When can we talk about implementing an Information Security Management System, according to ISO 27001?

Mr. Mustapha BOUZIANI [a] , Ms. Meriam MERBAH [b] , Ms. Malika TISKAR [c] , Mr. Aziz ET-TAHIR [d] , Mr. Abdelaziz CHAOUCH [e]

[a] Phd Faculty of Science KENITRA MOROCCO, mostafasalim1516@gmail.com
[b] Phd Faculty of Science KENITRA MOROCCO, meriam.merbah@gmail.com
[c] Faculty of Science KENITRA MOROCCO, malak_tis@hotmail.com
[d] Professor at High School of Technology Mohamed V University, RABAT, MOROCCO , ettahiraziz@hotmail.com
[e] Professor at Department of Organic Chemistry, Catalysis and Environment Laboratory Faculty of Science, Ibn Tofail University - KENITRA, MOROCCO, achaouch61@gmail.com,

Article History: *Do not touch during review process(xxxx)*

Abstract: Information Technology is developing at a high pace, but it remains vulnerable to various threats targeting its integrity, confidentiality and availability.

Each organization or institution projects its strategic vision for security concerns by focusing on the information system and risk management. Information security or ISMS is at the heart of this strategy and has become a major issue in information systems management.

To this end, it is necessary to know and understand the subject of the implementation of an Information Security Management System according to ISO 27001, which aims to protect any institution or organization from possible loss, theft or alteration of data. This procedure not only defends and preserves the computer systems against intrusions or disasters but also ensures its survival. This standard gives the conceptual good practices which are established to supplement the technical measures thanks to its security norm ISO27002, in order to ensure a full-fledged security...

Therefore, it is recommended to implement an ISMS based on ISO 27001 when risks related to the security of the company's data could come up.

Keywords: ISMS, Implementation, ISO27001, Information Security, IS, ISO27002, Confidentiality, Integrity and Availability, PDCA, ITIL, PISS, RISS.

Summary: Computer technology is developing at a high rate, but it remains vulnerable to various threats targeting its integrity, confidentiality and availability.

Each organization or institution projects its strategic vision for security concerns by focusing in particular on the information system and risk management. Information security or ISMS is at the heart of this strategy and has become a major challenge in information systems management.

For this purpose, it is necessary to know and understand the subject of the implementation of an Information Security Management System according to ISO 27001, which aims to protect the company from any loss, theft or alteration of data. This procedure not only defends and preserves the computer systems against intrusions or disasters but also ensures its survival. This standard gives the conceptual good practices which come to supplement the technical measures thanks to its standard ISO27002, in order to ensure a 360° security...

Therefore, it is recommended to implement an ISMS based on ISO27001 when risks related to the security of company data arise.

Keywords: ISMS, Implementation, ISO27001, Information Security, Confidentiality, Integrity and Availability, Implementation, PDCA**.**

1. Introduction

Information systems security remains at the top of the list of major issues facing IT executives. Potential concerns regarding computer and network intrusions as well as natural disasters are omnipresent.

As long as the relatively new threats and computer viruses, are proving to be particularly worrisome, a significant number of information systems managers who have responded to this concern, have migrated their organizations into the highly interconnected environment of modern technology, but continue to see the threats as a prospect of a pre-connected era. The use of information technology poses significant risks to information systems and in particular critical resources, due to its inherent nature; they then expose their organizations to potential risks that they are unaware of, refuse to recognize, or are often ill-equipped to properly manage and control such situation.

This notion of information security is becoming increasingly clear and defined. Indeed, organizations are becoming more and more aware of the importance of adopting a human resources solution and recruiting competent managers in this area. These measures aim, in particular, to ensure and manage better data protection by implementing or setting up an ISMS according to ISO/IEC 27001 while preserving the Confidentiality, Integrity and Availability of information.

2. The Problematic

In the ISO270xx family of information security standards, the two standards ISO/IEC27001 and ISO/IEC27002 complement each other, as they constitute a complementary pair in the field of security. Indeed, ISO27001 presents the requirements that can be the object of an ultimate certification, and ISO27002 presents the recommendations for the effective implementation of these requirements.

Several companies or organizations choose to mutualize ITIL and ISO27001 in order to ensure a good security management and to set up a complete ISMS.

The problem is to know when it is appropriate to ensure and implement an information security management system referring to the ISO27001 standard.

3. Methodology

Before proposing the solution, we will define the ISO27001/27002 standards.

ISO27001 in its 2013 version, is an internationally recognized methodology dedicated to information security. This ISMS standard, is in fact recognized as the "common language" for organizations, as it allows them to engage in the management of their information security and at the same time ensure the necessary protection of their competitive information advantages.

ISMS standard defines information security as the preservation against various risks, vulnerabilities and threats in order to ensure the confidentiality, integrity and availability of information, the following schema tries to emphasize this component :

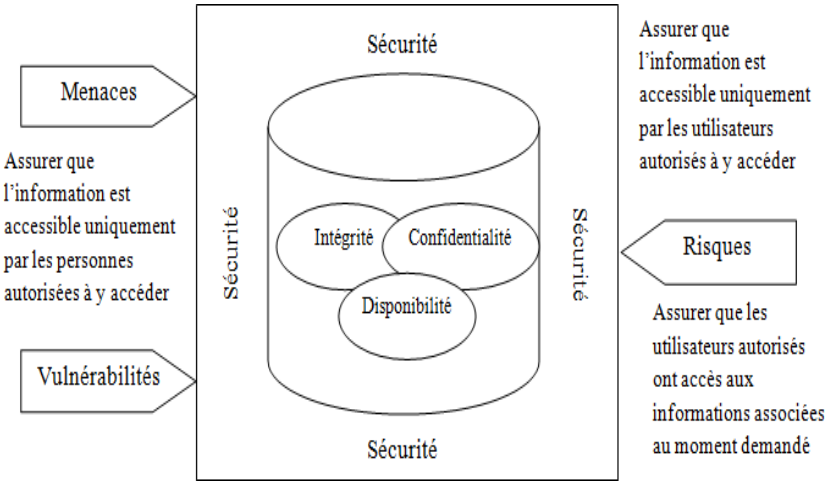

Figure.1. ISMS according to ISO27001

4. Repairing for an ISMS project and the PDCA cycle

- Detect promptly processing errors ;
- Identify immediately any non-compliance with safety rules and organize immediate escalation of incidents ;

- Verify that all safety-related tasks are actually carried out, whether by humans or automatons ;
- Identify actions to be taken to correct non - compliance to safety rules.

In terms of control, regular reviews of the effectiveness of the system should be carried out based on the results of audits, incident reports, in addition to and suggestions and comments received from the parties concerned. Besides, the levels of acceptable residual risk should be continuously reviewed and adjusted in line with the evolution in the organization, technology, laws and regulations, and public opinion.

Measurement requirements are explicitly contained in the standard, in the form of risk assessments, audits, incident and non-compliance data collection.

However, the standard lacks the metrics that would, with a single baseline, make it easier to compare certified entities.

5. Benefits

Adherence to the ISO 27001 standard has several benefits, including :

- Improving the effectiveness of information security ;
- Business differentiation ;
- Trust of business partners, stakeholders and customers (certification is proof of due diligence) ;
- The only standard with worldwide acceptance ;
- Potentials for lower insurance rates ;
- Compliance with mandates and laws (Data Protection Act, Communications Protection Act);
- Senior management takes responsibility for information security ;
- A standard allowing for the coverage of information technology as well as organization, personnel and facilities ;
- Staff responsibilities are targeted ;
- A mechanism to measure the success of security checks.

6. ISO27002

The security objectives indicate the goal to be achieved and the security measures activities relating to be taken to implement these measures.

ISO27002 is a tool to help implement ISO 27001. It includes an introductory clause on risk assessment and treatment, 39 security objectives, ranging into 133 organizational and technical security measures, relating to 11 areas :

- The security policy : expresses management's orientation and commitment to information security.
- The security organization: it makes it possible to identify the information security management responsibilities within the entity, including when third parties access the information or are responsible for its processing.
- Information classification or asset management : aims at maintaining the company's information assets.
- Human resources security: aims at reducing human-induced risks.
- Physical and environmental security: makes it possible to prevent unauthorized access to premises, information and their media, as well as any form of damage or deterioration to these premises.
- Operations and communications management: ensures the correct and secure functioning of information processing infrastructures and minimizes operational risks.
- Access controls: allow to control the logical access to the information assets.
- System development and maintenance: their function is to include security in the development and maintenance of information systems, from the specification and design phases.
- Security incident management: provides the traceability and analysis elements essential for corrective and preventive actions.
- Business continuity : it is achieved by putting in place countermeasures to interruptions in the entity's activities in order to allow vital processes to continue to operate despite major failures or disasters

impacting the information system.

- Compliance with internal and external regulations: its objective is to avoid legal, regulatory or contractual violations and to ensure the proper application of the security policy.

Indeed, most organizations today focus on the principles of protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification or destruction. The consequences of these incidents can range from degradation or disruption of service to customers to the failure of the organization.

This article therefore sets out a study of cases requiring the implementation of an Information Security Management System according to the ISO/IEC 27001v2013 standard; a management system then makes it possible to establish a policy, set objectives and achieve them. In other words, it is about implementing actions (technical, organizational) to achieve a previously set objective.

Management systems go far beyond the scope of Information System :

- The implementation of good practices and feedback from experience REX aims to improve the application of procedures ;
- Formal achievement of policy and process documents (such as the ISSP) supports audits and certifications.

This last point should not be overlooked: certifications have the virtue of increasing trust between organizations and their clients.

In order to ensure an ISMS accurately, it is necessary to ensure the great principles which result from it, in particular, the **confidentiality**, the **integrity**, the **availability** and the **traceability** of information in the broad sense!

In general, and to conclude, the ISMS presents a set of **tools**, **documents** and **methods**, which aims at setting and applying an information security policy adapted to the needs and the specifications of a company.

The implementation of an ISMS seems to be an asset. However, practically, how is it implemented?

7. How to set up an ISMS ?

Practically, the implementation of an operational ISMS is set out in the ISO27001 standard and is based on the principles and fields of quality. The Deming wheel PDCA approach, aims to maintain a continuous improvement of the system by developing four phases:

a) **Plan** : plans the actions to be implemented
b) **Check** : this step consists of evaluating the differences between the first two phases.
c) **Do**: the phase that consists of taking action, it is the operational phase that allows us to move towards the target previously set.
d) **Act**: the phase that allows to fill the gaps by corrective actions. The following diagram illustrates the scope of the project

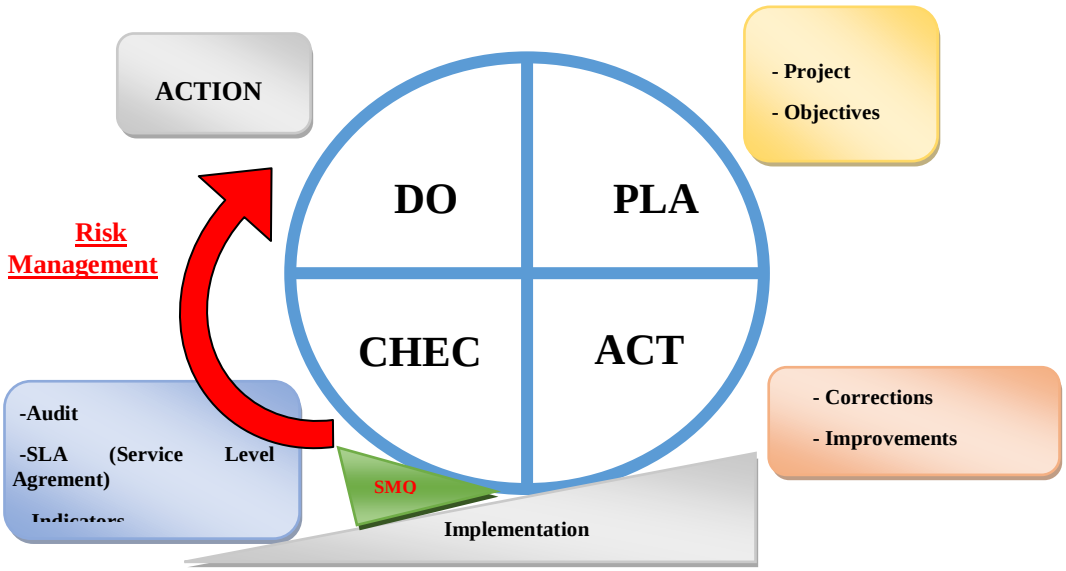

Figure.2. The ISO27001 PDCA cycle

The Information Security Management System (ISMS) Deming wheel (PDCA)

Referring to the field of information systems security and detailing at this stage the functionalities of each phase of this Deming wheel :

8. The four phases of the PDCA approach according to ISO27001

Phase 1 : Plan

The objective of this first step is to lay the foundations of an operational ISMS (ISO 27001 standard). If we refer to the reference document, it is about :

- Define the **policy** and scope of the **SMSI** ;
- Assess the **risks** and their treatment ;
- Choose the appropriate **safety measures** to control the risks.

In order to implement an **ISMS** and to start the **PSSI** well, this first step is essential and initiated by a document that frames the policy.

Phase 2 : DO

This phase is characterized by the implementation of the measures mentioned in the previous phase. It is about deploying security in an operational way.

It takes up the main lines of the security action plan of the PISS. Nevertheless, the implementation of an ISMS, in the sense of the ISO27001 standard, broadens the scope of application by completing the action plan :

- First, key performance or steering indicators are attached to each measure to assess its effectiveness and compliance. This process is not easy. However, the ISO27004 standard proposes a methodology to guide their development;
- Afterwards, the 27001 standard recommends to set in stone an awareness training for the company's staff to the ISS issues. This is a good thing, as it is one of the themes addressed in the Policy of Information Security System PISS!

In this phase, the role of the RSSI is oriented towards consulting. its role is also to assist the project management, to support the change within the project teams.

Phase 3: Check

This step is the central phase of the PDCA approach. It aims to implement the necessary means to measure the compliance of security requirements with the reference specifications of the ISO27001 standard.

This aspect has already been addressed during the development of the PISS : the role of the RISS is to verify the proper application of the requirements so that the defined target is reached as efficiently and quickly as possible.

In concrete terms, to measure the gaps between the measures taken and the reference level, the RISS can achieve (or propose to achieve) :

- **Internal audits** planned in advance or unannounced controls. Their objective is to determine, thanks to the previous indicators, the gap between the standard and the ISMS implemented. To carry them out, the RISS can proceed in 3 steps:

a) Set up a **REX procedure** (also called lessons learned) that allows each manager to report changes in his or her scope.

b) Assess the impact on the current version of the PISS.

c) Facilitate a management meeting to endorse changes.

- **Information System** maturity **audits** which aim to determine the issues related to the organization's information system, to measure the gap between what should be done and what is done, and to explain the actions to be implemented to manage the SSI in an adequate way. The ANSSI proposes a methodological guide to carry them out. ISO27002 can also be a solid basis.

- Penetration test campaigns or code reviews.

- During the "**Check**" phase of the **PDCA** process, the various control procedures also depend on the

company's culture and its level of awareness of ISS.

It should not be forgotten that the PISS has been translated into an action plan for its implementation. It is therefore also necessary to update this implementation methodology. Two scenarios are possible : if the urgency justifies it, it can be done immediately. If not, at the next deadline of the revisit.

In this context, the RISS can advantageously complete the necessary tools, thanks to the development and updating of an ISS dashboard for the management team.

Its objective is to provide all levels of decision-makers with a synthetic reference document that offers a technical, functional and organizational overview of the consideration of ISS.

The dashboard can also be used in the audit phases to measure the level of ISS awareness.

The **ANSSI** proposes a methodology for its elaboration. In parallel to the implementation process, this document proposes indicators at different levels :

- **Strategic** (e.g. status of the implementation of the PISS);
- **Functional** (e.g. follow-up of audits, progress of network security);
- **Operational** (identification of incidents, monitoring of staff awareness training).

Phase 4 : Act

This last phase aims at implementing corrective, preventive or improvement actions to reduce the dysfunctions identified in the previous phase. It is important to keep in mind that this four phases approach aims at a continuous improvement of the ISMS, in order to reach a maximum compliance with the reference texts.

It is deduced that the ISMS is a tool for continuous improvement of information security and that its general and primary goal is to guarantee the good control of the major risks of an organization in order to protect itself and to ensure the confidence of the partners.

After studying the four phases of **PDCA**, a presentation of the role of the Information System Officer RISS who is in charge of the project management. He defines the guidelines for the operations necessary to improve the measures according to the identified risks, the regulatory and technical monitoring he carries out, and the feedback from the ISMS stakeholders.

In summary, this first iteration of the PDCA cycle led to planning the implementation of requirements and security measures (Plan phase). Requirement implementations were cited in the **DO** phase with the use of a security action plan. With a first level of security and after having implemented these first measures, an evaluation of the effective application in the Check phase by measuring the gaps that still need to be closed in order to reach the set target. Finally, thanks to the gaps deduced, corrective actions are carried out in order to reduce the above mentioned gaps, with the final objective of reducing or eliminating the risks to the IS and achieving a higher and guaranteed level of security (Act phase).

Implementing the ISO27001 standard recommends a quality approach based on a continuous improvement approach (**Plan - Do - Check - Act**). The implementation and the setting up of an ISMS is guaranteed (in application of the ISO27001v standard) while keeping a continuous improvement of the security, by implementing the PDCA approach

In order to ensure a good result with a high level of security, it was necessary to bring the ISMS in conformity with the ISO27001 standard, to consider an ultimate certification which is a desirable and optional option to overcome the deficiencies, to make a maintenance, a regular follow-up and a continuous improvement.

Indeed, each organization still requires an ISMS to be implemented in accordance with the ISO27001 standard and will be developed as follows:

A. Stage and preliminary study

The General Management of the organization must follow up and validate the elements that are related to the ISMS. This must be done through a study of the state of the art of the security mechanisms, the identification of the scope of the ISMS stakeholders and their challenges.

B. Stage of selecting the SMSI scope and application area

Define the scope, i.e. the activities to which the ISMS applies, and justify any areas excluded from the scope.

C. Planning and safety policy

Once the scope has been chosen, define the information security strategy has to be defined to drive the compliance project. This declaration of intent is formalized by the **Security Policy** written and signed by the General Management.

D. Method and risk analysis

The company must **identify the risks on its perimeter**. To do this, it is necessary to choose a risk assessment method that is adapted to the context and challenges of the company.

In order to achieve the desired security objectives and depending on the identified risks, the security measures may vary. However, it is necessary to organize follow-up meetings of the project in order to optimize the implementation of these measures on the one hand, and to keep the management involved on the other hand :

a) ISMS use

Referring to the basic data and especially to the Deming Wheel PDCA: **Plan, Do, Check, Act**.

This model allows them to be optimized throughout their life cycle. The implementation of PDCA must be done since their definition.

b) Monitoring the SMSI

The SMSI is then a complex living whole whose "health" must be measured, and when necessary, "cared for". This must be translated in a practical way by :

- An internal audit ;
- The application of possible corrective actions in case of detecting cases of non-compliance ;
- A management review in order to consolidate past incidents and draw the current and future directions for its ISMS;
- A mock audit if the certification audit is planned in the schedule.

c) Certification and audit (optional but of added value)

An ISMS that has been implemented and meets all the requirements of ISO27001, can undergo examination by an accredited certification body, which will prove the effectiveness of its implementation in the organization and add value and importance to its information security.

This is followed by a review of the organization's management system documentation and its proper implementation after which the certification body will also conduct an audit exercise to test and judge the compliance of the procedures.

9. Conclusion

Through these ingredients, we have tried to define the ISO/IEC27001 and ISO/IEC27002 Information System standards in order to motivate small and medium enterprises and organizations to opt for better security of their data and information.

Thus we have also highlighted the steps to adopt to understand better what is the implementation of an ISMS according to ISO27001 and when to conduct it.

This action of implementing an information management system and an ISMS will become a necessity and even an obligation for any entity wishing to have credibility and confidence, measures that will undoubtedly lead to the progress and development of the company.

10. References

Pereira T and Santos H (2010) A security audit framework to manage Information system security. J. Comms. Comput. Inform. Sci. 92: 9:18.

Thomson KL and Solms R (2005) Information Security obedience: a definition. J. Comput. Secur. 24(1), 69-75.

Jaschob A and Tsintsifa L (2006), IT-Grundschutz: Two-Tier risk assessment for a higher efficiency in IT Security Management. ISSE 2006- Secur Electro Bus Process. Inform. Secur. Solut. Eur. Conf. Rome, Italy. pp: 95-101.

Dimitris Petropoulos, ISO/IEC 27001:2005, ENCODE Middle East, September 2006. Service de Normalisation Industrielle Marocaine (SNIMA), Moroccan Standard NM

ISO/CEI 27001, 2009 (classification index 00.5.701), Information Technology, Security techniques, Information Security Management Systems - Requirements, 2009.

Service de Normalisation Industrielle Marocaine (SNIMA), Moroccan Standard NM ISO/CEI 27002, 2009 (classification index 00.5.702), Information Technology, Security Techniques, Code of Practice for Information Security Management, 2009.

France: Solucum Group. Berteau, Michel, Doyen, and Eric. (2013). Benchmark of ISMS tools, 27001 club.

White Paper. Bloch, L., & Wolfhugel, C. (2011). Computer security: principles and methods. Paris: ed Eyrolles.

Lyon: Archives ouvertes Hal. Boulet, P. (2007). Management of Information System Security.

Paris: Lavoisier. Calder, A. (2009). Information Security based on ISO 27001/ISO 27002 "A Management Guide".

London: Van Haren. Calder, A. (2013). ISO27001/ISO27002 "A pocket guide". IT Gouvrnance Publishing.

Carpentier, J. F. (2012). computer security in small business " state of the art and best practices".

France: ed ENI. Chardonnet, A., & Thibaudon, D. (2003). Deming's PDCA guide "continuous progress and management". Editions d'Organization.

Del Duca, J., & Planche, A. (2012). la Sécurité Informatique "organize the security of your company's IS".

France: ED: ENI. Fernandez-Toro, A. (2016). Operational Security " practical advice to secure the Information System".

Eyrolles. Gallotti, C. (2019). Information Security" Risk Assessment, Management Systems, The ISO/IEC27001 Standard."

Lulu. Librairietechnique, s. e. (2016). ISO 27001 information security management.