ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 3, March 2013

Risk Management for ISO 27005 Decision support

Hanane Bahtit[1], Boubker Regragui[2]

PhD student, Information Processing and e-Strategy, ENSIAS, University M^{ed} V, Rabat, Morocco[1]

Professor, Information Processing and e-Strategy, ENSIAS, University M^{ed} V, Rabat, Morocco[2]

Abstract: The security of information systems focuses on raising the level of business security while aligning with its strategy and objectives. The family of ISO 2700x, whose theme is: Information technology - Security techniques, allows taking into account all of these security problems, by offering a pack of uniform and standards that respect the continuous improvement cycle PDCA.

Being closely linked to the security of information systems, the risk management consists of assessing the uncertainty of the future to make the best decision possible today. Risk management and all decision processes fall within this problematic. The decision making on the Information security risk management requires taking into account an increasing amount of data of different types and qualities. As a result, risk managers increasingly use computers to provide powerful tools for decision support.

The aim of this article is to make an overview of the ISO 2700x, focusing more particularly on the content of the ISO 27005 standard, dedicated to information security risk management. In this context, a UML modeling of the processes of ISO 27005 is presented as an improvement of this modeling by criteria and indicators that support the quality of decision making in various decision points. This is the vision of increasing the efficiency and effectiveness of decision making process.

Keywords: Information Systems Security, risk management, decision making, ISO 2700x, ISO 27005

I. Introduction

Consistent with the stakes and objectives of the organization, information system security returns to manage its risks. In fact, the information security risk management has become nowadays a common and essential approach.

There are several methods and standards for risk management (Mehari, EBIOS, ISO 27005, etc.). However, the development and evolution of these standards, do not exclude the human factor. Indeed, the risk manager intervenes repeatedly during the risk management process. This promotes subjectivity at the expense objectivity. The result of this management is not sufficiently analytical and is still largely informal. To overcome this lack of formalism and consider the prospect of automating the information risk management, we propose a modeling of the ISO 27005 standard by using UML 2.3. The choice of 27005 standard is motivated by the fact that it is becoming more and more as a method for assessing and treating risks. The choice of UML as modeling language is due to a formal and standardized language. UML is a meta-model which will better conceive abstract concepts and guidelines of the standard through their transformations in diagrams.

In this paper, we first analyze qualitatively the content of main standards as SWOT matrices. Then, we present a modeling of the ISO 27005 standard in order to remove ambiguities of interpretation and translate the theoretical guidance of this risk management standard in UML diagrams. Finally, in the context of automated risk management, we propose some criteria that will improve the quality of decision making at both decision points in the process of risk management.

II. ISO 2700x FAMILY

ISO / IEC 2700x is a family of international standards of Information Security Management System (ISMS). It covers all types of organizations and specifies the requirements and guidelines necessary to develop, implement, monitor, evaluate and improve an ISMS. ISO 2700x family comes in 13 volumes as shown in the following table:

TABLE 1. ISO 2700x family

	Title	**Publication date**
ISO 27000	ISMS -- Overview and vocabulary	2009
ISO 27001	ISMS -- Requirements	2005
ISO 27002	Code of practice for information security management	2005
ISO 27003	Information security management system implementation guidance	2010
ISO 27004	ISMS -- Measurement	2009
ISO 27005	Information security risk management	2008
ISO 27006	Requirements for bodies providing audit and certification of ISMS	2007
ISO 27007	Guidelines for ISMS auditing	2011
ISO 27008	Guidelines for auditors on information security controls	2011
ISO 27010	Information security management for inter-sector and inter-organizational communications	2012
ISO 27011	Information security management guidelines for telecommunications organizations based on ISO 27002	2008
ISO 27013	Guidance on the integrated implementation of ISO 27001 and ISO 20000-1	2012
ISO 27015	Information security management guidelines for financial services	2012

In what follows, we present a qualitative analysis of ISO 27001, ISO 27002 and ISO 27005.

A. ISO 27001

ISO 27001 is the ISO 2700x family central standard. It defines the conditions to implement an ISMS and it is designed to ensure the selection of adequate and proportionate security measures to the organization context. A qualitative analysis of this standard is given by the following SWOT matrix:

TABLE 2. 27001 SWOT MATRIX

Strengths	▪ Check ISMS complies or not with standards ▪ Communication easier ▪ Assign security budget to the most relevant measure	Weaknesses	▪ Do not ensure the effectiveness of measures implemented but only their existence ▪ Huge documentation work
Opportunities	▪ Belonging to the ISO family	Threats	▪ Low experience of accreditation organizations ▪ Consulting firms are also accreditation organizations

It should be noted the paradox of consulting firms. In fact, a consultant may be auditor at the same time.

B. ISO 27002

ISO 27002 is a code of good practice more than a standard. In adopting this standard, the organization must assess its own information security risks and apply appropriate controls. In fact, ISO 27002 provides general guidance on the selection and use of appropriate methods to analyze risks without prescribing a specific method. SWOT matrix corresponding to the analysis of the ISO 27002 is as follows:

TABLE 3. 27002 SWOT MATRIX

Strengths	▪ Optimize the costs of ISS by associating with ISO 27001 ▪ Increased knowledge of risk management ▪ Does not require a technical solution	**Weaknesses**	▪ Do not define adequate security measures in the context of the organization ▪ Indicates best practices for IS security approach without mentioning their implementation
Opportunities	▪ Belonging to the ISO family	**Threats**	▪ Slow cycle evolution of the standard in relation to the threats and security measures

C. ISO 27005

Intended to be used either autonomously or as a support for ISO 27001, this standard establishes a methodology, which defines techniques to implement in approach to risk management that could compromise the safety of the organization's information. The strengths and weaknesses of ISO 27005 are grouped in the following SWOT matrix:

TABLE 4. 27005 SWOT MATRIX

Strengths	▪ Flexible and reusable ▪ Continuous risk management ▪ Highlighting the human factor: the concept of responsibility	**Weaknesses**	▪ No specific methodology for risk management
Opportunities	▪ Belonging to the ISO family	**Threats**	▪ Lack of experience and practice (compared to Méhari and BIOS)

From the foregoing, it is clear that the standards of the ISO 2700x family are complementary rather than competitive. As well, weaknesses of each standard converge almost to the same point: how associate the guidelines of the standards to the context of organization.

Risk management is a key step in the procedure to follow to secure information systems. ISO 27001 imposes upon its implementation, a description of the risk assessment methodology chosen so as to be able to provide reproducible results, a report of the risk assessment and risk treatment plan. In the spirit of ISO 2700x family, ISO 27005 standard takes over and proposes an assessment, analysis and treatment risks process, in accordance with continuous improvement process of the information security suggested by ISO 27001.

In the follow up of this work, we will focus on the ISO 27005 standard as an information security risk management method. We begin with modeling the standard. Then, we build different decision points by decision criteria to allow the risk manager to perform a deterministic choice. Finally, we describe the risk assessment process.

III. MODELING OF THE ISO 27005 STANDARD

The risk management process related to the information system security, presented in the ISO 27005 standard, consists itself of several under process businesses. Each of these under process can be considered individually, although its output constitutes an input for the following process.

During the development of this work, these partial processes as well as the global process will be modeled in the form of diagrams of activities. Indeed, the diagrams of activities UML allow emphasizing treatments and allow representing graphically the behaviour of a method or the progress of a use case [1].

A. Information security risk management process

As shown in Fig. 1, the point of departure of the information security risk management process is the establishment of the context concerning the organization and which expresses its objectives and strategy. Then, a risk assessment is done to classify the risks according to an order of priority.

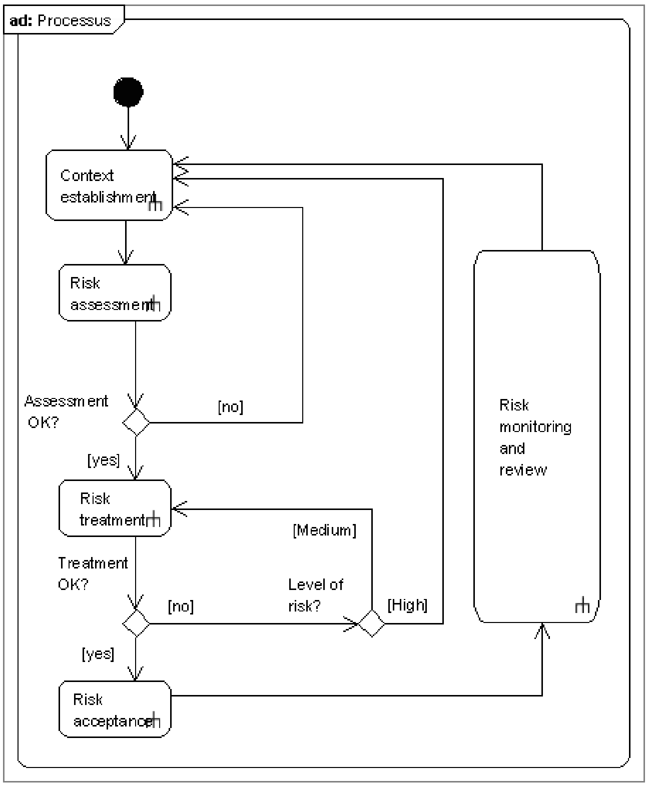

Fig. 1 The information security risk management process activity diagram

The information security risk management process has the peculiarity to be iterative. Two points of decision favor this.

The first point of decision aims at the result of risk appreciation. If it is not satisfactory, that is the appreciation does not provide enough information to determine correctly the necessary actions to return the risks to an acceptable level, then iteration towards the context establishment is required. Should the opposite occur, the process of risk management continues towards the stage of the risk treatment.

The second decision point comes consequently. If the results of the risks treatment are not satisfactory, the risk management process will be resumed either since the stage of the context establishment or since the stage of risk treatment.

According to ISO 27005 standard, the starting point for the resumption of risk management process is not indicated. To remedy this vagueness and represent this aspect, we choose to create a third decision point. Thus, if the level of risk is high then the risk management process will be repeated since the context establishment. Otherwise the process will be repeated since the risk treatment.

Now that the treatment was able to improve the level of the residual risk, the risks acceptance will take place in the process. The standard requires a continuous monitoring and review of the risk during all the risk management process. Let us note that activity diagram concerning the risk management process has no full stop seen the notion of continuity and risk management in the time which characterize the ISO 27005 standard with regard to the other existing methods [2].

Throughout the risk management process, the results should be communicated to the administration and all users. To model the communication process, we choose to integrate it as the last action in the five activity diagrams specific to the various activities of the overall risk management process.

B. Decision points

At decision points, the standard does not provide decision-making criteria that allow the risk manager to do a determinist choice. For example, on the first decision point appearing in the risk management process (Fig. 1), the manager asks the question on the reliability of the risk assessment, without having an indication on the way with which he can measure it.

In this section, we propose criteria and indicators to qualify the result of the risk assessment and risk treatment to help achieve the decision making process.

1) Is the result of the risk assessment satisfactory?

At this decision point, the risk manager asks if the assessment has provided sufficient information to determine correctly the necessary actions to be taken in order to address the risks and reduce them to an acceptable level. The input and output of this decision point are:

TABLE 5. DECISION POINT N°1

Decision point N°1	
Input	**Output**
List of classed risks in order of priority (Result of risk assessment)	Choose between : • A second iteration of the risk assessment • The direct passage to the risk treatment
Criteria related to context	

According to ISO 27005, a general rule to apply is: if the lack of information security can result in significant adverse consequences to an organization, its business processes or its assets, then a second iteration risk assessment, at more detailed level, is necessary to identify potential risks. In other words, the decision at this point depends on the nature of the risk. If it is a major risk, that is an event of high severity but a very low probability of occurrence, then it is worth reiterating at the risk assessment process. Otherwise, if the risk is minor, that it is characterized by a very high likelihood and a low impact, then the decision to take is to continue to risks treatment.

Then, formulation of the criteria is a key element. It should enable the distinction between major and minor risks. Indeed, if the objectives of an asset are extremely important for the conduct of organization, or if the assets present a high risk, it should make a second iteration of the risk assessment on the specific information assets [3]. As if the risks appreciated are minor, the transition to the stage of risk treatment is recommended. On the other hand, the classification of risks in order of priority means that we can easily establish the threshold distinction between major and minor risks. Knowing that major risks have generally an extremely low frequency rate, unlike the minor risks that are most often higher probability of occurrence, we choose to start this distinction by major risks.

The following algorithm will summarize the steps to follow for the risk manager can make a decision at the first decision point in the risk management process, related to the information systems security:

```
Algorithme  Decision point N°1
const
entier n ;        # n risks
major c'est 1 ;
minor c'est 0 ;
var
   entier i , j , k ;
proc
   TRAITEMENT (risk),
   APPRECIATION (risk);
fonc
CRITERES(risk): booléen;
Début
# $R_1$, $R_2$, ... , $R_n$ les risques classés par priorité
# $R_n$ le risque le plus prioritaire
pour k de n à 1 pas 1 faire
   si (CRITERES ($R_k$) =  minor) alors
   exit ;
   fsi ;
fpour
# $R_1$,...,$R_K$    minor risks
# $R_{k+1}$,...,$R_n$ major risks
pour i de 1 à k pas 1 faire
    TRAITEMENT ($R_i$) ;
fpour
pour j de k+1 à n pas 1 faire
    APPRECIATION ($R_j$) ;
fpour
fin Algorithme Decision point N°1
```

Let us note that the functions TRAITEMENT () and APPRECIATION () correspond to the processes of risk treatment and risk assessment, invoked in the risk management process, related to the information systems security [4].

According to this algorithm, the function CRITERES () applied to a risk, returns a Boolean to indicate the nature of the risk in question. In other words, its role is to be based on criteria that describe the context of the organization to say that it is a major or minor risk.

Criteria formulation

The question that arises at this stage is how to translate the context of organization as criteria for judging the degree and nature of risk?

Based on the fact that a risk is the potential of a given threat exploiting a vulnerability of an asset and thus cause damage to the company, several factors help determine whether the high-level assessment is appropriate to risk treatment (satisfactory assessment). In this vision, we propose to refer to questionnaires tool since it does not consider the probabilities associated with potential losses, but considering the magnitude of these losses [5].

Thus, the criteria formulation may include the following:

- What is the degree to which the organization activity depends on information assets (Confidentiality, Integrity, Availability, Non-repudiation, Accountability, Authenticity, reliability)?
- What is the degree of business objectives reached?
- What is the degree of legal and regulatory requirements reached?
- What is the degree of contractual obligations reached?
- What is the degree of unmet expectations and perceptions of stakeholders?
- What is the degree of negative impact on the financial value of the organization?
- What is the degree of negative impact on the reputation of the organization?
- What is the degree of disturbance of the action plans and deadlines?
- What is the level of investment in assets, in terms of development, preservation or replacement of assets?
- Does the asset have value assigned directly by the organization?
- What is the degree of criticality of information assets involved?

In the vision to implement the function CRITERES(), we propose to refer to multi criteria decision making approach [6] [7]. This is based on questions related to the impact of risk on the organization, and that the answers are as a function of the organization context, and allow giving a new value to it.

Indeed, taking into account the fact that a major risk is characterized by a very high impact, and that the criteria mentioned above to measure the impact of risk on the organization, we can estimate the impact of risk factor:

- A weights scale by assigning the highest weight to the most pressing criteria.
- A value scale by choosing appropriate extremes.
- A threshold S0 from which the risk is considered as major.

Thus, if the weight sum $R = \sum_i \text{poids}_i * \text{valeur}_i$ for a given risk is greater than threshold S_0 previously determined, then it is indeed a major risk. Otherwise the risk is called minor. In the next section, we focus on the second decision point.

2) Is the result of the risk treatment satisfactory?

At the second decision point, the risk manager will ask the following questions:

Are the risk treatment actions feasible?
Were the residual risks brought to an acceptable level?

If the answer to the last question is no, then the risk manager has two solutions: reducing the risk acceptance threshold (context establishment phase) or provide additional security measures (risk treatment phase) [8].
The risk acceptance process must, in turn, ensure that residual risks are explicitly accepted by the directors of the organization.
The input and output of this decision point are:

TABLE 6. DECISION POINT N°2

<table>
<tr><th colspan="2">Decision point N°2</th></tr>
<tr><th>Input</th><th>Output</th></tr>
<tr><td>Risk treatment plan</td><td rowspan="2">Choose between :
• A direct passage to the risk acceptance
• A new iteration of the risk assessment with revised context
• Additional security measures</td></tr>
<tr><td>List of residual risks</td></tr>
</table>

It is clear that the direct passage to the risk acceptance is determined by the degree of acceptability of residual risks. It follows that the manager is reduced to estimate the level of residual risks in order to compare it with the acceptance criteria that are based on the context and objectives of the organization.

In case the value of the residual risk exceeds the acceptance criteria threshold, the manager is in an awkward choice between a new iteration of the risk assessment with probably a revised context, and implementation of additional security measures. During the first iterations, the best solution is to lower threshold of risk acceptance, previously established. In the case where the residual risk is not always fulfill the acceptance criteria, another iteration of the risk treatment may be necessary before to switch to risk acceptance process.

In the follow up of this work, we detail the risk assessment process based on its UML modeling.

C. Risk assessment processes

At this stage of the risk management process, it is to describe qualitatively or quantify the risks to classify them according to their gravity or other criteria.

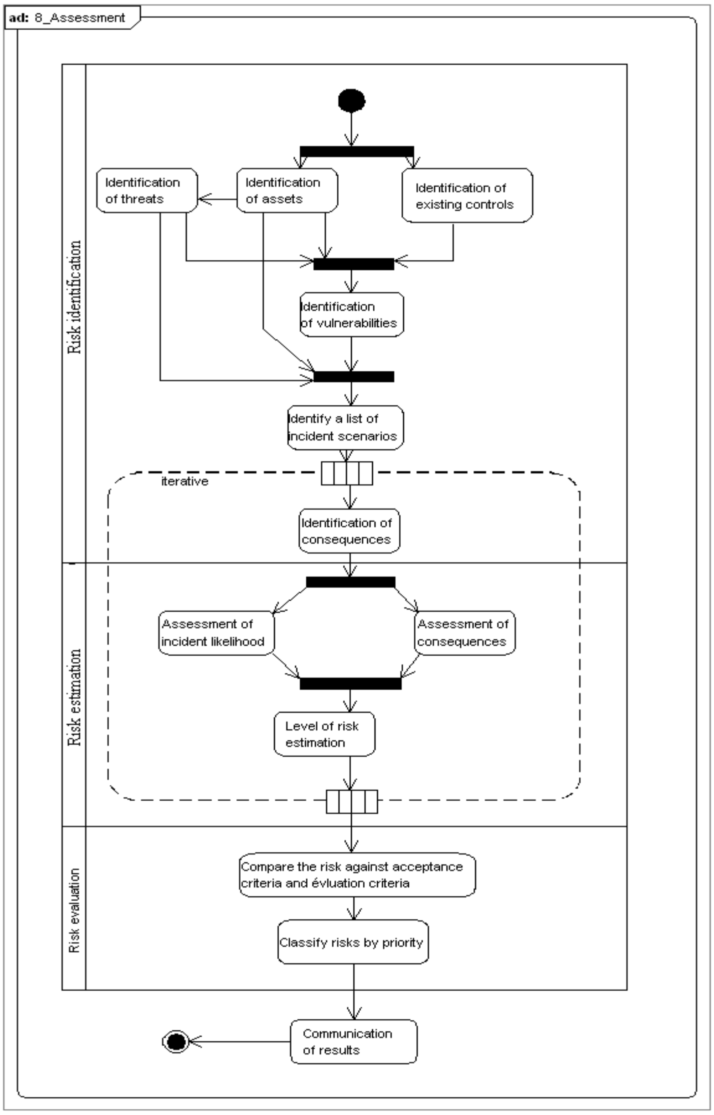
ad: 8_Assessment
Risk identification
Identification of threats
Identification of assets
Identification of existing controls
Identification of vulnerabilities
Identify a list of incident scenarios
iterative
Identification of consequences
Risk estimation
Assessment of incident likelihood
Assessment of consequences
Level of risk estimation
Risk evaluation
Compare the risk against acceptance criteria and évluation criteria
Classify risks by priority
Communication of results

Fig. 2 The Information security risk management process activity diagram

1) Risk identification :

It is advisable first, to identify assets which all have some value for the organization. According to the appendix B of the ISO 27005 standard, there are two types of assets:

- Primary assets: they are the information and the businesses processes.
- Supporting assets: they are physical assets as staff, material, site, etc.

Even if the ISO 27005 standard does not clarify it, it is better at this stage to establish a scale of assets valuation. For example, we can, wonder about the replaceability of the asset, the skills necessary for its use, its purchase cost, its maintenance cost , etc. [9]

If the list of assets is ready, it is necessary to identify the threats. That is to say, all that has the potential to damage assets. Let us note that the threats identification is made only on supporting assets and that every asset can be exposed to several threats. Then, it is necessary to identify the existing control to avoid the redundancy.

From what precedes, the vulnerabilities identification (the asset weaknesses) is feasible as well as the formulation of the incident scenarios. Indeed, an incident scenario is the description of a threat exploiting certain vulnerability or a set of vulnerabilities in an information security incident [10].

So, and for every incident scenario, we shall determine the consequences that losses of confidentiality, integrity and availability can have on assets [11].

2) Risk estimation :

The following stage in the risk assessment consists in estimating the risk level. For that purpose, it will be necessary in first place to assess the consequences by basing itself on the consequences measures scale. In second place, this should take into account of how often the threats occur and how easily the vulnerabilities may be exploited, to assess the likelihood (the probability of the occurrence) of every incident scenario [3]. These two actions can be made at the same time. In third place, the risk level will be estimated by taking into account the previous both appreciations:

- The maximum of the security needs concerning the impacted element: max (add (CID))
- The potentiality of the vulnerability exploitation by the threat (the likelihood)

Risk assessment is an essential step in the risk assessment process. On this point, the ISO 27005 standard imposes no formula linking qualitative and quantitative, but provides three possibilities of calculation in the appendix. It is probably in this calculation phase where development opportunities for owner methods are possible.

3) Risk evaluation :

Now that every risk has a value, this should lead to compare them against risk evaluation criteria and risk acceptance criteria. This will give rise to a list of the risk classified according to the priority.

IV. CONCLUSION

Currently, security is no longer an option. High pressures required by the market, forcing companies to rethink their security methods. Thus, comply with the ISO 2700x family, enables the responsible for information systems security to manage a continuous and consistent security measures in time, to establish a level of trust between stakeholders and strengthen thereafter, the brand of the company.

Risk management helps the company to identify and address the risks that it faces. Thereby increases the likelihood of successfully achieving the objectives of the company. Based on the general concepts specified in 27001, ISO 27005 is designed to help a satisfactory implementation of information security based on a risk management approach.

In this article, we tried to improve the decision making process in order to help achieve the overall risk management process. In fact, we proposed indicators and criteria used to make decisions making effectively and efficiently.

However, the approach proposed in the first decision point ignores the aggregation of several low and medium risk which can result in significantly higher overall risk should be treated accordingly as major risks. Again, the value of risk impact on the organization activity can be expressed qualitatively and quantitatively, however, a method of assigning a financial value can generally provide more information for decision making and thus allow a more efficient decision-making process.

In this context, the weighted sum used to estimate the value of risk has certain limitations such as the interpretation of the weight which is not very clear because it includes both the notion of relative importance of criteria and the normalization factor of criteria scales values. It would be useful in a future work, to approach this estimation by Bayesian networks or networks of neurons.

REFERENCES

[1] Laurent Audibert, UML 2 : de l'apprentissage à la pratique, édition ellipses 2009.

[2] H. Bahtit, B. Regragui, Évolution de la famille des normes 2700x, JNS1, ENSA de Marrakech, Mars 2011.

[3] ISO/IEC 27005, Information technology — Security techniques — Information security risk management, first edition, 2008.

[4] H. Bahtit, B. Regragui, Modélisation des processus de la norme ISO 27005, JNS2, ENSA de Marrakech, Avril 2012.

[5] Rex Kelly Rainer, Jr., Charles A. Snyder and Houston H. Carr, Risk Analysis for Information Technology, Journal of Management Information Systems, Vol. 8 No. 1, p 129-147, 1991.

[6] Jean-Charles pomerol, S. Barba-Romero, Choix multi-critères dans l'entreprise, Hermés, 1993.

[7] BRANS Jean-Pierre, MARESCHAL Bertrand Prométhée, « Gaia : Une méthodologie d'aide à la décision en présence de critères multiples », Ellipses, 2002.

[8] Anne. Lupfer, Gestion des risques en sécurité des systèmes d'information - Mise en oeuvre de la norme ISO 27005, Groupe Eyrolles, 2008.

[9] Hervé Schauer, Méthode de management des risques ISO 27005, 2010.

[10] ISO/CEI 27002, Information technology — Security techniques— Code of practice for information security management, 2005.

[11] ISO/CEI 27001, Information technology — Security techniques—Information security management systems —Requirements, 2005.

BIOGRAPHY

Hanane Bahtit is a PhD student at National School of Computer Science and Systems Analysis, University Mohammed V – Souissi, Morocco (ENSIAS). His research interests are in the field of information security risk management.

Boubker Regragui is a Professor at National School of Computer Science and Systems Analysis, University Mohammed V – Souissi, Morocco (ENSIAS). Head of Department Telecommunication Networks and Head of the research team TIES (Information Processing and e-Strategy). He has guided several research scholars.