Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk

Mohamed Ghazouani
ENSEM
Casablanca, MAROC

Sophia Faris
ENSEM
Casablanca, MAROC

Hicham Medromi
ENSEM
Casablanca, MAROC

Adil Sayouti
ENSEM
Casablanca, MAROC

ABSTRACT
Risk management methodologies, such as Mehari, Ebios, CRAMM and SP 800-30 (NIST) use a common step based on threat, vulnerability and probability witch are typically evaluated intuitively using verbal hazard scales such as low, medium, high. Because of their subjectivity, these categories are extremely difficult to assign to threats, vulnerabilities and probability, or indeed, to interpret with any degree of confidence. The purpose of the paper is to propose a mathematical formulation of risk by using a lower level of granularity of its elements: threat, probability, criteria used to determine an asset's value, exposure, frequency and existing protection measure.

General Terms
Security risk assessment, risk management system, framework, audit, information system.

Keywords
ISO27005, MEHARI, EBIOS, SP800-30 (Nist), CRAMM.

1. INTRODUCTION
Risk management methods enable the organization to plan and implement programs to maximize their opportunities and to control the impact of potential threats. There are many risk management methods in use today. A method or framework for managing risks aims at assisting an organization manages its risk exposures effectively through the application of the risk management process at various levels within of the organization [1].

A risk management method is a sequences of activities based on a published standard that systematizes the five phases that comprise risk management, namely, [1]

- Identification of threats and vulnerabilities impacting the organization's IT assets
- Risk assessment
- Risk mitigation planning
- Risk mitigation implementation
- Evaluation of the mitigation's effectiveness

This is a common step but there is no a common calculation method. This paper is presented as follows: in the section 2 it will give a survey of available information security risk management methods and tools, the section 3 will present a description of EBIOS, Mehari, SP800-30 (Nist), CRAMM and ISO27005, in the section 4 it will give a comparative analysis, the section 5 will propose the approach and in the 6 it will introduce the mathematical formulation of risk.

2. REVIEW OF EXISTING METHODOLOGIES AND TOOLS
Many methodologies exist to assess the security risks associated with unauthorized leakage, modification and interruption of information used by organizations. This section provides an overview of available security risk analysis methods and tools.

Table 1: Risk Management/Risk Analysis Methods and Tools. [1]

Risk Management Methods	Risk Management Methods Tools
• Control Objectives for Information and Related Technology (COBIT) • CCTA Risk Assessment and Management • Dutch A&K Analysis • EBIOS • ETSI • Factor Analysis of Information Risk (FAIR) • Fundamental Information Risk • Management (FIRM) • Failure Modes and Effects Analysis (FMEA) • Facilitated Risk Assessment Process (FRAP) • Information Risk Assessment • Methodologies (IRAM) • ISAMM • Information Security Forum (ISF) Methods • ISO TR 13335 (a Technical Report which is a precursor to ISO/IEC 27005); • ISO/IEC 27001 • ISO/IEC 31000 • Methodology for Information Systems Risk Analysis and Management (MAGERIT) • MEHARI • MIGRA • NIST SP 800-30 • NIST SP 800-39 • NSA IAM / IEM / IA-CMM • OCTAVE • Open Source Security Testing Methodology	• Acuity Stream • Acuity Stream • Archer • Axur • Callio • Methodology (CRAMM) • Casis • Citicus ONE • Cobra • CRAMM • EAR / PILAR • EBIOS • GSTool • GxSGSI • ISAMM • Modulo Risk Manager • Proteus Enterprise • RA2 Art of Risk • Resolver Ballot • Resolver Risk • Risicare • Riskwatch • RM Studio • Risk Manager • RiskOptix • MIGRA • RSAM • vsRisk

Risk Management Methods	Risk Management Methods Tools
• Manual (OSSTMM) • Practical Threat Analysis (PTA) • Simple to Apply Risk Assessment (SARA) • Security Officers Management and Analysis • Project (SOMAP) • Simplified Process for Risk Identification (SPRINT)	

As seen in Table 1, there is no dearth of guides, methodical approaches, and support tools, all of which aim at an objective analysis intended to determine the amount of risk that various IT assets and systems are subject to. The challenge of all these approaches is the complexity of the problem they face, a complexity in the sense that there are many elements to be considered and that, if they are not rigorous, the conclusions will be unreliable [2].

Based on the above methodologies, researches and others work described in [3] [4] [5] [6] [7] this work propose an integrated use of Mehari, Ebios, CRAMM and SP800-30(Nist) to develop a new approach based on ISO 27005 witch should be enhanced through a new mathematical formulation of risk.

3. RISK METHODOLOGIES

3.1 EBIOS

The EBIOS methodology has been created in 1995 by the DCSSI (Direction Centrale de la Sécurité des Systèmes d'information) a government entity attached to the French Prime Minister within the SGDN (Secrétariat Générale de la Défense Nationale), the French National Security Agency.

The method includes 5 steps as illustrated in figure 1:

1. Context;
2. Security needs;
3. Threats analysis;
4. Identification of security objectives; and
5. Identification of security requirements.

3.2 MEHARI

MEHARI is a risk analysis and management method developed by CLUSIF and supported by software managed by the company Risicare (http://www.risicare.fr). MEHARI, originally developed in 1996, aims at assisting the executives (operating managers, CISO, CIO, risk manager, auditor) in their efforts to manage the security of Information and IT resources and to reduce the associated risks. MEHARI is compliant to ISO 13335 risk management standard and is suitable for the ISMS process described by ISO 27001. It allows the stakeholder to develop security plans, based on a list of vulnerability control points and an accurate monitoring process to achieve a continual improvement cycle. MEHARI provides [8] as illustrated in figure 2.

1. Knowledge bases of risk situations
2. Rules for the consolidation of the risk analysis resulting in an optimal setting of action plans
3. Analyze the major stakes
4. Analyze the vulnerabilities
5. Decrease and manage the risks
6. Monitor the security of information
7. Audit data base

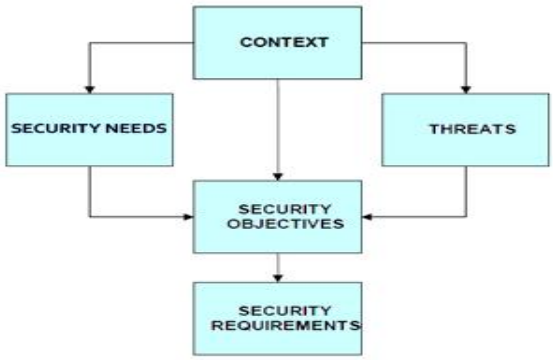

Figure 1: High Level Structure of EBIOS Methodology

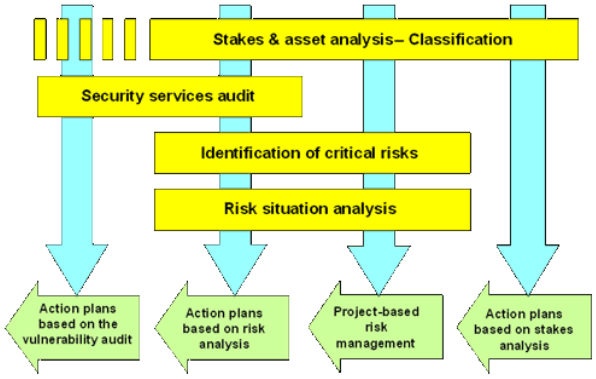

Figure 2: Methodology embodied in MEHARI

3.3 SP 800-30 (NIST)

NIST SP 800-30 is a standard developed by the National Institute of Standards and Technology. Published as a special document formulated for information security risk assessment, it pertains especially to IT systems. Figure 3 gives an overview of key steps to complete a comprehensive risk assessment program as outlined in NIST SP 800-30.

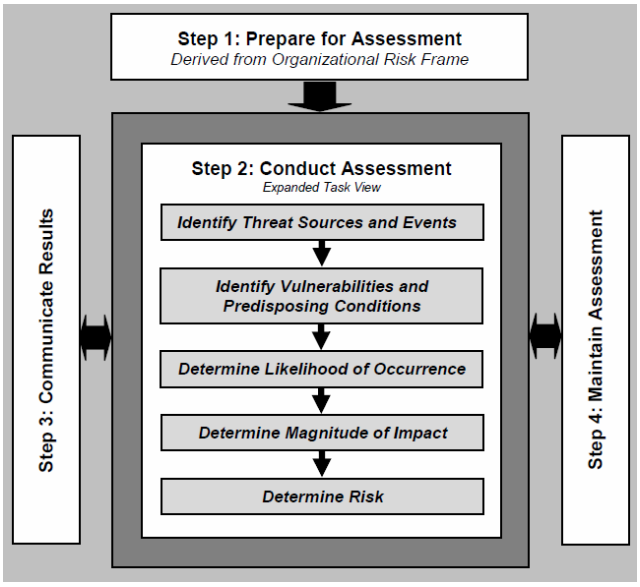

Figure 3: Methodology embodied in MEHARI

3.4 CRAMM

CRAMM is a software-based (Windows-based) security risk assessment and risk management methodology. CRAMM is more of a qualitative methodology than a quantitative methodology. CRAMM is based on three fundamental stages:

1. Assessing the value of the information, and identifying the assets which support the business process;
2. Identifying what threats may affect the system and how vulnerable is the system to those threats; arriving at a conclusion about the risks. The next step is to derive measures of risk, and these are derived from a combination of the threat, the vulnerability, and the asset value. The measures of risk are scaled, so that the security requirements to be established are matched to the degree of risk.
3. Identifying how the risks can be countered, including what improvements are required to existing control measures

Figure 4: High Level Structure of CRAMM Methodology.

3.5 ISO27005

The purpose of ISO 27005 is to provide guidelines for information security risk management. It supports the general concepts specified in ISO 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. It does not specify, recommend or even name any specific risk analysis method, although it does specify a structured, systematic and rigorous process from analyzing risks to creating the risk treatment plan [9].

Is a Standard that encompasses the code of practice for information security management describing a set of information security control objectives and a set of generally accepted best practice security controls [1].

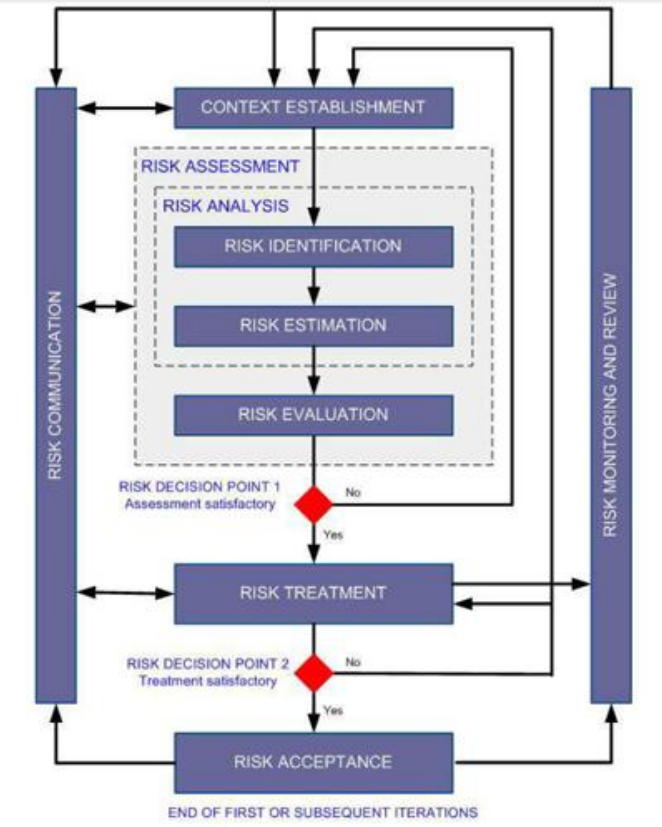

Figure 5: Information security risk management process

ISO 27005 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security."

Figure 5 gives an overview of the Information security risk management process in ISO 27005.

4. COMPARATIVE ANALYSIS

By analysing the studied methodology, a synthetic comparative table can be proposed (Table 2).

Table 2. Synthetic comparative table

Generic ISRM phase and its output	**CRAMM phase**	**NIST SP 800-30 phase**	**OCTAVE phase**	**EBIOS phase**	**ISO 27005 phase**
System Characterization Output:: inventory list of assets to be protected, including their acceptable risk level	Asset Identification	System Characterization	Identification of Critical Assets and Corresponding Security Requirements Identification of Current Security Practices	Study of the Organization Study of the Target System Determination of the Security Study Target Expression of Security Needs	Identification of Assets
Threat and Vulnerability Assessment Output: list of threats and corresponding vulnerabilities endangering the identified assets	Threat Assessment Vulnerability Assessment	Threat Identification Vulnerability Identification Control Analysis	Identification of Threats and Organizational Vulnerabilities Identification of Current Technology Vulnerabilities	Study of Threat Sources Study of Vulnerabilities Formalization of Threats	Identification of Threats Identification of Vulnerabilities
Risk Determination Output : quantitative or qualitative risk figures/levels for identified threats (input: threat probability and magnitude of impact)	Asset Valuation Risk Assessment	Likelihood Determination Impact Analysis Risk Determination	Risk Determination for Critical Assets	Comparison of Threats with Needs (Risk Determination)	Identification of Impact Assessment of Threat Likelihood Assessment of Vulnerability Likelihood Risk Estimation
Control Identification Output: list of potential controls that can mitigate the risks to an acceptable level	Countermeasure Selection	Control Recommendations	Identification of Risk Measures	Formalization of Security Objectives	Evaluation of Existing and Planned Controls
Control Evaluation and Implementation Output: list of cost-efficient controls that have to be implemented to reduce the risk to an acceptable level	Countermeasure Recommendation	Control Evaluation Cost/Benefit Analysis Control Selection Safeguard Implementation Plan Development Control Implementation	Protection Strategy Development Risk Mitigation Plan Development	Determination of Security Levels Determination of Security Requirements Determination of Security Assurance Requirements	Information Security Risk Treatment (Risk Avoidance, Risk Transfer, Risk Reduction, or Risk Retention

5. PROPOSED APPROACH

This paper proposes a qualitative approach for assessing information security risks; it utilizes concepts defined in ISO27005. The approach provides an easy-to-apply information security risk analysis spanning the enterprise. With this approach:

- The list of relevant assets can be established
- Threats can be identified
- vulnerabilities can be identified
- Probability that a threat will occur can be assessed
- The impact if the threat does occur can be assessed
- The risk levels can be established
- Mitigating controls and safeguards are identified
- Implementation action plan can be developed

This approach opts for a qualitative risk analysis for applications and databases. The quantitative method evaluate, based on judgment, experience, and situational awareness:

- The exposure of the asset and frequency of the threats to get the likelihood value.

- Control is the result from the audit questionnaires based on Mehari.

Probability = (exposure + frequency) / 2 * 1 / Control

- The confidentiality, integrity and availability of information to get the impact value. These three—the loss of confidentiality, integrity, and availability—are ranked as the top business liabilities by organizations. [10]

Impact = Max of (confidentiality, integrity, availability)

  - Confidentiality concerns the protection of sensitive information from unauthorized disclosure.
  - Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
  - Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities. [1]

Approaches that can be used for qualitative analysis include, but are not limited to, internal interviews, internal surveys, internal questionnaires, storyboarding and internal Focus groups. For this project the authors chose internal surveys and internal questionnaires, because surveys and questionnaires are usually the best mechanism to accomplish data collection when you have to query a large group of individuals. There will always be cases where the recipients will need additional clarification by conducting a focus group. [10]

The approach consists of three stages:

5.1 Communication

This layer is composed of:

- Chief Information Security Officer (CISO). The CISO develops and maintains enterprise security and risk policies, oversees vendor and technology risk management, and influences user behavior.
- Users. The asset owners, prior to the focus group, they all received an electronic questionnaire or survey about the asset they use.
- Collaborators. All employees involved in the process of risk assessment.

5.2 Processing

The processing layer consists of the following steps:

- **Data collection**. This phase does not actually take a lot of manpower in terms of the security office but it does take a long time because the activity mainly relies on collecting data from different parts of the organization. [10]. Depending on how many assets are being analyzed and the turnover time for collection from other departments, this phase could last from a few weeks to several months. Its why this phase should be done through a questionnaire and survey send to those concerned. The main output for this phase is a matrix containing all the application, databases, asset owners, technical contacts, description of the asset and the results of control score.
- **Risk estimation**. Once all the necessary information has been collected the next step is to start risk estimation activities. The main activities in this phase are the calculation of the impact and probability for each threat. Using this formula RISK= IMPACT x PROBABILITY by a simple multiply the impact and likelihood scores to obtain the final risk score as shown in Table 3. The main output for this phase is the score risk.

Table 3. Sample Risk Score

E-mail system			
Threat	**Impact**	**Probability**	**Risk score**
Disclosure of confidential data	5	1	5

- **Risk assessment**. The first thing to do is make sense of the risk scores. Based on the results of the previous activity all we really have are a bunch of numbers. The challenge is to take these numbers, and transform them into something that is of a more "human readable" format by using a risk threshold chart based on the ISO 27005 as illustrated below in Figure 6. This allowed us to categorize each risk into buckets of HIGH, MEDIUM, and LOW.

By utilizing this technique, it's easy to prioritize the high risk items for remediation. This does not mean that only HIGH risk items should be remediated. The system use this risk classification method as more of a prioritization technique and what would subsequently be targeted for remediation based on this analysis is based on the organization's risk acceptance process. Some organizations may only ever address high risk items while others may choose to address all risks to some extent.

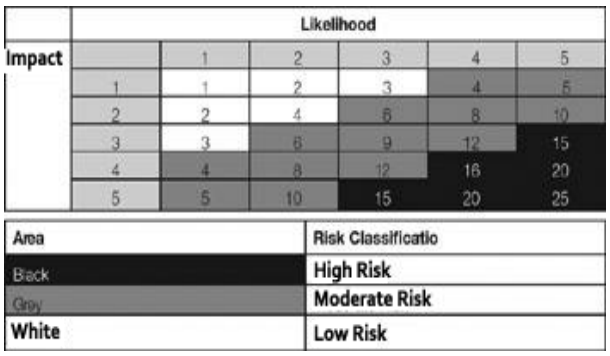

Figure 6: Risk threshold chart

- **Risk treatment**. Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories :
  - **Avoidance**. Risk avoidance involves eliminating the risk-producing activity entirely (or never beginning it).
  - **Transferring (sharing).** Risk transfer strategies turn over or share the responsibility of performing a risky activity to another party. Examples of risk transfer are transferring the liability for losses to an insurance carrier, or outsourcing an activity to a contractor with the stipulation that the contractor assume the risk.

- **Acceptance.** After all reasonable and cost effective risk responses have been taken, an organization is left with risk acceptance.
- **Reduction**. If the user chose to reduce the risk the system propose a list of safeguards measures and controls to be implemented. Controls are mechanisms that detect or prevent threats sources from leveraging vulnerabilities and thus are closely tied to likelihood as it affects the probability of a risk [10].

An action plan and a summary report are derived at the end of these steps. The action plan suggests administrative controls, technical or physical to be applied within the information system.

6. MATHEMATICAL FORMULATION OF RISK

6.1 Survey of Existing Formulations

There have been several discussions about different risk formulas, most of them derived from the guidance in the NIST SP 800-30 documentation. The following are some common existing formulations, but are not limited to:

- Risk = Probability * Imapct
- Risk = Threat x Vulnerability x Cost of Asset
- Risk = Threat x Vulnerability x Impact
- Risque = Probabilité x Gravité.

6.2 Proposed Mathematical Formulation of Risk

ISO/IEC 27002:2005 defines "Information Security" as the "preservation of confidentiality, integrity, and availability of information" and ISO/IEC 27005:2008 defines risk as "a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event" [ISO27005].

In the context of information security management systems, ISO27000 defines terms as follow:

Threat: A potential source of an incident attack that may result in adverse changes to an asset or group of assets of an organization.

Vulnerability: A weakness of an asset that can be exploited by a threat.

Control: Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be administrative, technical, management, or legal in nature.

Impact: A measure of the effect of an event.

Probability is a measure of how likely it is that particular event will occur.

Risk: The (mathematical) combination of the likelihood of an event and its impact.

Let Aj be an physical or logical IT asset, and let Ti be threat (exogenous inimical actions, activities, attacks, random events, incident, and so on) that cause an impact I(Ti,Aj) to asset Aj with probability P(Ti,Aj).

As explained in section 5:

- The impact I (Ti,Aj) to asset Aj is defined as the maximum value of (confidentiality, integrity, availability). Let C be the criteria used to determine an asset's value due to the loss of confidentiality, integrity and availability as the result of an incident. Non-repudiation, accountability, authenticity and reliability should also be considered. Note that for simplicity, this paper treats only the first three criteria. So the impact I(Ti,Aj) = Max(C1, ..,Ck).

- The probability = (exposure + frequency) / 2 * 1 / Control

Let EAj be the exposure of the asset, FTi be the frequency of the threat and RA be the result from the audit questionnaires based on Mehari.

P(Ti,Aj) = (EAj + FTi)/2 * 1/RA

Following the definition of risk described above, the risk is:

Risk = (Probability of event occurring) × (Impact of event occurring).

Risk (Ti,Aj) = P(Ti,Aj) * I(Ti,Aj)

A risk is mitigated when an asset is protected by a protection measure Ri.

The formula became Risk (Ti,Aj U Ri) = P(Ti,Aj U Ri) * I(Ti,Aj U Ri) with Risk (Ti,Aj U Ri) < Risk (Ti,Aj).

7. CONCLUSION AND FUTURE WORK

In general, the safety of SI has several objectives. Safety, then, must protect information such as company assets against data loss, disclosure or alteration to ensure continuity of business operations. This research document could form the basis for a technical project to develop an actual web-based Information Security Risk Management Tool to achieve theses objectives. In the future, this project could then also include the COBIT standard to assist organizations in exactly on 'what' must be done.

8. ACKNOWLEDGMENTS

I would like to thank to my advisor Ms. H. Medromi, PhD. Faris Sophia amd Adil Sayouti for their invaluable guidance and many useful suggestions during my work on this paper. I would also like to express my gratitude to all those who gave me the possibility to complete this paper.

9. REFERENCES

[1] By Jake Kouns and Daniel Minoli 2010. ISBN:9780471762546. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams

[2] MARGERIT – Version 2: Methodology for Information Systems Risk Analysis and Management. Book I – The Method, Published by MINISTERIO DE ADMINISTRACIONES PU´ BLICAS, Madrid, 20 June 2006 (v 1.1), NIPO: 326-06-004-8.

[3] By E. Andreas, F. Stefan, N. Thomas : AURUM : A Framework for Information Security Risk Management. Hawaii International Conference on System Sciences – 2009.

[4] By K. Hemanth, B. Sofiene, A. Logrippo : A framework for risk assessment in access control systems. computers & security 39 (2013) 86 – 103

[5] M. Raydel, F. Stefan : Automation Possibilities in Information Security Management. 2011 European

Intelligence and Security Informatics Conference. 259-262.

[6] S. Mohamed, A. Abdulkader : A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics. 2011. 107-118.

[7] S. Palaniappan, A.Rabiah, Y. Mariana : A conceptual framework of info structure for information security risk assessment (ISRA). Journal of Information Security and Applications. 2013. 45-52.

[8] By Jake Kouns and Daniel Minoli 2010. ISBN: 9780471762546. Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams.

[9] Information technology—Security techniques—Information security risk management. INTERNATIONAL STANDARD ISO/IEC 27005 First edition 2008-06-15.

[10] Mark Ryan M. Talabis and Jason L. Martin 2013. ISBN:9781597497350. Information Security Risk Assessment Toolkit: Practical Assessments Through Data Collection and Data Analysis

[11] Prentice Hall; 3 edition, 2009. Stuart J. Russell and Peter Norvig, "Artificial Intelligence: a Modern Approach".

[12] Roxanne E. Burkey and Charles V. Breakfield (eds.) 2001. Designing a Total Data Solution: Technology, Implementation, and Deployment. ISBN:9780849308932

[13] Automating System Security Audits. *ISACA Journal*, volume 1, 2004.

[14] "Autonomous and Intelligent Mobile Systems based on Multi-Agent Systems" Auteurs: A. Sayouti and H. Medromi. Book Chapter in the book "Multi-Agent Systems - Modeling, Control, Programming, Simulations and Applications", ISBN 978-953-307-174-9, InTech, April 4, 2011.