal data deemed adequate by the supervisory body that it has established, including the National Commission for data Protection CNDP.

The CNDP enforces the rights (of access, rectification, and opposition) of any person concerned with the automatic (computer) or non-automatic processing of personal data.

We can consider that the CNDP exercises one of the functions performed by the CNIL in France (Commission Nationale Informatique et Libertés). The CNIL is responsible for ensuring respect of human identity, privacy and freedom in a digital world.

4.3.2 *The Consumer Protection Act*

The provisions and mechanisms for implementation of the new law 31-08 relating to consumer protection are always at the center of debate.

Entry into force in April 2011, the law intervenes to protect consumer rights, the right to information, to retraction, the freedom of choice and representation, and the right to protection against unfair terms that may figure in some mortgage or consumption contracts.

Indeed, the right to information takes on great importance in the new law. Accordingly, legislation compels suppliers to enable, by all appropriate means (marking, labeling, posting), consumers to know the essential features and prices of the product, asset or service in order to help them make a rational choice, taking into account their needs and resources. In addition to the prohibition of misleading advertising and soaring sales, legislation has regulated comparative advertising, distance selling, sale, canvassing, the lottery, as well as sale with bonuses. By virtue of 206 articles, the aforementioned law is meant to grant consumers the status of full economic players. And that is by laying down the conditions and procedures regarding compensation or reparation for the damages affecting them; and by ensuring the representation and the defense of consumer interests through consumer associations constituted in accordance with the provisions of law 31-08.

4.3.3 Law No. 97-17 on the Protection of Industrial Property (promulgated by Dahir No. 1-00-91 of 9 Kaada 1420 of 15 February 2000)

This Law is to protect patents, layout-designs (topographies) of integrated circuits, industrial designs, trademarks, trade or service, trade name, indications of source and designations of origin and the repression of unfair competition relating to the foregoing.

Problematic

The tools should contain the list of laws in a knowledge base and the ISD is to comply with these laws. Because the laws evolve, the tools integrating IT governance must evolve, too. You need therefore a cognitive tool to change this knowledge base.

In this paper, we propose the integration of a modular and scalable multi-agent system to change the laws in governance platform.

5. MULTI-AGENT SYSTEMS

5.1 *Expected Properties of our platform*

Governance platform for ISD reflects the complexity of the tasks entrusted to it and of the environment in which it must operate. Many properties for the platform to offer are sought: action, adaptation, anticipation, learning, independence, intelligence, self-organization, perception, reactivity. The scientific community has proposed many techniques meeting these properties but their sound blending remains a research prospect.

5.1.1 Intelligence

The intelligence word refers to a faculty whose contours are not significant from a scientific point of view. There is no single and acknowledged definition of intelligence; we talk about forms of intelligence or intelligences. Under this denomination are brought together different event groups and activities such as the adaptation of the means to achieve a goal, the use of real or abstract tools for action, building representations of external or internal phenomena that are then used to understand and prepare future action. Intelligence does not therefore consist solely in the handling of knowledge, i.e., cognition; it is also present in the voluntary actions of living things as these actions may amount to the resolution of the problem or to decision making.

The aim of a platform is to create a system capable of carrying out properly the mission entrusted to it. The challenge is to achieve its goal in increasingly complex missions within increasingly varied and unpredictable environments. To this effect, it uses, develops and/or experiments with information processing techniques, taking little cognizance of what relates or not to intelligence. This pragmatic approach is similar to that of Mc Farland [McFarland, 1993] when connecting the intelligence level of performance with a given function. This level of performance is relative but can be used to compare different systems. Studies on humans or animals, and on the mechanisms that can be linked to intelligence must not however be ignored. They are a very interesting source of inspiration for IT professionals.

5.1.2 Autonomy

Autonomy is the ability to withstand external shocks using internal resources. Autonomy is a relative rather than absolute power. For ISD, it is linked to its capacities—capacity for decision-making and action, strength, energy resources, perceptive sense...— to the characteristics of the environment in which it is immersed and their variations, and finally to the tasks to perform. The concept of autonomy is complex when considering the interaction of an ISD with its environment. It involves both a system’s independence from, and dependence on, the environmental constraints, in that it is from that environment that the system derives the necessary information liable to determine the action it should take towards autonomy.

There are many definitions of autonomy. Here are two examples. According to Mc Farland [McFarland, 1993], one can predict the behavior of an automatic system as soon as one knows its inner workings. An autonomous system maintains accordingly its own control and possesses thereby a kind of motivation; as a result, this makes relatively uncontrollable by an external system. According to Steels [Steels, 1995], a system is autonomous if it develops laws and strategies that would enable it to control its behavior. In fact, autonomy is a relative capacity and we can consider that there is an insensible progression from the lowest to the highest level. It represents the ability to choose a strategy in terms of sub-goals and/or means to achieve a set goal. We believe that a system can be qualified as autonomous if it chooses to execute laws without developing them. This point of view considers autonomous any reactive system that independently selects its behavior, but solely in terms of the events perceived in its environment. For some, this system can be described as purely automatic and deterministic. With these systems, Braitenberg [Braitenberg 1984] has demonstrated that an observer may attribute to them an autonomous behavior while they are composed of deterministic elements only. Autonomy may appear to the observer's eye when they do not know the inner workings of a system. Thus, it does not seem impossible to attribute to a system some autonomy through a sound blending of deterministic components whose actions depend on its perceptions.

5.1.3 Adaptation

Adaptation is an essential characteristic of living beings. It allows them to be in harmony with their living conditions. It consists in the ability to maintain performance in the face of environmental changes, tasks or one’s own abilities. It results in different skills including learning, development and evolution. The ability to adapt can be assessed with respect to the variation it brings to the system or to the evolution of the phenomenon, which is held to trigger it. We can therefore consider that adaptation is a relative capacity for which we can distinguish several levels. For example, for a mobile system, the lowest level may consist in the simple adjustment of a few parameters. In an ISD, adaptive capacity includes learning ability and cannot exist in the same system unless the capacity for autonomy at a similar level makes it possible. Autonomy and adaptation therefore evolve simultaneously.

5.1.4 Learning

Learning is a process of acquiring knowledge. For an ISD, knowledge may relate to its environment, the relationship between its actions and perceptions, and the relationships between its behavior, goals and their achievement. Learning can allow a system to adapt its behavior to the situation at hand. In the current state of research in this area, there is a supervised learning, where the system is guided toward the phenomenon we want it to learn, and an unsupervised learning in which the system is left to itself. Learning is usually a long process and requires relatively favorable conditions in order to be completed. The system typically uses a learning base that must be representative of the phenomena to learn and the conditions in which they are encountered.

It is desirable that a system learns by itself all the knowledge it needs, but it seems impossible or inappropriate in practice. Some knowledge must be provided to the system. For example, learning in a risky environment may lead to irreparable injury before learning anything about the hazards. As we show where danger lies to a person before he or she becomes a victim, knowledge whose cost of acquisition is too high or impossible to satisfy must, similarly, be fed into the system. We can then provide the system with all the knowledge made available and useful by its creator. This idea is faced with the problem of adaptation that does not take place because of the fixed nature of the implicit knowledge provided. Thus, there seems to be a difficult compromise between the choice of innate knowledge and the one to be acquired.

5.2 Expected Properties of our platform

A good platform for governance must be modular, integrating the different expected capabilities as cited above. A multi-agent system is a set of agents that have certain autonomy, a certain degree of artificial intelligence, and a representation of their environment; they interact with it, they are able to take the initiative to communicate with each other, and they can adapt to different situations. The need for these concepts at the different levels of the governance platform indicates a need for autonomy and intelligence and validates somehow our choice of a multi-agent approach. [6]

5.2.1 Agent

An agent [7] is a located entity, real or virtual, acting in an environment, able to perceive it, to act thereon and interact with the various components surrounding it. An entity is an agent if it is capable of exercising local control over its processes of perception, communication, knowledge acquisition, reasoning, decision-making and execution. The main characteristics of an agent are:

- Autonomous
  - An agent has a certain degree of autonomy,
  - An agent has certain states (inaccessible to other agents and system components)
  - An agent can make certain decisions with respect to its states (without direct outside intervention).
- Located
  - An agent is located within its environment (physical or virtual)
  - An agent has a representation of its environment.
- Reactive
  - An agent can perceive its environment via sensors,
  - An agent can act on its environment through effectors.
- Social
  - An agent is able to interact and communicate with other agents (via communication languages)
  - An agent is able to cooperate to solve problems or complete tasks.
- Proactive
  - An agent is able to "take the initiative" to achieve its goal or perform tasks (and to adopt appropriate behaviors).
- Active
  - An agent is still active. It therefore necessarily runs in a thread or a separate process.
- Learning
  - An agent is able to learn and evolve in proportion to this learning,
  - An agent is able to change behavior (based on past experiences).

5.2.2 Multi-Agent Systems

A multi-agent system (MAS) is a company of agents where interactions between agents and their environment lead to a behavior conducive to the achievement of an overall goal. The main characteristics of a multi-agent system are:

- A set of agents acting and working independently of each other,
- Each agent is part of the system,
- Each agent works to accomplish its tasks,
- Each agent is able to communicate and interact with other agents,
- An agent cooperates with other agents when necessary,
- An agent is able to coordinate its activities with other agents to access the resources and shared services that it needs (to achieve its goals)
- The agents have a common goal (if it is not a reactive or emerging MAS), each agent has a partial view of MAS.

6. THE PROPOSED MAS LAW

In this paragraph, we propose a general architecture integrating a multi-agent system law within the platform of governance GRC. This architecture is designed to address the issue related to the diversity of laws.

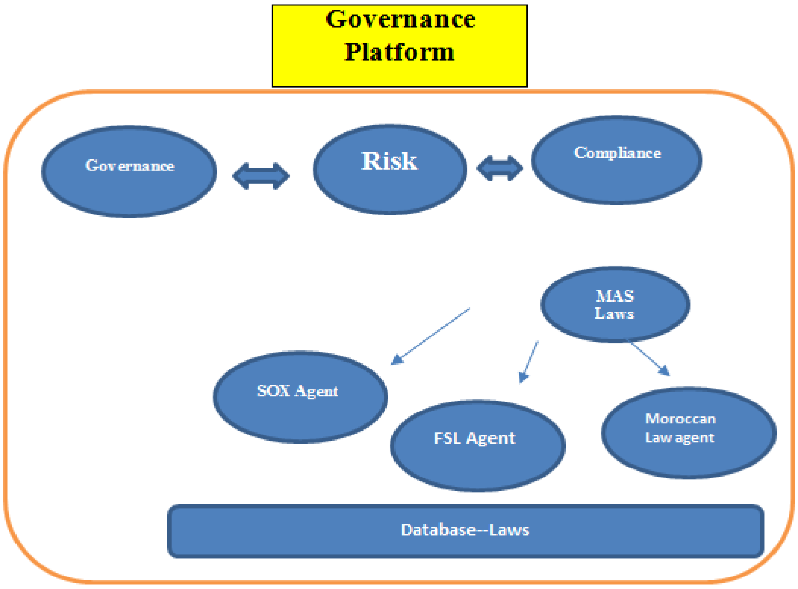

Fig 6. General Architecture proposed for MAS Laws

7. CONCLUSION

Our In this paper, we have proposed the integration of a modular and scalable multi-agent system.

We have studied the reference frames of IT Governance as well as the laws related to the compliance of information systems. The issue of the compliance obligation for IT managers has led us to think about developing a platform based on a modular, scalable multi-agent system to help laws evolve within a governance platform.

This platform can meet the compliance requirements of information systems. A reflection needs to be engaged on a larger scale, however, to help this platform develop, taking into account globally the parameters of Governance, Risk and Compliance. template.

8. REFERENCES

[1] White Paper: KPMG: Governance, Risk Management and Compliance: Increase value by monitoring controls.

[2] COBIT 4.1 by The IT Governance Institute (ITGI) ISBN: 9781933284729.

[3] www.itilfrance.com, [Ferber, 1995] J. Ferber. "Multi-agent systems, towards a collective intelligence." InterEditions 1995.

[4] New Methodology for Governance of Information Technology-based Multi-Agent System. Authors: Jamal Skiti & Hicham MEDROMI

[5] The Governance of the Information Technology based Multi-Agent System and the COBIT framework. Authors: Jamal Skiti & Hicham MEDROMI

[6] "Autonomous and Intelligent Mobile Systems based on Multi-Agent Systems" Authors: A. and H. Sayouti Medromi Book Chapter in the book "Multi-AgentSystems Modeling, Control, Programming, Simulations and Applications ", ISBN 978-953-307-174-9, InTech, April4, 2011.

[7] J. Ferber. "Multi-agent systems, towards a collective intelligence." InterEditions 1995.