Securing an Enterprise through Governance, Risk and Compliance Using an IT GRC Platform Based On Multi-Agents Systems

Mohamed GHAZOUANI, Redouane ELALJ

Abstract— **The implementation of appropriate security controls for an information system is an important task that can have major implications for the operations and assets of an organization. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. One such intelligent choice is Securing an enterprise through Governance, Risk and Compliance. This paper aims to make an implementable, realistic, cost-effective, and workable platform available to IT managers which they can adapt to their own enterprises. Our methodology gives answers to several important questions that should be answered by organizational officials when addressing the security considerations for their information systems.**

Index: IT GRC, COBIT, MEHARI, Multi-agent system (MAS).

I. INTRODUCTION

Information is a key resource for all businesses, and from its creation to its destruction, technology plays an important role. The inappropriate use of technology could adversely affect the Company's performance and competitiveness or put them at risk of violating the law. As a result, today, more than ever, enterprises and their executives strive, based on an integrated approach to information technology governance, risk and compliance (IT GRC), to maintain high quality information to support business decisions, generate business value from IT-enabled investments, achieve operational excellence through the reliable and efficient application of technology, maintain IT-related risk at an acceptable level, optimize teh cost of IT Services and technology and comply with laws, regulations, contractual agreements, policies, etc.

II. GOVERNANCE

During the past decade, the term "governance" has risen to the forefront of the organization's thinking. Organizations from around the world have taken advantage of the establishment of good governance while others, devoid of such governance, suffered significant setbacks. The best way to ensure that the compromise does not happen is to implement and sustain IT governance program within the organization [1]. Developing policies represents the first step for any effective risk management and compliance program. Policies help align the organization to management's vision, effectively communicating how leaders wish the organization to operate and providing important guidance to management. Policies help align the organization to management's vision, effectively communicating how leaders wish the organization to operate and providing important guidance to management. Most managers welcome these guidelines when determining their course of action. While many policies appear to be obvious, most organizations implement governance based on established frameworks (such as COBIT 5). Developing an effective set of policies is a top–down effort based on an established framework, sensitivity to the objectives of the organization, the risks management faces, and regulatory compliance.

Policies support the organization's governance by meeting stakeholder needs and addressing risk. The upper-level management communicates their strategy through a collection of policies provided to the management.

The risk assessment highlights the most important areas of concern and allows management to construct policies that address these areas, and most policies follow established frameworks.

III. RISK MANAGEMENT

Risk management is the practice of looking at what could go wrong and then deciding on ways to prevent or minimize potential problems. It encompasses four components: frame risk (i.e., establish the context for risk-based decisions); assess risk; respond to risk once determined; and monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.

Risk assessment allows managers to evaluate what needs to be protected relative to operational needs and financial resources. This is an ongoing process of evaluating threats and vulnerabilities and then establishing an appropriate risk management process to mitigate potential monetary losses and harm to an organization's reputation [1].

Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization" (ROSS Gemini Centre 2011).

IV. COMPLIANCE

Compliance is the term that has a general meaning that is closest to the way it applies specifically to GRC. Compliance

Mohamed GHAZOUANI, ENSEM (National and High School of Electricity and Mechanics Hassan II), Casablanca, MAROC
Redouane ELALJ, EIGSI, Casablanca, MAROC

in general means that you are satisfying a set of conditions that has been set forth for you. Compliance implies that someone else has set those conditions up and that you must meet them. That's exactly what's going on in GRC. Most of the time, when people talk about compliance, they are referring to external standards for which compliance is mandatory. The word compliance also sometimes refers to internal standards as well.

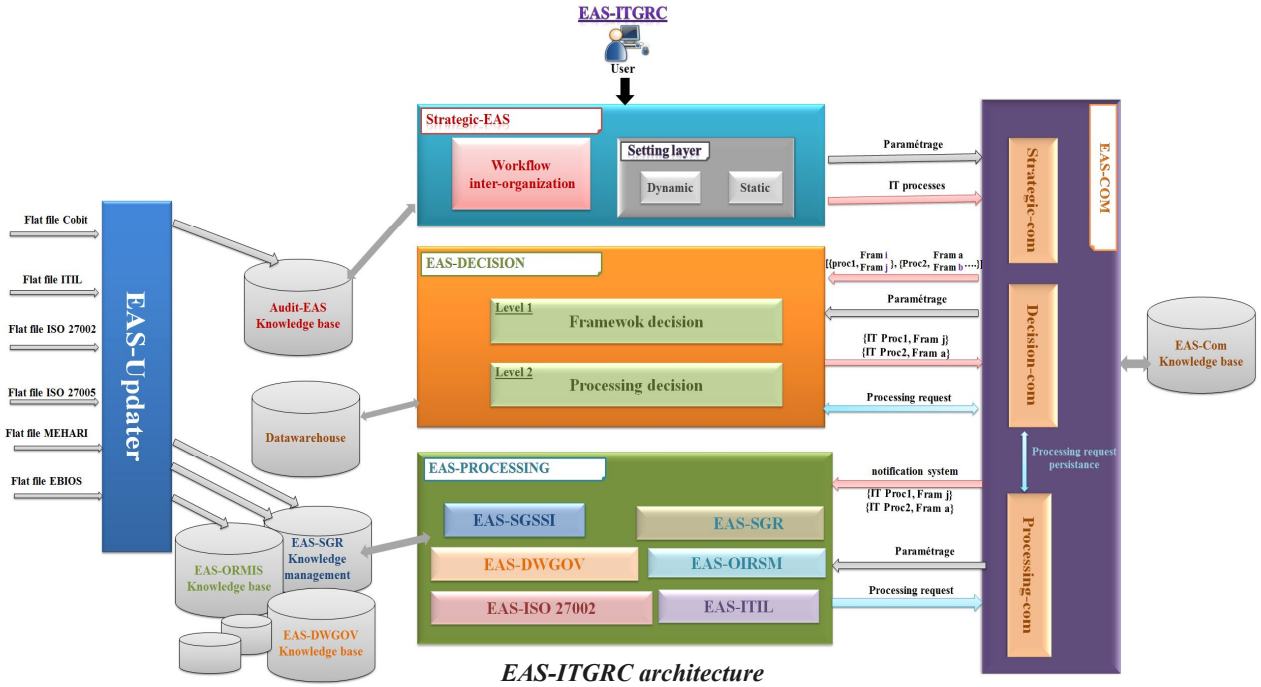
Defining the C in GRC as standing for controls can broaden the discussion. Compliance is what we have to do, and controls are the way we do it. Furthermore, controls are a way to monitor that the business is compliant, and also efficient and orderly in every way. [2]

V. PROPOSED SOLUTION

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



EAS-ITGRC architecture

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 platform is based on the standards and methods of Governance, Risk and Compliance Information Systems (IT GRC), the most common (COBIT, ITIL, PMBOK, ISO27001, ISO27002, ISO27005, Mehari, EBIOS) The proposed solution using a massive undertaking, activity and Information System (SI) any, to manage its IT processes in line with its business strategy involving business managers with management information system. It can optimize IT investments by monitoring business strategies in order to create more value, making them more efficient IT processes and control risk and compliance related to SI. It deploys a variety of good practices of IT Governance and made a smart choice by the constraints and corporate settings best framework to evaluate the objectives and processes in question.

A. COBIT

COBIT (Control Objectives for Information Business year related Technology) is a methodology for evaluating IT services within the company. [3] 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. "

B. ITIL

ITIL [4] 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.

C. 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 [5]. 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.

D. MEHARI

MEHARI is a risk analysis and management method developed by CLUSIF and supported by software managed by the company Risicare [1] (http://www.ysosecure.com). 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 [6].

E. EBIOS

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité - Expression of Needs and Identification of Security Objectives) is a method for analysis, evaluation and action on risks relating to information systems. It generates a security policy adapted to the needs of an organization. The method was created in 1995 and is now maintained by the ANSSI, a department of the French Ministry of Defense.

The five steps of the EBIOS method are:

- Circumstantial study - determining the context;
- Security requirements;
- Risk study;
- Identification of security goals; and
- Determination of security requirements.

F. PMBOK

The PMBOK® Guide defines a process as “a set of interrelated actions and activities performed to create a pre-specified product, service or result.” It goes on to say that “project management processes ensure the effective flow of the project throughout its life cycle.” Processes get things done.

Each process has pre-requisites (known as inputs), tools and techniques you can use to actually do the process, and then outputs: one of more things that you get as a result of having done the process. The achievement of those things lets you know the process is over (at least until the next time you need to use it) [7].

VI. MULTI AGENT SYSTEMS

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].

A. Agent

Agents are software entities that have a very specific task and that decide for themselves what they have 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.

[1] http://www.ysosecure.com, accessed December 2016

- 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.

B. 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:

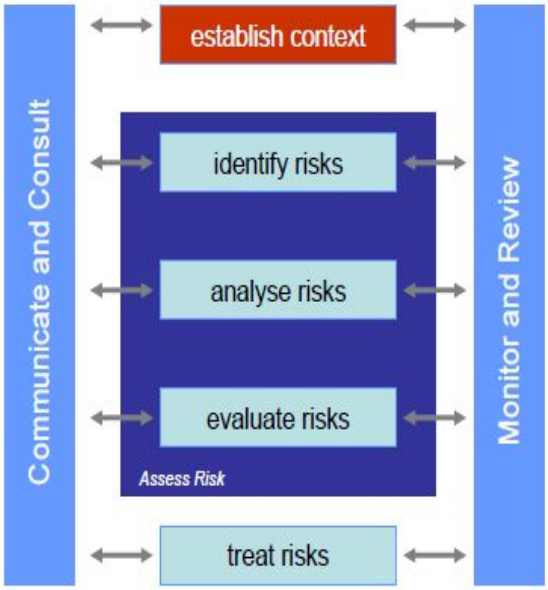
- Pro-activeness. [10] Intelligent agents are able to exhibit goal-directed behavior by taking the initiative in order to satisfy their design objectives.
- Reactivity. Agents are crucial when operating in an unpredictable environment containing a large number of data sources scattered over multiples 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.

VII. EAS-SGRSSI

Each member of the Systems Architecture Team (EAS) works on a subsystem individually and EAS-SGR (Security Risk Management System) is one of these subsystems.

IT risk management needs to be an ongoing activity, not a one-off exercise. It begins with a framework, and this is the one that works for us.

The steps in the figure 2 describe the core activities within our subsystem. The figure shows structured steps, but in practice the steps are highly fluid and have fuzzy boundaries. Large amount of feedback and interaction often occur between the steps.



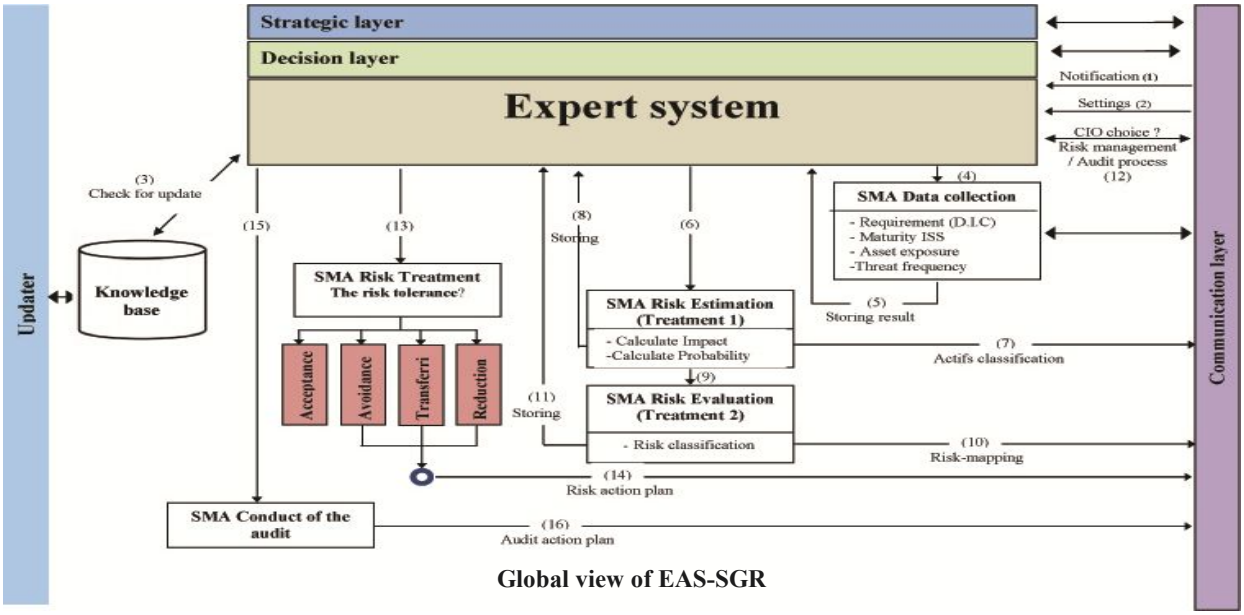
í ⋇ ɱ *Risk* management process steps

- Establish the context – establish the external, internal, and risk management context in which the rest of the process will take place. Criteria against which risk will be assessed should be established and the structure of the analysis defined [11].
- Identify risks – identify where, when, why, and how events could prevent, degrade, delay, or enhance the achievement of organisational objectives
- Analyze risks – identify and evaluate existing controls. Determine consequences and likelihood and hence the level of risk. This analysis should consider the range of potential consequences and how these could occur
- Evaluate risks – compare estimated level of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities
- Treat risks – develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs
- Monitor and review – monitor the effectiveness of all steps of the risk management process. This is important for continuous improvement. Risks and the effectiveness of controls and risk treatments need to be monitored to ensure changing circumstances do not alter priorities.
- Communicate and consult – communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole [11].

VIII. PROPOSED ARCHITECTURE

Figure 3 graphically illustrates the global view of the EAS-SGR Tool. This section discusses its components.

The system is totally interactive and based on multi agent system which is composed of the following component: Expert system, Data Collection agent, Estimation agent, Evaluation agent, Treatment agent and Audit agent.



Global view of EAS-SGR

Expert system is in charge of creating Goal-directed behavior to solve the problems it receives from communication layer. It handles all communication with the manager and communicates with the Collect agent, Estimation agent, Assessment agent, Treatment agent and Audit agent in order to manage the planning and execution.

Collect agent is in charge of sending audit questionnaires and survey to users or collaborators and ensure respect duration, retransmit, make a first consolidation and detect anomalies in respondents' answers. 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 8.

Estimation agent handles the execution of the impact and the probability calculation.

Assessment agent has the role of classifying the risk based on the ISO 27005 risk assessment matrix.

An agent 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.

Treatment agent is in charge of, according to the user choice, risk treatment. It suggests administrative controls, technical or physical to be applied within the information system and propose solutions that were applied to similar problems by consulting knowledge base or communicate with the historian agent.

Audit agent includes a detailed questionnaire assessing multiple areas of the organization. When finished, EAS-SGR Tool generates a comprehensive report which can be used to get an overall view of the organization's security situation and identify specific areas of the organization where security is at a mature and strong level. The manager can import his own questionnaire.

CONCLUSION

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. This research document could form the basis for a technical project to develop an actual web-based Information Security Risk Management Tool to achieve these objectives. In the future, this project could then also include others standards to assist organizations in exactly on 'what' must be done.

REFERENCES

[1] Ken E. Sigler, James L. Rainey III "Securing an IT Organization through Governance, Risk Management, and Audit" , ISBN-13: 978-1498737319, 2016.
[2] Denise Vu Broady, Holly A. Roland , "SAP GRC For Dummies, ISBN: 978-0-470-33317-4, 2008.
[3] s.elhasnaoui, a.chakir, m.chergui, h.iguer, s.faris and h.medromi, "Communication system architecture based on sharing information within an SMA", 2015.
[4] 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.
[5] S.Elhasnaoui, H. Medromi, S. FARIS, H.IGUER, A. Sayouti —Designing a Multi Agent System Architecture for IT Governance Platform‖ International Journal of Advanced Computer Science and Applications IJACSA Volume 5 Issue 5 May 2014.
[6] TALABIS, Mark et MARTIN, Jason. Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis. Newnes, 2012.
[7] OSP International LLC, 2015, [Online]. Available: www.project-management-prepcast.com.
[8] RUSSELL, Stuart J. et NORVIG, Peter. Artificial intelligence: a modern approach. 2009.
[9] WOOLDRIDGE, Michael et JENNINGS, Nicholas R. Intelligent agents: Theory and practice. The knowledge engineering review, 1995, vol. 10, no 02, p. 115-152.
[10] BURKEY, Roxanne and BREAKFIELD, Charles V. (ed.). Designing a Total Data Solution: Technology, Implementation, and Deployment. CRC Press, 2000.
[11] Joost J.L.M. Bierens, "Drowning: Prevention, Rescue, Treatment",2014.

Mohamed GHAZOUANI is an engineer at the Ministry of Finance. In 2009 he had a master's degree in software engineering at the University of Quebec in Montreal. In 2011 he is enrolled on the Phd in the ENSEM - University Hassan II Ain Chock - Casablanca. His area of research focuses on the information systems governance based on Multi-agent systems.

Redouane ELALJ is a professor of computer science at EIGSI, engineering school.