Regulations, Frames of Reference, Information Systems Security and it Governance

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

Bouchaib Marah
TIC Team, LSI,
ESTEM Research Center
Casablanca, Morocco

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

Adil Sayouti
TIC Team, LSI,
ESTEM Research Center
Casablanca, Morocco

ABSTRACT

By virtue of the multiplicity and diversity of laws regulating the field of information technology governance, those in charge of information systems in SMEs-SMIs are faced with a problematic of compliance obligation, especially that the laws are now of international and national order.

This work is concerned with information systems security and the crucial role it plays to ensure an effective governance of information technology (IT). An essential component of internal control imposed by financial security laws as well as by major IT governance frameworks, the security of information systems is one main leverage for a policy of compliance and standardization. Indeed, compliance with laws and regulations with the aim of enhancing the transparency and credibility of the mechanisms of information production and operation needs the implementation of a set of procedures and controls that meet safety requirements in terms of availability, integrity and confidentiality. These procedures introduce major changes with regard, in particular, to information visibility within the business, organizational and management processes, and human resources management.

Keywords

Information systems security, governance, IT governance, compliance, reference frameworks.

1. INTRODUCTION

Governance refers to the set of measures, rules, decision-making bodies, information and surveillance systems that ensure proper operation and control of a state, institution or organization, be it public or private, regional, national or international. One speaks of "good governance" in the highest political circles as a national necessity aiming at efficiency for an effective management of the state.

Originally, the concept of governance was first developed in the reports issued by such national organizations as the United Nations, and particularly its development program agency UNDP. This program is the global UN development network promoting change and connecting countries to knowledge, experience and information resources to help their people improve their living conditions.

In addressing such an issue, this paper offers to follow these steps: after a brief introduction, the second section defines the concept of IT governance. In the third, we present a state of the art of the different standards and regulations that exist in the market. In the fourth section, we attend to three ways to ensure effective security of the information system, namely the definition of a clear and concise security policy, the implementation of new organizational and control procedures and the allocation of licenses to various stakeholders of the system. The final section concludes the paper.

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.

An essential component of corporate governance, IT governance represents the set of audit and control processes that guarantee the integrity, completeness and traceability of information; the aim is to reduce operational risks arising from the use of IT (Georgel, 2006) [1]. IT governance also describes the selection and use of organizational processes destined to making decisions efficiently and effectively with respect to the acquisition and deployment of IT resources and competencies (Luftman et al., 2004) [2]. It thus determines how IT-related strategic decisions are made, responsibilities are assigned to those tasked with the implementation of these decisions and how the results of these decisions are measured and controlled through assessment and monitoring mechanisms (Peterson, 2004; Weill, 2004; Symons, 2005) [3]. These decisions concern the strategic areas of IT governance as defined by the IT Governance Institute (ISACA subsidiary), namely strategic alignment, risk management, resource management, measuring performance and delivered value.

However, far from its theoretical and advantageous formal framework, the implementation of effective IT governance is constrained by several factors that may be related to the centralization of decision-making and investment productivity (Kavanagh and Suppert, 2007) [4]. Effective IT governance requires real, significant organizational change in the practices and procedures (Rau, 2004) [5], and calls accordingly, while it takes some time to implement, for support structures as well as for communication mechanisms and effective coordination (Kavanagh and Suppert, 2007) [4].

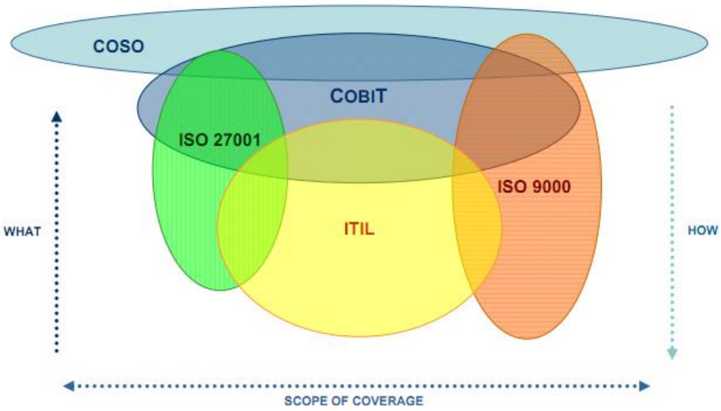

Fig 1: Governances Referential

3. STATE OF THE ART: REGULATIONS AND PRINCIPAL FRAMES REFERENCE OF IT GOVERNANCE

3.1 Regulations

Financial scandals and fraudulent behavior of some companies have induced public authorities, shareholders and potential investors to consider IT governance a crucial activity of information systems governance. Thus, a regulatory framework is required to control and monitor the flow of information within the company, namely the financial aspects of the information system.

In this regard, the Sarbanes Oxley Act, passed by the US Congress in July 2002 as a reaction against the numerous accounting and financial scandals (e.g. Enron, Tyco International, WorldCom), is meant to severely regulate the production of accounting and financial documents, and to enhance financial transparency and the confidence of real and potential investors in the markets. Indeed, this law targets directly fraud factors in an attempt to strengthen supervision of the administrative and audit committees, increase alertness and auditors' independence, reinforce internal control and risk management, and create sufficiently dissuasive penalties to deter accounting fraud.

Articles 302 and 404 are particularly directly related to IT governance. On a practical level, the official report, released over many consecutive years in the United States by the Computer Security Institute, mentions a lack of enthusiasm on the part of the companies surveyed regarding the impact of the Sarbanes Oxley Act on improving safety and information systems governance.

In France, the Financial Security Act of 2003 is aimed primarily at consolidating auditors' independence and strengthening corporate governance, while ensuring better security for savers and insurees through structural reforms and modern financial instruments. The point is to guarantee the reliability and transparency of the information disclosed to shareholders by way of a proper risk assessment.

In June 2004, the Basel Committee at the Bank for International Settlements adopted a new capital adequacy framework in Basel, Switzerland. The Basel II prudential standards provide a means for a better understanding of the banking risks, and mostly credit risk—in particular equity requirements. It provides a more comprehensive coverage of banking risks and encourages institutions to improve their internal risk management. They propose notably the establishment of the McDonough ratio, which limits the amount of loans granted in proportion to the level of equity and loan risk. These standards have followed from the standards issued by Basel I agreements, whose Cooke ratio did not take finely into account the risk.

In Tunisia, the promulgation of the law in October 2005 on strengthening the security of financial relations accorded greater responsibility to financial auditors to ensure that control procedures are implemented in the Tunisian financial market.

In Morocco, the long expected 08-09 law on the protection of personal data has just seen the light of day along with its implementation decree— one first step of reform taken by Morocco towards openness and modernization. However, the road is still long for its popularization in the different socio-economic spheres of the country. The 31-08 Act on consumer protection remains at the core of the debate.

3.2 Key IT Governance Frameworks

Compliance with laws and regulations regarding the safety of financial information requires the use of a recognized framework for internal control assessment and risk management. The best-known reference frameworks are:

COBIT (Control Practices), which incorporates the five strategic areas of IT governance, and provides managers and IT auditors with a control and security framework. This is based on a set of processes and performance indicators aimed at improving the quality of information in terms of effectiveness, efficiency, confidentiality, availability and integrity. It thus offers the means of control and decision support in order to maximize the expected benefits of the use of IT, favoring thereby the company's strategic choices.

COBIT is process-oriented. It defines IT activities in a generic process model that can be divided into four areas. These are "Plan and Organize", "Acquire and Implement", "Deliver and Support", "Monitor and Evaluate".

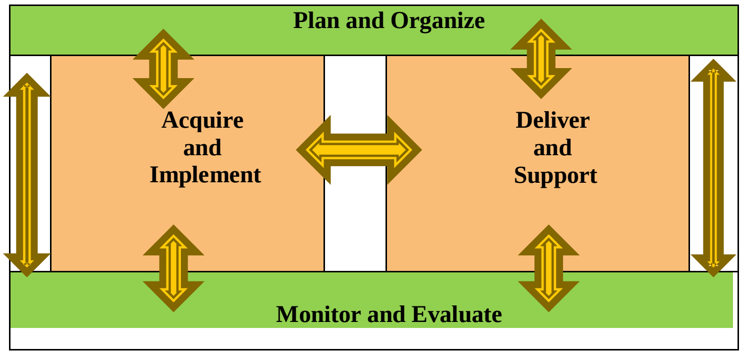

Fig 2: COBIT Process

ITIL (Information Technology Infrastructure Library) brings together a collection of good practices and recommendations for the effective and secure organization of an information system through infrastructure management and IT services. This reference frame has a double technical and managerial perspective. The COSO framework is to assess and manage business risk in order to preserve and create value for all stakeholders through general computer controls and application controls required for the efficiency and security of the information system.

As part of ITIL, service quality is based on a structuring of activities into interdependent, measurable and repeatable processes.

A large number of companies today recognize this process-based management approach of activities as most effective. ITIL has adopted this solution by cutting IT-service management into processes:

The first of these is the inclusion of customer expectations in the implementation of IT services that English speakers call the Customer Focus.

The second principle is the life cycle of IT projects, which need to integrate from the outset different aspects of IT service management.

The third founding concept recommends setting up interdependent ITIL processes to ensure the quality of services.

The fourth and last principle is the implementation of a quality approach for services installed together with a quality measurement set from the users’ perspective.

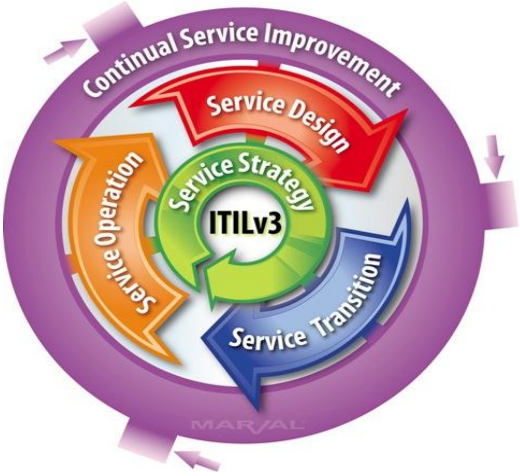

Fig 3: ITIL Processes

Accordingly, compliance with regulations and standards can be integrated as part of an organizational change through the implementation of effective and efficient controls whereby new requirements at the organizational, managerial and human levels are imposed. In addition, the security management of the information system lies at the center of an active IT governance.

4. SI SAFETY: AN ESSENTIAL COMPONENT OF SI GOVERNANCE

The information systems security of a company has become a vital element for the development and sustainability of its business alongside the notable changes occurring in its economic and technological context, particularly the strong evolution of computing, the Internet and their uses. The need to provide correct, reliable and up-to-date information locates information systems security at the center of executives’ and IT managers’ concerns (Damianides, 2005) [6] as an essential component of governance (Hawkins, and al. 2003) [7] and compliance (Brown and Nasuti, 2005). [8]

Indeed, security involves the protection of information resources (including personal information and financial users, research projects, virtual prototypes of products, .. etc.) of the company; it rests mainly on three elements, namely confidential ity, integrity, and availability (Canavan, 2001; Vermeulen and Solms, 2002) [9]

While confidentiality must ensure access to resources for authorized persons,the integrity of information concerns the authenticity of data that can be changed only by authorized persons. Availability is the concept that guarantees access to information when the user needs it.

Thus, to meet the increased requirements of integrity and transparency, the security of the information systems appears to be an essential component in the process of compliance through the definition of a security policy, the implementation of new organizational and control procedures, and the delineation of authority and responsibility of the different stakeholders in the management of information systems.

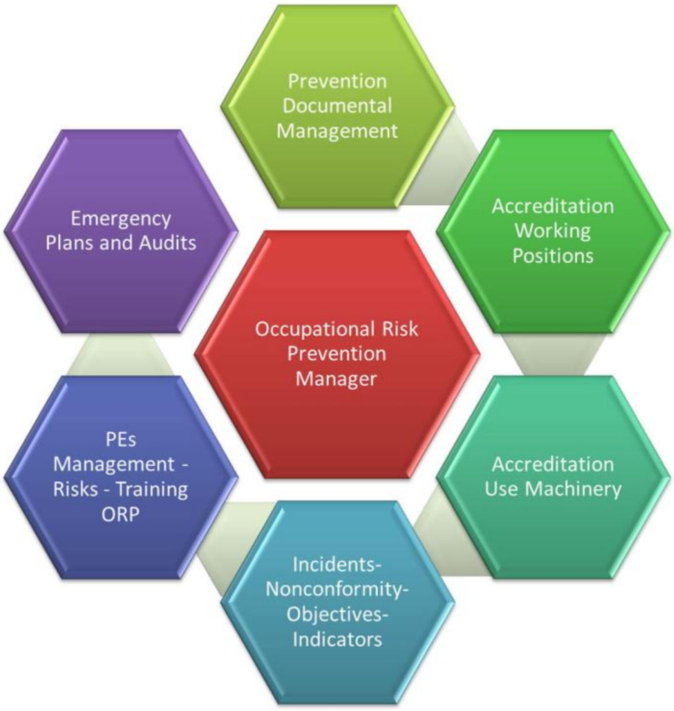
Prevention Documental Management
Accreditation Working Positions
Emergency Plans and Audits
Occupational Risk Prevention Manager
PEs Management - Risks - Training ORP
Accreditation Use Machinery
Incidents-Nonconformity-Objectives-Indicators

Fig 4: Risk Prevention Manager

4.1 Visibility of Information and Security Policy

The ISO 17799 standard stipulates that security policy is a formal document that provides rules and guidelines to manage and support information security. Defining a security policy aims primarily to outline the business requirements for information visibility based on its sensitivity and confidentiality.

It aims to develop security strategies to protect the most critical information and to set the security controls framework (Llorens and Lever 2003) [10]. It includes documents and guides describing formally principles or rules that the people entitled to access the company’s information system have to abide by. It is also described in a number of operational and technical procedures, concisely explaining the steps to follow in order to achieve a specific security objective. Security policy takes into account the size of the company, its nature and its business needs and the degree of openness of the corporate network and the organization of its services. It also takes into account changes in business strategy as well as the technological choices made for its implementation.

Companies introduce security policies to minimize the risk to an acceptable level by using security solutions tailored to their needs and in proportion to the characteristics of their services.

Implementation involves the use of methods and techniques to perform a risk analysis in order to assess investment opportunity in terms of the importance of the information to protect and depending on the probability of occurrence of an assault, while focusing on reducing risk and optimizing costs. Thus, the company determines the level of risk it is willing to accept on its resources compared to the cost induced by the threats it incurs (Brenton and Hunt [11], 2003; Llorens and Lever, 2003 [10]). Furthermore, security policy rests on three pillars: prevention, detection and response (Canavan, 2001) [9]. Prevention consists in implementing the necessary and sufficiently dissuasive measures to limit the exploitation of vulnerabilities in the corporate network. Detection involves laying down a set of procedures to identify potential problems. The quicker the detection, the easier the correction and the response. The response is developed within an appropriate plan that specifies the actions to undertake and responsibilities. A security policy should cover elements relating to: (i) infrastructure security (the logical and physical security of the equipment and network connections, both internal and external such as those provided by network providers; (ii) access security (the logical security of local and remote access to corporate resources, managing users and their access rights to the company's information system); and (iii) Intranet security in the face of Internet or third parties (logical security of access to corporate resources by Extranet and access to external resources via Internet). Hence, the development of a security policy appears to be a necessary step for the implementation of the rules of a good governance of the information system. Yet it is far from being a routine or easy exercise to perform. The official report published by the CLUSIF (French Club of Information Systems Security) for the year 2008 indicates an average rate of companies that have made a formalization of their security policy with a slight decline of 6% compared to 2006 with respect to large companies.

4.2 New Organizational Procedures and Management

The new procedures arising from security policy are necessary for its implementation because they set the conditions of exploitation and production of information in the company's value chain. These often involve a redefinition of internal organization and management procedures in order to allow for a better identification of production operations and sales transactions, keeping thereby a record of both internal and external actions, determining the types of control, and implementing effective coordination and communication mechanisms for an active management of information flows within the company. In this regard, a documentation of the various processes of information production (Davenport and Beers, 1995) [12] help the company to improve its quality in terms of relevance and authenticity. However, the dynamic nature of security policy in terms of changes in business strategy, namely IT deployment, requires constant updating of various procedures and rules of operation. Similarly, the increasing complexity of digital attacks (internal and external) requires a change of rules and security mechanisms intended as part of security policy.

4.3 Allocation of Responsibilities and Authority

The classification of information according to their strategic or operational importance implies a classification of users of the information system through a definition of access rights, traceability of evidence and archiving of the traces of the actions performed at the level of each process within the business. Indeed, a good IT governance implies a clear definition of responsibilities and authority in terms of the different categories of employees involved in carrying out the strategic objectives. In this regard, Rau (2004) [5] proposes a governance organization model at several levels in which he describes the role and responsibility of each entity and the relationships between them.

Users can be classified into at least three categories: authorized users, users with partial access, and users with public access. This is likely to establish, at several management levels, a model of the trust to be assigned to different users of the information system, taking into account the company's security objectives. Indeed, attacks by internal employees who have important knowledge of controls and processes within the company are the most dangerous to the security of information systems. The ITUC report of 2008 indicates that abuse of access into the internal network constitutes the second attack after the viruses registered by the companies interviewed.

Furthermore, negligence, errors of design or in programming, and the handling of technicians or managers can cause serious, unexpected damage. It should, therefore, be necessary to enhance employee awareness of the security issues through training and education programs while increasing their understanding of the new procedures in place.

4.4 Architecture

We propose in this paragraph our global architecture that regroup multi-agents laws in the GRC governance platform.this architecture has been created in order to resolve the problematic related to laws diversities

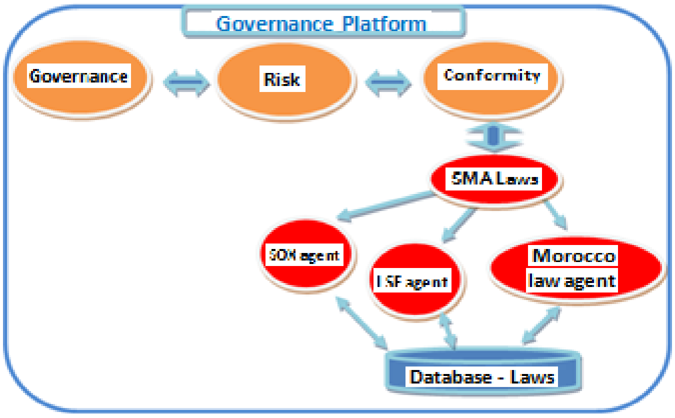

Fig 5: general architecture proposed of SMA laws

5. CONCLUSION

This research has sought to address corporate information systems security by focusing on the key role it plays to ensure the reliability and integrity of information as part of an effective IT governance. Our interest has particularly been in the impact of the constraints of regulation and standardization on the information systems management. We have aimed to show that information security constitutes one main leverage within a compliance process, allowing for better use and traceability of information in general and not only financial information.

However, further studies might demonstrate that the specificity of a company's field of activity greatly influences the measures implemented in order to set the rules of good governance of the information system, and therefore the procedures of compliance with the security laws of financial information.

A subsequent case study of a trading bank, for instance, may show certain specificities of the banking practice and that these laws remain too vague and broad to apply properly to this sector.

Given the exploratory nature of this work, it would be appropriate to consider studying several contexts in the hope of proposing an explanatory frame of reference for process integration of the standards and regulations proper to the banking sector.

6. REFERENCES

[1] Georgel F. (2006) IT Governance: Strategic management of an information system, Dunod, p. 290.

[2] J. Luftman, Bullen C., D. Liao, Nash E. and C. Neumann (2004) Managing the information technology resource, Upper Saddle River, NJ: Pearson Prentice Hall R. Peterson (2004)

[3] R. Peterson (2004), "Crafting information technology governance", Information Systems Management, 21, 4, pp. 7-22

[4] S. C. Kavanagh and Suppert M. (2007) "We're all together in IT: Aligning Technology with Business through IT Governance", Government Finance Review, 23, 3, pp. 24-

[5] K. Rau G. (2004) "Effective governance of IT: design, objective, roles, and relationships", Information Systems Management, 21, 4, pp. 35-42

[6] Damianides M. (2005) "Sarbanes-Oxley and IT Governance: New Guidance on IT control and compliance" Information Systems Management, Winter, 22, 1, pp. 77- 85

[7] K. W. Hawkins, Alhajjaj S. and S. Kelley S. (2003) "Using CobiT to secure information assets" The Journal of Government Financial Management Summer, 52, 2, pp. 22-32

[8] Brown and W. Nasuti F. (2005) "are Sarban-Oxley and enterprise security: IT governance and what it takes to get the job done," EDPACS, 33, 2, pp. 1- 20

[9] J. Canavan E. (2001) "Fundamentals of Network Security", 319 pages, Boston, London: Artech House

[10] C. Llorens, Lever L., (2003), Network Security Dashboard,

[11] C. Brenton, Hunt C., (2003), Network Security, SYBEX, 490P

[12] T. H. Davenport and Beers, Mr. C. (1995) "Managing information about processes" Journal of Management Information Systems, 12 (1)

[13] COBIT® Control Practices., (2007): Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition.