Revue du Contrôle de la Comptabilité et de l'Audit
ISSN: 2550-469X
Numéro 4 : Mars 2018

A new approach to the governance and security of public administration information systems in Morocco

Une nouvelle approche de la gouvernance et de la sécurité des systèmes d'information de l'administration publique au Maroc

Houssain KOUNAIDI
FSE UM5 Rabat

Abdellatif RYAHI
FSE UM5 Rabat

Mariem CHERKAOUI
FSE UM5 rabat

Mohamed GUEDIRA
Enseignant chercheur FSE UM5 Rabat

Abstract

Following the acceleration of the development of digital transformation worldwide, we are now witnessing the rise of vulnerabilities in information systems in several countries. Hence the importance for organizations to adopt new organizational and technological strategies, in order to optimize the risks weighing on information processed in the information systems. As a result, the consideration of risk at the organizational level is the subject of much scientific research.

The purpose of this article, is to draw up an inventory of the approach recommended to secure the information assets of public administrations in Morocco based on the analysis of security risks, by taking a practical case study "a large public administration in Morocco "whose name will not be exposed for reasons of security and confidentiality, and also propose recommendations for a successful program of security (IS) effective.

Keywords: Governance, practices, information system Security, information system, public administration, regulatory legislation.

Résumé:

Suite aux accélérations du au développement de la transformation digitale au niveau mondial, on assiste aujourd'hui à la montée en puissance des vulnérabilités des systèmes d'information dans plusieurs pays. D'où l'importance pour les organisations d'adopter de nouvelles stratégies organisationnelles et technologiques, afin d'optimiser les risques pesant sur l'information traitée au niveau des systèmes d'information. Par conséquent, la prise en compte du risque au niveau des organisations fait l'objet de nombreuses recherches scientifiques.

Cet article examine la relation entre les difficultés de la gouvernance des systèmes d'information (SI) au sein des administrations publiques au Maroc, à travers le volet sécurité, et le niveau de maturité des systèmes d'information mis en jeu.

Mots-clés : Gouvernance, pratiques, sécurité des systèmes d'information, système d'information, administration publique, législation règlementaire

Introduction :

It is increasingly recognized that (IS) now contains the strategic, technical, business, administrative and financial data of any organization. By the same token, these (SI) are an essential vulnerability, facing threats that can be varied and destructive. Thus, the security of (IS) is an area that is growing in size. It is certainly complex where the technique and the human factor are closely linked.

Several reference varieties are also published by international standards, the purpose of which is to guide organizations in setting up an IT risk management process to identify protective measures adapted to the company's situation and values. , while protecting the most important IT assets.

Based on a global vision and an analysis of the current situation in the field of security of (IS), we have noticed that the security of (IS) in the public administration cannot meet the challenges posed by the unlimited evolution that knows the domain cyber security. And, therefore, the non-satisfaction of the needs of the information systems directorates (ISDs) and the business divisions.

In view of this, the Moroccan government's guidelines for protection of (IS) at the national level in 2011 led to the emergence of the role of the Directorate-General for Information Systems Security (DGSSI) and the National Center for the Protection of Personal Data (CNDP). These are at the heart of the organization and security of (IS) in the public and private sectors.

We have judged that the sensitization of the leaders and the implementation of the security policies of the (IS) through the audit of the security of the (IS) is the solution best adapted to begin to answer these needs, And also will increase our visibility, will accelerate our intervention and reduce our security costs.

It is highly recognized that (SI) now contains the strategic, technical, business, administrative and financial data of any organization. By the same token, these are an essential vulnerability, facing threats that can be varied and destructive. Thus, the security of (IS) is an area that is growing in size. It is certainly complex where the technique and the human factor are closely linked.

Based on a global vision and an analysis of the current situation in the field of security of (IS), we have noticed that the security of (IS) in the public administration cannot meet the challenges posed by the unlimited evolution that knows the domain ducyber security. And consequently, the non-satisfaction of the needs of the information systems directorates (ISD)

and the business directions.In this context, we conducted case studies in the form of a survey barometer on the level of maturity of governance and the security of public administrations in Morocco.A first study is carried out on the average level of maturity of Moroccan organizations compared to ISO27002 and a second study is made on the evolution of trends in the use of (IS) at the level of public administrations and private and finally, an assessment on the security level of (IS) of a public body in Morocco whose name will not be exposed for reasons of security and confidentiality.

Indeed, the safety and security of information are two primary elements for the proper functioning of any organization regardless of its size or complexity. It is in this sense that it is increasingly recommended to engage in a reflection on the safety culture in public administrations in Morocco, involving all actors, from management to the basic user. For that, the audit of the security as well as the identification and the evaluation of the risks are processes which allow all the public administrations to initiate a global approach of the security and the circulation of the information.

This evolution has therefore filled the needs of many users who are not necessarily in good faith. They can exploit the vulnerabilities of networks and systems in order to access confidential information and use it in their own interests. As a result, these networks have become targeted by such threats and their security is becoming increasingly important. The establishment of a security policy around these systems is therefore decisive.

Ensuring the security of the (SI) public administration (PA) is one of the priorities of the organization's information systems department (ISD).

Referring to the international standard ISO 27002, the audit of security consists in doing, in some ways, an inventory of the audited organization, while being based on the different domains (the eleven chapters) recommended in the standard. This analysis will make it possible to identify the areas to be secured, to identify in a fairly precise manner, on the one hand the vulnerabilities of each component and on the other hand, the risks that run. As is the impact of these vulnerabilities on the overall functioning of public administrations.

The audit will provide recommendations to minimize the risk of unavailability, or threats to the integrity or confidentiality of the information.

In this context, information security is considered a major issue for all public administrations in Morocco. There is also the difficulty of implementing (IS) governance in public administrations. To update the (SI) security policy, a security audit must be done to verify the

gap between the current situation, on the different organizational and technical levels, and the state of the art.

According to the Directorate-General for Information Systems Security (DGISS) "In the face of these risks and threats and as is happening in advanced countries in the field of information systems security, the Committee Strategic Information Systems Security (CSSSI) established by decree No. 2-11-508 of 21 September 2011 adopted on December 05, 2012 the national strategy of cyber security.

To overcome this problem, we propose a new approach to security governance within the public administration based on the analysis of security risks, taking the organization into question without citing its name for reasons of security confidentiality as a framework.

1. Theoretical framework of the study

1.1Management of security :

Security plays a cross-cutting role for better protection of information assets. Security of (IS) is paramount for making effective decisions for business leaders.According to Khoo, information security is defined as "the protection of the confidentiality, integrity, and availability of information and its critical elements, including software and hardware that use, memorize, process and transmit this information through the application of principles, technologies, training and sensitization ".In another setting, several studies have focused on information security risks (Solms and Von Solms, 2004, ITGI, 2005 Pironti, 2006). The reduction of technological risks is achieved through the implementation of a security framework based on policies, standards and guidelines. Information security is a management activity in the context of corporate governance. which indicates strategic directions for security activities and ensures that objectives are achieved. In addition, it ensures that information security risks are managed appropriately and that corporate information is used responsibly (OGC, 2009). For Gerogel (2005) "security is about tactical and operational plan while risk management is strategically positioned. » IS governance does not negate the importance of IT security, but positions it as an answer to specific, clearly identified risks.

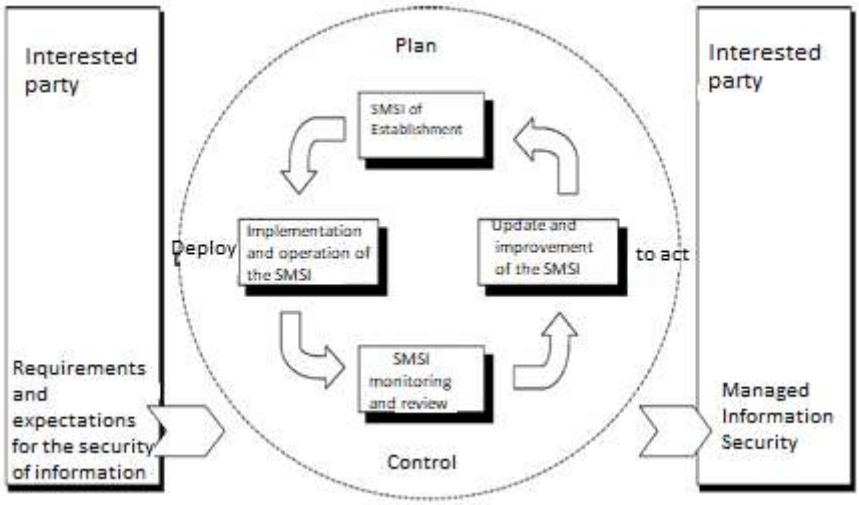
Since 1995, several standards directly or indirectly related to WSIS have been published. For example, BS 7799, BS 7799-2, ISO 17799, ISO 27001 and ISO 27002 were introduced in succession.ISO 27001 has established itself as a reference for WSIS. Based on BSI BS 7799, and adopted in 2005 by ISO as ISO 27001: 2005, it currently specifies the requirements that an organization must meet to set up an ISMS.

Adopting a process approach, the standard highlights the best security practices and especially organizes them over time. This recent standard defines the set of controls to be carried out to ensure the relevance of the WSIS, to exploit it and to make it evolve.

The ISO27001 standard is based on the 11 chapters (ie 133 measurement points of the ISO27002 standard) to ensure the relevance of the safety commitments defined by the management. The continuous improvement approach is the core of the standard. It is articulated around the model Plan, Do, Check, Act (Model PDCA or Deming Wheel).

The adoption of the PDCA model also reflects the principles set out in the OECD Guidelines (2002) governing the security of information systems and networks. This standard provides a robust model for implementing these principles in the guidelines governing risk assessment, design and implementation of security, and the management and reassessment of that same security.

Figure 1: PDCA Model Applied to SMSI Processes



Source: ISO (2007)

ISO 27002 deals with information security according to 11 axes: (see table below)

1. . The securitypolicy,	7. Operationalsafety and networks
2. Organisation security	8.security of developpement
3. Classification of assets	9.Security related to human resources
4. Security incident management	10. Compliance withlaws
5.Physical security and the environment	11. Continuity management
6.Access management	

ISO 27002 stands out as an excellent framework for information security, covering all dimensions: organization, process and technology.

According to ISO 27002, (IS) safety is based on four types of indicators:

- Confidentiality: Is issued the information to authorized persons only
- Integrity: Issued unfalsified information
- Availability: Ensures complete continuity of service
- Traceability: Event Logging, Evidence Research

1.2. Governance and risk management:

In the context of (IS) governance, security plays a very important role in securing the data that exists at the level of government IT centers.

Highlighting a perception of security, often reduced to the IT domain alone, is a lack of a comprehensive corporate strategy. While IT security is necessary, it is still insufficient to deal with risks such as cybercrime.

To address good risk management, the Information Systems Security Directorate has developed a simplified information security risk management process derived from the model proposed in ISO / IEC 27005, and good practices related to information security in Moroccan context.

Beyond the theoretical framework of this research, we conducted an empirical study that looked at a sample of CIOs in the Moroccan public sector, in particular a large public administration. But because of the sensitivity of public data, governments cannot allow full transparency in research.

This is why, on the public-sector side, we have relied on security studies on document analysis and security audits (IS) carried out by public authorities.

As a matter of fact, it is only today that public administrations are accompanied by the DGSSI / maCERT (Vulnerabilities and Threat Detection Center) which deals with the assessment of risks to (SI) administrations, public bodies and infrastructure of vital importance and strengthens the foundations of security: legal framework, awareness, research & development training. In addition, the DGSSI attaches great importance to the promotion and development of national and international cooperation, all of which is included in a national strategy for security of (IS) in Morocco.

The ultimate goal is to see the level of maturity of security and IS governance in, especially that in a large public administration Morocco.

2. Methodological approach :

In the context of (IS) governance, it is necessary to integrate a global approach to security, which proposes to give a complete vision of the level of security of the organization, to highlight deviations from objectives, identify IS risks, identify corrective actions to be taken and help to assign the right priorities to different projects.

This global approach must also ensure prerogatives, namely the transparency of information, the accessibility of information, the reliability of information and data, the security of information and data and the traceability of information.

The governance of information security is clearly proactive in the sense that it is a desire to protect the heritage of all the information assets of the organization, this of course requires the establishment of security standards (standards ISO 27001, ISO 22301, COBIT, ITIL, etc.).

Information security governance is a cross-cutting process that ensures the security of the organization's information systems, which defines a program, activities, and organizational security objectives.

- **IS Security audit approach:**

According to the DGSSI "The audit of information systems security is an evaluation to ensure the effectiveness of the security measures in place, to adopt the adoption of adequate protection solutions and to reduce the risks that could compromise security of the IS. It is therefore imperative that administrations and public bodies update their information system by carrying out IS security audits.

These are therefore evaluations, investigations, audits or controls, grouped under the term audit due to regulatory or normative requirements. Indeed, these requirements stipulate that these operations correspond to written procedures with identified officials, which explains the appearance of this term in French.

The audit is perceived as a continuous improvement tool, because it allows to take stock of the existing in order to identify the weak points or non-compliant (according to auditing standards). This observation, which is necessarily formalized in the form of a written report, makes it possible to take the necessary actions to correct discrepancies and dysfunctions.

The security audit of (IS) goes through seven mandatory phases in order of priority that assess the compliance of the organization against an international standard ISO 27002, see below these phases:

- Project framing
- Audit and risk identification

- Audit of risk applications
- Development of the IS security policy
- Development of procedures related to IS security
- Development of an IS security guide.
- Development of the SI security dashboard.

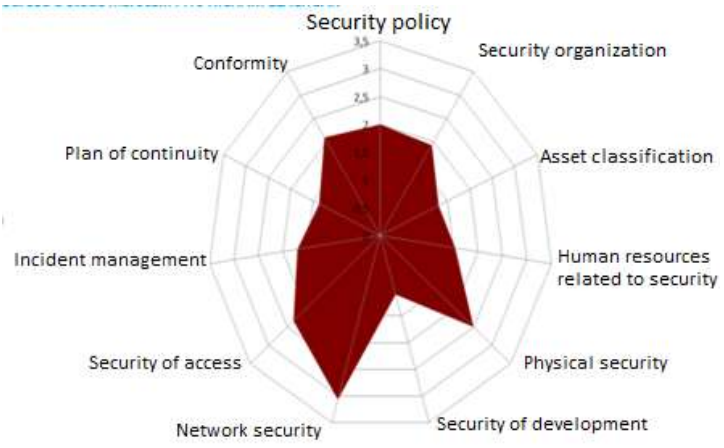
The ISO 27002 standard provides a good governance and management framework for the information system. Indeed, it addresses the issue of security with a balanced approach between technical, managerial, human and procedural factors.

3. Study results: Levels of maturity of the Public Administration Information Systems in Morocco

3.1 Results of the study 1 :

The studies that were made by a Moroccan research firm of a barometer of the Security of (IS) in Morocco edition 2014 composed of a sample of 30 public and private organizations showed the level of average maturity of Moroccan organizations compared to ISO 27002. See the figure below:

Figure 2: the results of the study on maturity levels of IS security in Morocco



Source: 4th edition of Med-IT 2012, Xcom and Infomineo, in partnership with APEBI

The final conclusion of this study indicates that the average score is 7.61 / 20, the lowest score is **= 4.36 / 20** and the highest score is **15.27 / 20.**

This explains why public administrations are not at the same level of security of their information systems and yet it is necessary to make the top management aware of the major risk that may impact their information systems.

3.2 Results of the study2 2

According to a study "1stBarometer of the SI Function in Morocco Edition 2012" which aims to establish a repository allowing a continuous analysis of the evolution of trends in use in (IS) at the level of public and private institutions.

The objectives of this study include:

• Make an inventory of the integration of information systems in the Moroccan company;

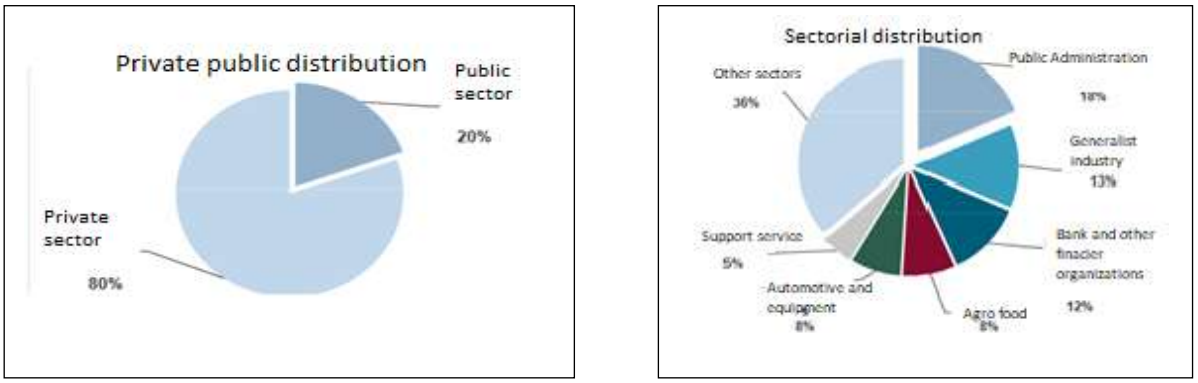
• Identify the challenges and priorities of the Directors of Information Systems;

• To measure the adequacy between the needs of companies in information systems and the solutions proposed on the market.

The sample consists of 102 directors (Public-Private Distribution) and Moroccan IT managers, both online and by telephone interview.

The public sector accounts for 20% in this study, the rest is private. See the figure below:

Figure 3: 1st Barometer of the IS Function in Morocco Edition 2012



Source: 4th edition of Med-IT 2012, Xcom and Infomineo, in partnership with APEBI

As a synthesis we based ourselves on the security part IS by drawing the results of the study:

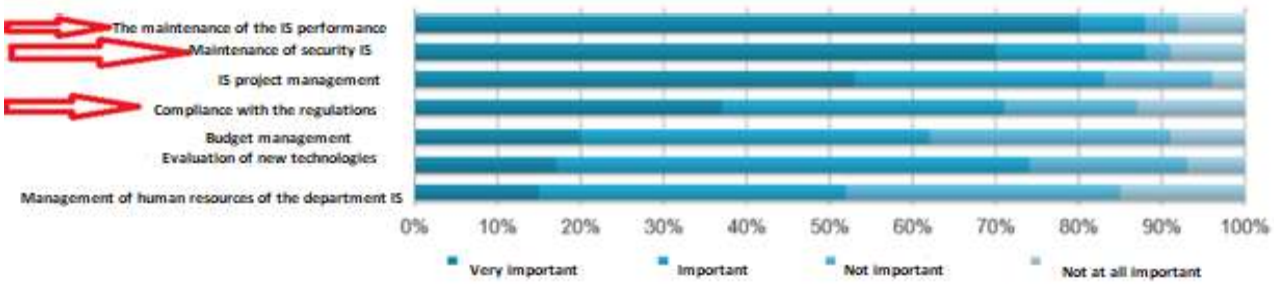
• On the basis of the analysis of the information technology (IT) workforce ratio of the overall workforce of the company, on average one Moroccan woman dedicates one (1) IT resource for 65 employees

• Maintaining the performance of the information system and its security remain the main challenges for Moroccan CIOs (88% of CIOs).

• In fact, for 80% of them, security is considered as the ultimate investment priority for Morocco.

We also note that following these descriptive statistics of the organization of (CIO) in Morocco, a high importance is given to the security part of the information systems.
(See screenshot taken from Barometer Study Report - Figure 7).

Figure 4: the results of the 1st CIO Barometer in Morocco.



Source: 4th edition of Med-IT 2012, Xcom and Infomineo, in partnership with APEBI

In conclusion, maintaining the performance of the information system as well as its security remain the main challenges facing Moroccan CIOs. These challenges remain 'inescapable' and do not allow them to focus more on the budgetary and HR challenges of the IT function.

4. Empirical study: IS security of a large public administration in Morocco .

Starting from the interest granted to digital security in Morocco, the large public administration in Morocco is part of the ducyber security approach by developing a security policy for these information systems that are specific and adapted to its needs.

Our study focuses on a large public administration that has an (IS) department. For the realization of our IS security audit, we performed the following actions:

• An awareness of the work carried out by the public administration in question.

• An understanding of the devices (operational and in the process of being set up) relating to the security of the information system of the administration in question.

• A knowledge of the requirements in terms of security

• Interviews with certain actors of the administration in question based on the ISO 27002 standard.

• An analysis of the information system of the organization in question based on the ISO 27002 standard.

• An analysis of the network architecture of the organization in question

• Intrusion tests internal and external of the IS of the administration in question.

• A knowledge of the environment of the machine room / computer park.

Methodological approach: qualitative approach people resources

Our approach aims, through interviews with the members of the Information System Department, and business departments to identify organizational, functional and / or technical non-compliance impacting the information system according to the chapters of the ISO 27002 standard.

The choice a focused, on 20 frames and responsible (IS) belonging to 5 business divisions, 4 directorates at the level of the regions including the direction of the information systems.

These interviews were accompanied by site visits to assess the level of safety offered according to the recommendations of the standard.

The consolidation of the information collected and its correlation on all the findings is the subject of an audit report whose objectives are to expose the specific context-specific vulnerabilities of the administration of the administration in question according to the international standard ISO27002 that they could be identified during interviews and site visits.

4.1 Result of the security audit of information systems the administration surveyed.

- **The audit is based on three axes:**

Organizational Audit: assess the organizational aspects of security management for the entire activity.

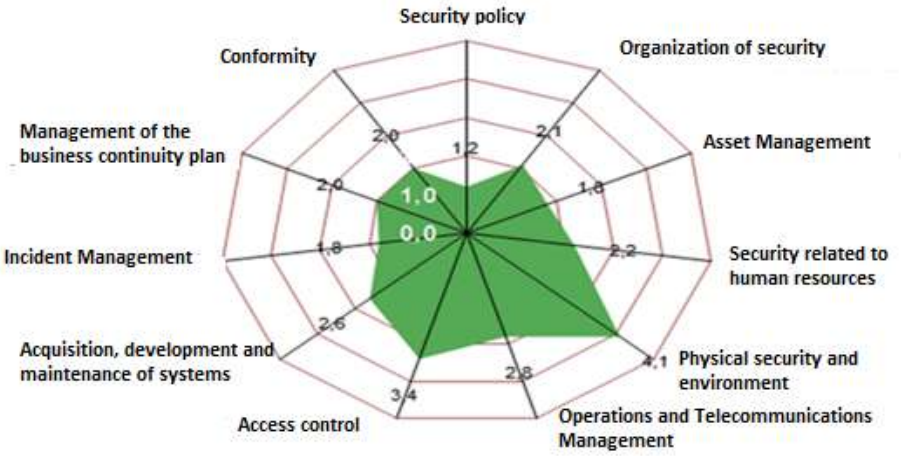
Environmental Audit: the physical security of facilities, the physical access mode of staff and visitors, authentication procedures, personnel security and Datacenter compliance with international standards of environmental safety.

Technical audit: refers to the technical configurations of the applications, servers, databases, network components and security elements on the headquarters of a given administration, and intrusion tests, internal and external.

- **The results of the audit:**

The level of maturity of the administration surveyed Morocco compared to ISO 27002. See figure: below:

Figure 5: Result of the survey of the security audit of the public administration information system of a large size in Morocco.



Source: 4th edition of Med-IT 2012, Xcom and Infomineo, in partnership with APEBI

4.2 : sample of the study:

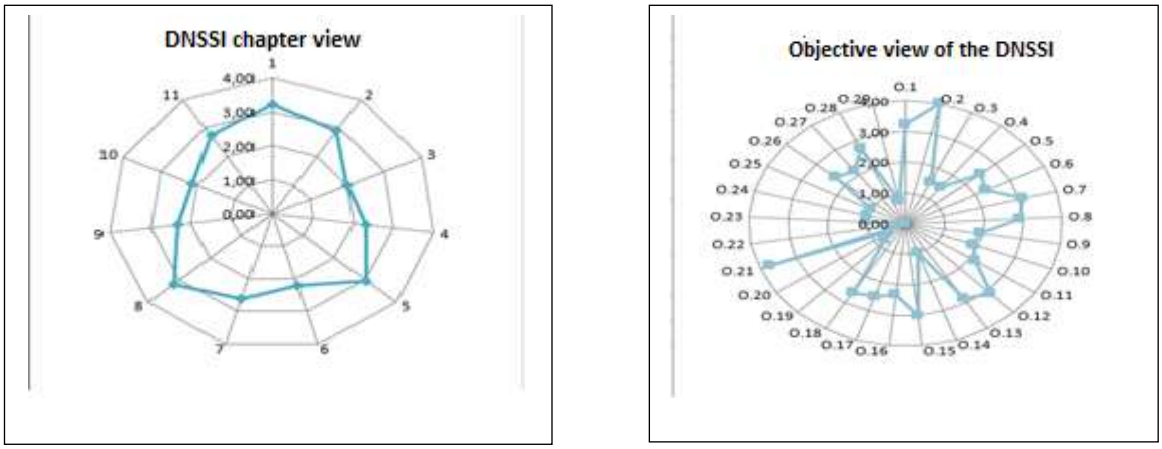
The study based on a questionnaire of follow-up of the implementation of the national directives of the security of (IS) sent by the national defence.

Within the framework of the implementation of these directives within the administrations and public organizations, the DSSIG produced this document, whose objective is to enable them to:

- Measure the maturity of the security of their information systems;
- Provide safety indicators to define areas of progress and to be part of a process of continuous improvement.

The results obtained with respect to the DGISS's Directives are the level of maturity which represents 23.80%.

Figure 6: The rosette of the ISO standard



Source: 4th edition of Med-IT 2012, Xcom and Infomineo, in partnership with APEBI

We note from this result that efforts still need to be made to improve the security level of the public administration information systems of a large size in Morocco.

5. Recommandations :

In the light of the foregoing, we recommend that to improve the security of the public administration information system of a large size in Morocco in a specific way and the general public administration, the following points:

• The approach must be at four levels (Governance, Management, Technology and Human).
• Include mobile in the perimeter of security (IS).
• Support the change of the profession of Information Systems Security Officer (RISS).
• Associate research centers and civil societies for comprehensive and effective treatment.
• Join in continuous improvement.
• Maintain control of cyber security internally.
• Develop the cyber culture.
• Set up information platforms and cyber aggression alert tools.
• Make data a central part of the strategy for public administrations.
• Create an interdepartmental network to exchange on good practices of the security of (IS)
• Strengthen Moroccan legislation, particularly on data storage and protection (CNDP).
• Respect the "DGSSI official bulletin" n ° 4656 DE 6 rejeb 1437 (April 14, 2016)
• Involve other users of information systems in complying with the Information Systems Security (IS) Charter, in order to minimize risks.
• Generalize the business intelligence approach and consider data as a strategic asset.

Conclusion:

Despite efforts and action plans for information systems security within public organizations, there are still efforts to be deployed, the approach to IS security must be at four levels (Governance, Management, Technology and Human Resources).
Failure to comply with the national information system security guidelines developed by the DGSSI remains a major risk for the National Information Systems Security Policy (NISSP).

Bibliographie :

- Brodeur D. et Tardif P.M., Planification et organisation des TI, In Elbekkali A., Bédard S., Benmahbous M., Bistodeau D., Brodeur D., Georgel F., Lachapelle É., Magnan P., Saint-Germain R., Tardif P. M., Vergé R., Gouvernance, audit et sécurité des TI, édition CCH, Québec, 2008, pp. 153-522.
- Bulletins d'information Officiel de maCERT/DGSSI voir le site www.dgssi.gov.ma ;
- CIGREF « Alignement stratégique du système d'information » Comment faire du système d'information un atout pour l'entreprise ? septembre 2002
- CIGREF « Gouvernance du système d'information » Problématiques et démarches, septembre 2002
- CIGREF « Systèmes d'information : Innovation & création de valeur » recherche au cigref décembre 2007
- Club Urba-EA « urbanisme des systèmes d'information et gouvernance » édition Dunod, Paris 2006.
- Efernandez-Toro A., Management de la sécurité de l'information : Implémentation ISO 27001, Eyrolles, novembre 2007, pp. 15-255.
- Elbekkali A., Bédard S., Benmahbous M., Bistodeau D., Dominic B., Georgel F., Lachapelle É., Magnan P., Saint-Germain R., Tardif P.M., Vergé R., Gouvernance, audit et sécurité des TI, édition CCH, Québec, 2008, pp 6-522.
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information — Vers une culture de la sécurité. Paris: OCDE, Juillet 2002.
- L'ISO, la norme internationale : ISO 27001, les exigences du système de gestion de la sécurité de l'information, ISO copyright office, Publié en Suisse, 2007, pp. 6-42
- « Thibaut Chevillotte, Manager Sécurité, CGI Business Consulting » 2013 GROUPE CGI INC

- Marie Despres-Lonnet, « Yves Chevalier : Système d'information et gouvernance », Études de communication [En ligne], 32 | 2009, mis en ligne le 31 août 2009, consulté le 01 octobre 2016. URL : http://edc.revues.org/958
- MEHARI-2007 : Présentation générale – 06 février 2007 présenté par le CLUSIF ;
- Rapport d'Etude : « Baromètre de la Sécurité des systèmes d'information au Maroc Edition 2014 » Hicham ElchgarIT6 ;
- Rapport d'Etude « 1erBaromètre de la Fonction SI au Maroc Edition 2012 » Casablanca Maroc.
- Thibaut Chevillotte, Manager Sécurité, CGI Business Consulting » 2013 GROUPE CGI INC
- http://www.cairn.info/revue-systemes-d-information-etmanagement-2012-1-page-113.htm