# CONSIDERATIONS REGARDING THE RISK MANAGEMENT OF SUSTAINABLE ACCOUNTING AND FINANCIAL INFORMATION SYSTEMS (SFAIS)

Roxana Maria MARIN[1], Cornelia Maria NITU[2], Anca Marta CIOBANU[3], Mihai Andrei MIRICA[4]

**Abstract.** *The exponential evolution of the electronic domain, information systems and information communication technologies globally have transformed the traditional information structures of global economic entities into recent decades, bringing new challenges including the governance of financial information systems. At the same time, they raised a number of concerns about organizational protection and risk management.*

*Faced with organizational pressures and external competition, many economic entities rush into implementing financial accounting information systems without careful planning and understanding of the concepts of security and associated risks. Therefore, rigorous risk management should not be excluded in order to implement and pilot operationally a Sustainable Accounting and Financial Information Systems (SFAIS) project.*

**Keywords:** Risk Management, Sustainable Accounting and Financial Information Systems, Security

## 1. Introduction

The key elements of the piloting of any implementation project of the SIF. in any economic entity are the organizational chart of the project, the planning of activities and the budget of the project. The organizational structure of the project, also called the technical organizational chart of the project, has the role of ensuring the consistency of the technical documentation, analysis, administrative and financial activities on the project, on the one hand, and the role of establishing the responsibilities of each member of the project team [1].

Planning of activities is relatively simple in appearance, but complex in accomplishment. After inventory of all the activities to be done, it must be positioned in time according to the availability of resources and for the continuous supply of deliverables. The budget of the project allows the value of the activities

[1]PhD, Valahia University of Targoviste, Romania (e-mail: roxybelleami@yahoo.com).
[2] PhD, Valahia University of Targoviste, Romania (e-mail: cornelia.nitu@aconaudit.ro).
[3] PhD, Valahia University of Targoviste, Romania (e-mail: marta.ciobanu6@gmail.com).
[4] PhD, Valahia University of Targoviste, Romania (e-mail: andrei_mirica@yahoo.com).

included in the project structure to be highlighted. Monitoring the budget execution of any project involves knowing all the tasks included in the project.

Like any other budget, the management of a SIC project involves some prudential measures, namely [2]: the separation of the investment expenses from the running costs, the running costs of the project; separation of intangible expenses, material expenses; verification of maintenance and operating costs allocated to investments; accurately identifying and evaluating profits and generally financial results; establishing beneficial partners of profit or other financial and / or tax benefits.

Returning to the operational pilotage issue of a SFAIS project, any project director aims and wants to realize a true pilot project and not only to coordinate the ongoing activities. In fact, the piloting of a project implies the simultaneous achievement of the following objectives: piloting the time required for the project to be carried out; economic pilot of the project; risk management; relational driving [3].

Piloting the time required to carry out the project: modernizing the SIC. for the outsourcing of accounting services is a project for cost control and profitability control. Pilotage of such a project involves a timely planning of achieving the expected results. This timing of the results is dependent on the evolution of technology and its behaviour over time.

In general, the development of such modernization projects of SFAIS generates the following trends (Figure 1): during the period of the project's approval, there is a need to carry out some activities in parallel with each other.

Throughout the course of the simultaneous activities, the management team's concern for the realization of the SIC project [4] must pursue convergence towards the same objectives of all activities undertaken; it is preferable to reduce the effects of the activities carried out with the support of the intangible assets in order to reduce the impact of the planning; the complexity of the modernization projects of SFAIS, requires the adhering partners to the project detailed planning and with well-defined deadlines; in the framework of the modernization projects of SFAIS

Planning is not only a piloting tool but also a better communication tool for evaluating effective progress towards the end of the project [5]. The cutting of time-based planning must be strictly related to resource management and commitment.

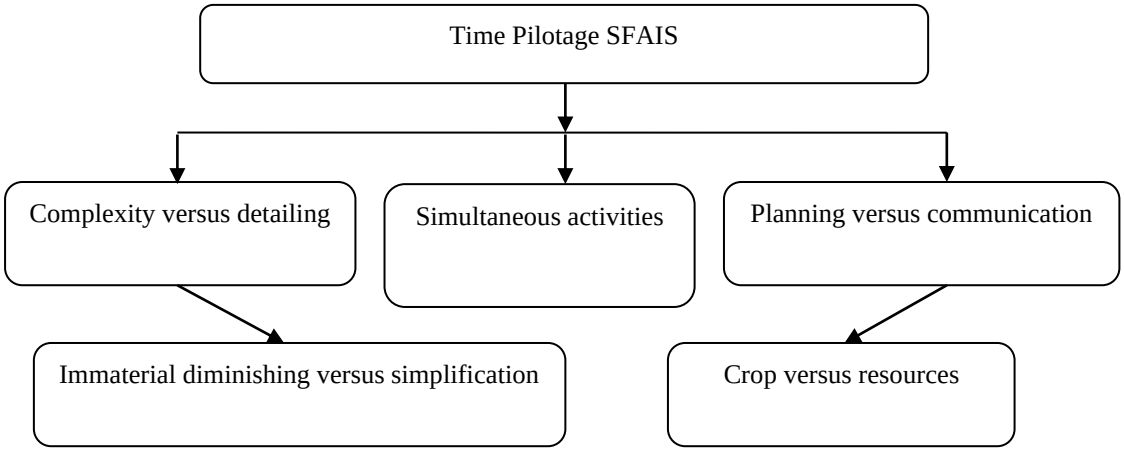


**Fig. 1.** The evolution of the centralization of computer production in the big economic entities

*Economic Pilotage*: like all the economic projects and the modernization project of SFAIS for the outsourcing of accounting services, represents for the project manager an essential concern for compliance with the costs, the observance of the deadlines, the observance of the technical specifications and the level of services provided in the contract. From an economic point of view, such a project is subject to failure to apply penalties provided for in the contract and / or other economic sanctions. In essence, the sanctions refer to exceeding deadlines and cost overruns [6]. A specific grid with criteria adapted to the project will be attached to the service contract.

*Risk management*: the risk is "the possibility of a project not being executed according to the forecast at the date set, at the cost and specification foreseen". In other words, the deviations found cannot be accepted, as a rule, by the beneficiaries. Risk assessment can be made either during project execution or at the end of the project. By their nature, the risks can be: endogenous and exogenous [7]. Endogenous risks are due to the activities carried out and are determined for the development and finalization of the projects. Exogenous risks, as a rule, do not generate disturbing factors for the good progress of the modernization project of SFAIS

Specialist literature recognizes in principle the following organizational risk typology (Figure 2): risk-person, are the risks generated by human activity to achieve the objectives of the project, but also as a result of the collaboration between the right people to achieve the project; risk-procedure, addresses the risks arising from the quality of the management tools used; product risk, concerns the

risks arising from the difficulty in knowing the characteristics of the finished product and its associated quality [8].

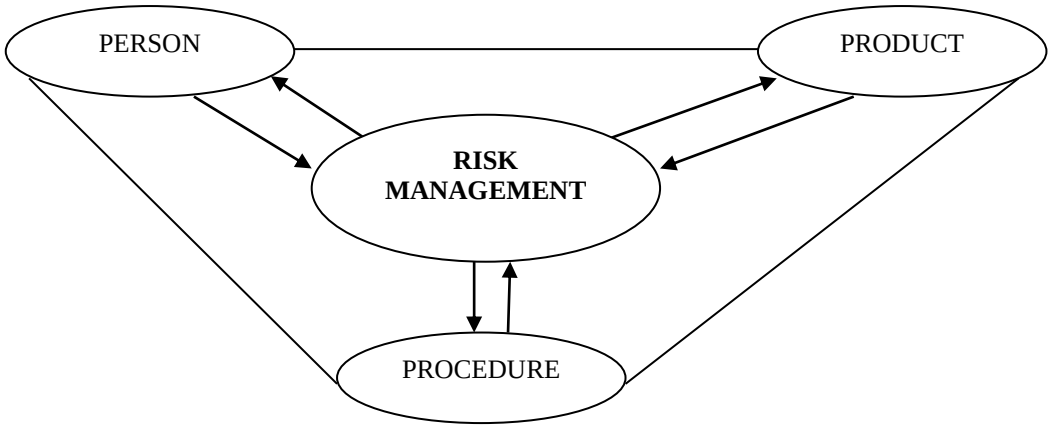


**Fig. 2.** The typology of risk in the new SFAIS

During the development of a modernization project, the managerial team can treat the emergence and behaviour of endogenous and exogenous risks. Of course, the management team can not intervene on the causes, but it can mitigate the effects, sometimes going as far as eliminating them. It is possible that some unfavourable events may compromise the project's objectives during the course of the project. In this situation, the risk can either be delayed or may be due to an erroneous diagnosis. Preventive, identifying possible risks may lead to the reduction or elimination of effects. That is why, throughout the development of the modernization project of SFAIS it is advisable to have and use a risk book, a tool strictly necessary for good risk management [9-11].

Relational pilotage often involves the need for profound changes in structure, procedures and relationships between project actors during the course of the project, all necessary to improve the sustainability of the project. Obviously, these often-ad-hoc changes mainly destabilize personnel management and human resource management [12]. Relational pilotage can intervene in the management of such a project by elaborating in detail some principles of change management.

## 2. Security of the new SFAIS for the outsourcing of accounting services

Once the new SFAIS have been adopted. are an integral part of the functioning of the economic activities adhering to this type of outsourced accounting service contract. The protection and security of the information systems of the economic entities is a permanent obligation of the state and is part of the priority policies for the protection of the economic entities and the citizens of the country [13].

On the other hand, economic entities also have the obligation to protect the malfunctions of their own information systems in order to avoid abusive use of data. In principle, the security of any information system used by the economic entity, especially the new SFAIS. for the outsourcing of accounting services, involves the initiation of certain protection and security measures and procedures regarding: asset protection; risk evaluation; identifying vulnerabilities; implementation of security policies of the SFAIS; operational security measures; control and prevention.

The assets of economic entities are composed of material and non-material items. As a rule, for goods of a material nature such as inventories, products and tangible assets, their management and control is made with some ease, with comparable inventory lists available periodically [8]. Significant difficulties are in the management of intangible assets such as intangible assets, which in most cases include software. Some of these intangible assets purchased are found in the accounting records and inventory lists [10].

Others, such as those created in economic entities, are not wholly registered in the accounts of the economic entity. In all cases, the law specifies and obliges the users of these software programs to accurately identify the ownership of these assets and to ensure secure coded conservation, specifying the owner, the publisher, the license to use, eventually the cession of the user and/or maintenance rights [14].

Obviously, databases or files for which there is no document on the owner of intangible assets may not be disposed of or sold. For all the other databases existing in the records of the economic entities adhering to the SFAIS, the protection of assets is imperative, partly subject to the laws in force, of the managers of economic entities and employees accountable according to the individual job sheet.

Concluding, the security of the new SFAIS has a clear and precise goal of proposing organizational solutions for its assets, or even appropriate techniques, capable of protecting information of any kind. In all cases, absolute confidentiality and access to information should only be ensured by authorized persons for the well-defined perimeter.

## 3. Risk Assessment of Economic Entities Utilizing SFAIS

Use of SFAIS allows the development of network activities with the specialized structures of the proprietary economic entities, but also with the customers and suppliers, respectively with any partner in a relationship accepted by the general administration. All these exchanges of information generate many risks for the SFAIS. Hence, we note the need for the economic entities benefiting from the

SFAIS to protect themselves against these risks. Of course, working tools, office space locations, workstation distances can at any time increase the risk exposure of SIF information [15]. Therefore, in the exercise of service duties all SFAIS users must make a compromise between: useful and necessary; the need for protection; the priority operational needs for information security; the need for mobility; financial availability and technical possibilities.

Risk Management and Security of the SFAIS it should be taken into account that all risk assessment approaches are made to identify potential attacks as a global approach. having in mind that any SFAIS remains exposed on the one hand due to the working tools used and on the other hand due to the involvement of the human factor, characterized by specific vulnerabilities [16]. In the approach of risk management, the risk assessment of economic entities using a SFAIS however, remains a random element.

Risk assessment also implies quantifying the impact on economic and financial performance of economic entities. These incidents may produce the following effects (Fig.3): disturbances or disruptions in the production activity of economic entities; loss of outlets; financial losses, plant and equipment and/or technology; loss of image and/or trust of customers, partners or even employees; loss of structure within the SFAIS. Once the risks are quantified, the potential risks and likelihood of occurrence are assessed in the following terms: non-objective risks, low risks, medium risk and high risk.

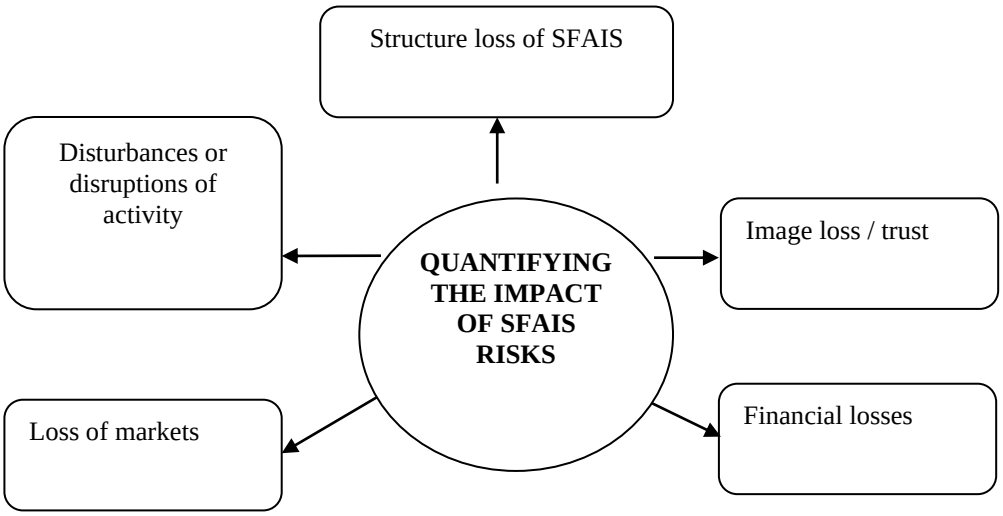


**Fig. 3.** Quantification of the impact of the risks on the economic entities using SFAIS

## 4. Identify the vulnerabilities of SFAIS

Most authors of scientific papers in information systems management consider the following vulnerabilities of SFAIS [11]: lack of professional training of the user; the use of inappropriate or unscheduled software programs by SFAIS; accessing SFAIS by unauthorized persons; natural disasters or theft of information system management.

Essentially, the security of the SFAIS, an integral part of the global security of the economic entities adhering to the SFAIS, must protect against the following forms of attacks: physical attacks, as a rule, infrastructure of the whole SFAIS; electronic attacks by launching computer programs or applications with viruses or jamming; attacks of computer programs involve the physical destruction of computer programs, physical alteration due to improper storage or exploitation, malicious intent on the part of users; malicious intervention of the human factor, modifying information from naïve or corrupt reasons; the internal intervention of people who want to have information about significant resources. For all the vulnerabilities and for the security of the new SSIF, economic entities need to develop specific safeguards and security procedures.

## 5. Implement Security Policies of SFAIS

Each adhering economic entity at the new SFAIS has to draft its own security regulations SFAIS and associated procedures to ensure a systemic and preventive approach to the potential threats posed by the risks mentioned above. It can be said that all economic entities are threatened by the existence of risk; they are not exposed to the same level. Certain aggravating factors, such as: the volume and complexity of activities; the global evolution of information systems; the nature and specific nature of activities, often competitive; organizational culture and the experience gained by economic entities in the security and protection of the SFAIS.

The package of regulations and procedures adopted by the adhering economic entity at the new SFAIS is the reference document for defining the objectives to be pursued with regard to the security of the SFAIS. For the effectiveness of these documents the following are necessary: the choice of the best methods for the elaboration and implementation of security policies SFAIS; compliance with ISO standards for the development and implementation of security policies; avoiding obstacles due to the lack of experience and maturity of the personnel involved in the elaboration and implementation of the security policies of the SFAIS; identifying and completing, whenever necessary, databases with a high or insufficient sensitivity in the implementation of the SIF; ensuring a sufficient budget to meet all the objectives of the new SFAIS; carrying out studies to find out the need for an external insurance contract against risks for the new SFAIS. It

should be noted that the whole security policy implementation system of the SFAIS must be ordained in a well-protected cycle of documents, comprising three sections: planning; protection and reaction.

## 6. Operational security measures of the SFAIS

The following operational security measures of the SFAIS are strict and obligatory: coding the entire informational circuit of the SFAIS; double coding of symmetric activities; the use of public encryption for asymmetric activities; authentication; electronic signature; providing infrastructure for asymmetric activities. The encoding of the information circuit requires the following security missions: confidentiality; login; integrity.

All software must have the contents of confidential documents illegible for all who do not have the passphrase. Double coding of symmetric activities involves the existence of at least two people in the user group who agree on an access password in the system. The use of public encoding is a practice used for asymmetric activities, for which the recipient is the only one who can use a password for decoding.

Authentication is usually used in communications between two user users accepted by SFAIS, for which each assumes the role of interlocutor and verifier. The electronic signature, introduced in 2001, allows for increased security of exchanges by electronic mail. The use of an electronic certificate allows inter alia: authentication of the emitter; the integrity of the transmitted data packet; avoid rejection of data exchanges.

The provision of infrastructure is mandatory for the procedures for operating and administering the secure electronic certificate. All asymmetric activities require complex databases and software programs that are password-protected at all ends of the new SFAIS 's networks, with password exchange insurance.

## Conclusions

We can conclude that in order to support and implement a Sustainable Accounting and Financial Information System, risk management is the key process that enables business entity managers to balance operational and economic costs through protective measures while at the same time gaining benefits by protecting information systems and financial data accounting.

# R E F E R E N C E S

[1] Dhillon G, Backhouse J. Technical Opinion: Information Security Management System in the New Millennium. Communications of the ACM. 2000 Jul 1; 43 (7): 125-8.

[2] Hubert, P., Systemes of Management Information, Ed. Gualino, Paris, 2008.

[3] Boehm BW. Software risk management: principles and practices. IEEE software. 1991 Jan; 8 (1): 32-41.

[4] Bandyopadhyay K, Mykytyn PP, Mykytyn K. A framework for integrated risk management in information technology. Management Decision. 1999 Jun 1; 37 (5): 437-45.

[5] Cardona OD. The need to rethink the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management. InMapping vulnerability 2013 Jun 17 (pp. 56-70). Routledge.

[6] Cucui I, Ionescu CA, Coman MD. The binomial of modern management accounting: advanced production technologies–advanced cost calculation methods. Academy of Romanian Scientists, Vol 2, No.1, 2016:7.

[7] Stoneburner, Gary, Alice Y. Goguen, and Alexis Feringa. "Sp 800-30 Risk Management Guide for Information Technology Systems." (2002).

[8] Coman, M., Coman M.D., The Integration of TIC in the Accounting Information System of Small and Medium-Sized Enterprises, Valahian Journal of Economic Studies 4, no. 2 (2013): 7.

[9] Coman DM, Horga M, Coman DM. The Information Integration in the SMEs. Valahian Journal of Economic Studies. 2016 Dec 1; 7 (2): 69-78.

[10] Coman DM, Coman MD, Horga M. Information Technology for Fraud Detection. Valahian Journal of Economic Studies. 2014 Jul 1; 5 (3): 85.

[11] Conway RW, Maxwell WL, Morgan HL. On the implementation of security measures in information systems. Communications of the ACM. 1972 Apr 1; 15 (4): 211-20.

[12] Ionescu CA, Coman MD, Cucui G, Stanescu SG. Supply cost minimization using mathematical models and methods of optimization. Journal of Science and Arts. 2018 Apr 1;18(2):397-404.

[13] Costi, B., Accounting information in the decision-making process, Studia Universitatis Vasile Goldis Arad, Economic Sciences Series, Year 2, Part 2, 2010.

[14] Cucui G., Cucui I., Anica-Popa I., Using web mining technologies to improve competitive intelligence capabilities: a historical perspective, 2010 Transformations in Business & Economics. Supplement A, Vol. 9, p461-471

[15] Kankanhalli A, Teo HH, Tan BC, Wei KK. An integrative study of information systems security efficiency. International Journal of Information Management. 2003 Apr 1; 23 (2): 139-54.

[16] Oprea, D., Analiza şi proiectarea sistemelor informaţionale economice, Ed. Polirom, Iaşi, 2003.

[17] Stoneburner, Gary, Alice Y. Goguen, and Alexis Feringa. "Sp 800-30. risk management guide for information technology systems." (2002).