Construction of the First Component of a New Information System Security Governance Framework: 4D-ISS Risk Management Model

Mounia Zaydi, Bouchaib Nassereddine

Abstract— **nowadays, organizations are looking for ways to grow their revenues, gain a competitive advantage and improve their business. To remain competitive and consolidate their position in the market, companies should use and process all the information they have to better support their missions. In order to achieve this, managers must take into account the risks that weigh on the business, especially risks related to information system security (ISS), and they should be able to minimize their impact on the organization. Information system security risk management (ISSRM) helps managers to control business practices and improve business processes. However, it remains a difficult concept to put in place and maintain. In this sense, we propose a new concise, clear and methodical model of ISSRM that is broken down to four phases and conform to continuous improvement approach.**

Index Terms—**ISS process, information system security, risk management, compliance, governance, ISSRM**

I. Introduction

The information system security (ISS) become a point of increasing concern; it has now reached a critical point where the growth and functioning of the entire economy depend on it. The combination of factors explains that the security of information and communications is now the top priority for any organization information system (IS). More and more organizations need mobility, globalization and application outsourcing to manage the constraints of their business. This has considerably facilitated illegal and remote access to valuable economic information. Such security challenges require the use of an information security governance program, with a systematic process of ISS risk management and regulatory compliance. With this in mind, organizations are increasingly required to identify their organizational needs for information security requirements, including an effective information security management s

system (ISMS) [3] while staying in compliance with the law and reglementations, based on risk management, and then to master governance of its system. To sum up, it is necessary to use a holistic approach that is, at the same time, adapted to the organization's environment and aligned with the organization's overall risk management approach. This paper lays down the conceptualization of the ISSRM at first, and proposes a new process involving functional business units throughout its deployment. The rest of the paper is divided into seven sections: the first one is about the discipline of ISSRM, its concepts and its foundations, as well as its contribution to create value in the target organization, the second section is devoted to the previous researches in this field, the third section proposes a new process of the ISSRM aligned with the continuous cycle of improvement in this case the PDCA [1], [2] used in the standards of management systems, such as ISO 27001 [3] in the Information Security. This will provide the approach with flexibility and pragmatism to be used in all circumstances and especially in organizations where everything changes constantly. The PDCA is a guide that adapts to all types of organizations and situations. With that in mind, the fourth section aims to conceptualize this process using the BPMN notation and to properly carry out its implementation; Section 5 will follow up by specifying the prerequisites and requirements for a successful implementation leading to a discussion; in section 6, to explore the advantages and limitations of this process. Finally, the seventh section will present futures actions to consider.

II. Related work

An analysis conducted by the OCEG [4] in 2015 focuses on the several approaches of risk modeling as well as its concepts; it examines a selection of well-established paradigms for the risk modeling information security. However, the scope of that study differs from ours as it covers a wide range of risks, including strategic, financial, and operational and project risks; while our research focuses specifically on the security risks of information systems that affect their essential pillars, which are confidentiality, integrity, non-repudiation, authentication, and information availability. Especially since this study does not propose a conceptual model. Barateiro and al. [5] propose an alignment strategy between risk management, governance and enterprise architecture activities to provide systematic support for mapping and tracing the identified risks for artifacts modeled in an environmental assessment. The

Manuscript received April 4, 2018; revised April 16, 2018. This work was supported in part by IR2M Laboratory at the Faculty of Science and Technology in Settat, Morocco.

Mounia ZAYDI is currently towards her PhD degree in information system security governance at Hassan 1st University Settat, Morocco. (Phone: 212-666-940-289; e-mail: m.zaydi@uhp.ac.ma).

Prof. Bouchaib NASSEREDDINE is an associate professor at Hassan 1st University in Morocco and he is the Head of Master of Computer Science at the Faculty of Sciences and Technology, Hassan 1st University, Settat, Morocco (e-mail: nassereddine_bouchaib@yahoo.com).

document proposes a risk management framework, including an XML- specific language for RM (Risk-DL) and clearly explains the link with ISO 31000 [6] [7].Innerhofer - Oberperfler and Breu [8] present an approach to assess and analyze risks related to information technologies, organizations and projects. The purpose of the approach reduces the gap between the point of view of stakeholders and security management. They propose information security models according to a meta-model. Using the same approach, Ertaul, L. and Sudarsanam, R [9] propose using Zachman's framework to define and design tools to secure an organization. In order to implement security planning especially for IT.SABSA [10] is a methodology for developing a risk-based enterprise information security and information assurance architectures and for providing security infrastructure solutions that allow critical business initiatives. The methodology is based on the SABSA model, based on the Zachman Framework [9], adapted in some ways to the security vision. The Open Enterprise Security Architecture Guide [11] is a guide providing a comprehensive overview of security issues, principles, components and concepts. The five previous references develop conceptual or methodological advances linking the business to ISSRM, but none of them proposes an integrated and complete model for both business and information security. Goldstein and Franck have proposed a series of 23 requirements, their modeling approach focuses on modeling and design information security management concept [9].They also integrate into their approach the security risk with multiple perspectives of the enterprise [12], they extend their exclusive modeling framework (MEMO) and its set of domain-specific modeling languages (DSML), with the aim of supporting the management of IT security. With that said the common goal of defining a DSML that improves an existing method enterprise modeling. However, their scope is broader than ours, simply because they review multiple business perspectives, while we focus on the asset perspective. Our conceptual model would be the first brick of our ISS Governance Framework that could be adopted with any technology. CORAS [13] is a risk analysis approach based on ISO 31000 [7]. It is based on the idea that graphics models are actively used throughout the risk analysis process to embrace various analytical tasks and activities, and to exploit results [14].However, CORAS introduces its own diagram types and does not rely on business models to perform the ISSRM. The goal of our research project is to build a conceptual mapping of the processes that compose our final model of ISS governance, namely, risk management, compliance and governance, in order to take advantage of risk as an instrument to manage business strategies that are often not synchronized with those of the IS. Although conceptualization and mapping are widely linked, we focus here on conceptualizing this new security risk management process.

In conclusion, all previous research has provided initial and promising contributions to manage the potential ISS risks that affects the assets of the organizations. However, we highlight the lack of processes that have become an ISSRM model and are integrated with the organization's vision of ISS governance; to help align the business with IS strategy.

III. Information System Security Overview

To fully grasp the ISSRM, its aims and its limits, we start by explaining the notion of risk, its underlying concepts, its foundations and its management cycle.

A risk can be defined as a combination of the likelihood of damage and its severity [15]. Information Security Risk: Is the possibility, that in presence of a given threat exploits the vulnerabilities of an asset or group of assets and harms the organization, Assets are defined as all resources that are valuable to the organization while being fundamental for its proper functioning. There are two categories of assets, those related to the business and those related to the IS. As for business assets, we mainly find information (for example credit card numbers) and processes (such as transaction management or account administration).The business assets of the organization are often entirely (or almost) managed through the IS, which leads to a dependence of these assets toward the latter. This is called "system assets". Systems assets include technical elements such as hardware, software and networks, but also the environment of the IT system, such as users or buildings. This set that forms the basis of IS [17] [22]. The risk is measured in terms of the combination of the likelihood of an event and its consequences. It constitutes the probability of exploiting a vulnerability in the current environment, resulting in a certain level of loss of confidentiality, integrity, and / or availability of an asset, a group of assets, or the whole organization as shown in the diagram below "figure 1".

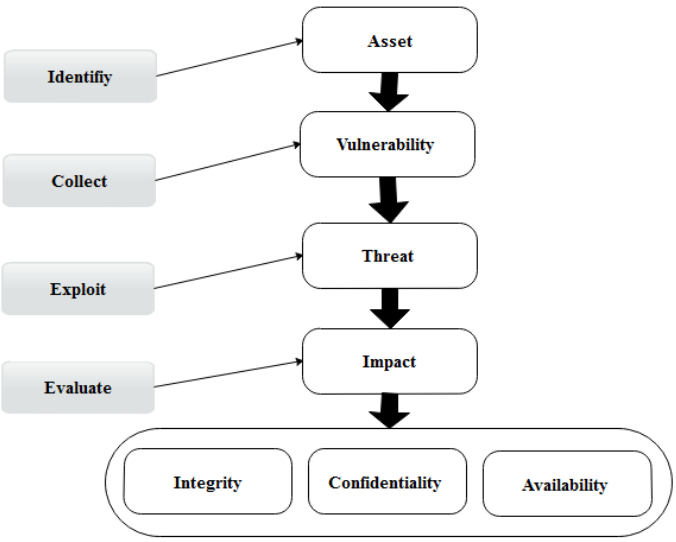

Fig. 1. Risk Modeling

A complete definition of risk seems necessary to identify (1) the threat actor, the human or non-human entity that exploits a vulnerability; (2) The vulnerability defined by the National Institute of Standards and Technology (NIST) as a state or a weakness of the security procedures, controls, technical, physical or other, likely to be exploited by a threat (3) The threat; defined by ISO 27002 [23] as the cause of potential impact on the organization; and (4) Impact is the consequence of the undesirable results. (5) Affected asset - information, process, technology; is the most important component of risk. Assuming that the endangered asset cannot be eliminated, the only risk component that can be controlled is vulnerability. In order to be able to estimate the level of risk and then to choose an appropriate treatment strategy, including [17] ***Avoidance*** (eliminate, withdraw from or not become involved) ***Mitigation*** (optimize,

ISBN: 978-988-14049-0-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

mitigate and attenuate), ***Transference*** (Sharing, outsource or insure), ***Acceptance*** (accept knowingly).

Finally choose and put in place the necessary controls to reduce the risk to an acceptable level, we will be referring to the most recognized risk equation in the world of ISSRM [18]:

RISK = VULNERABILITY * THREAT * IMPACT

The risk management of the ISS is therefore the process of identifying, understanding, assessing and mitigating risks - and their underlying vulnerabilities, and the impact on information, information systems and entities. In addition to identifying risks and risk mitigation measures, a risk management method and process will help to: identify key information assets. A risk management program can be built also to identify critical people, business processes and technology resources, in one hand understand why selected critical assets are required for operations, to ensure the fulfillment of the organization's mission and continuity of their operations in the other hand.

IV. Proposition of a new ISSRM process: 4D-ISS

The purpose of this research project, is to have a powerful ISSG Framework that optimizes the management of the ISS, from this perspective it has proved essential in our approach to establish the components of the ISSG in Generic processes that can adapt to any organization, regardless of technology, industry and size, which will eventually be merged into one unified process. This paper proposes the first process of our Framework in this case, 4D-ISS, which inherits a set of foundations of good practices in the field of ISSRM.

The ISSRM wants to be a transversal pillar of IS management, its alignment with business strategies presents a major challenge. Having a cyclical process, continuous in time that adapts to the continuous improvement approach presents itself as a good candidate to respond to this situation. It is within this vision that our process will initially meet this alignment theoretically and then after, it will be evaluated after its implementation. This process is broken down into four major phases called 4D-ISS, ***(D1)*** Define risks and its different components. ***(D2)*** Direct them in terms of their priorities and criticality to bring relevant treatment. ***(D3)*** Deploy the controls of safety, and ***(D4)*** decide on the risk-management strategy that remains after the implementation of the so-called "residual" mitigation measures in order to evaluate the measures implemented. The iterative approach schematized at the level of figure 2 below.

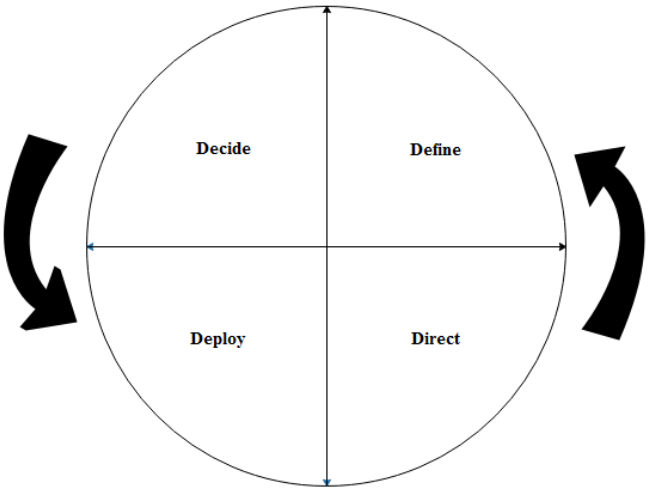

Fig. 2. Information system security risk management proposed process – 4D-ISS

A. *Strategy location of IDS agent*

The new process consists of four components; "Define" for the identification, evaluation and prioritization of risks. "Direct" for controlling risks and choosing the most appropriate treatment strategy. (Acceptance, transfer, mitigation or refusal), with (organizational, technological and management) measures. "Deploy" for the effective implementation of the measures chosen during the "Direct" phase and the "Decide" phase, is the measurement and evaluation phase of the relevance and the degree of resistance of our measures, facing the various attacks likely to harm the system, and it is during this phase that we decide on the residual risk.

The assignment of defining roles and responsibilities is a critical success factor to ensure a clear and focused implementation of the 4D-ISS process due to the need for interaction between groups and division of responsibilities. The R.A.C.I matrix specifically designed to provide responsibility management information. It indicates the level of responsibility each human resource has with regard of each activity carried out in a company; taking in consideration of the work to the resource that must approve or receive notification regarding the tasks done [19]. Figure 3 shows the ISS- risk management methodology flowchart.

B. *"Direct" in the 4D-ISS process*

Now comes the time to address the most important risks by identifying appropriate actions to minimize them. In the previous phase, the security risk management team identified the assets, potential threats, vulnerabilities that could be exploited, and the existing controls that would protect these resources. Based on the results of the "Direct" phase, we get to choose an appropriate action to conduct each risk, define the functional requirements (instructions describing the functionalities required to mitigate the risks), propose the controls that are more likely to minimize the level of risks, evaluate these controls in order to determine the degree of possible minimization of the risks associated to the assets identified, estimate the costs of each proposed control and then select the final solutions to be implemented from the analysis costs.

ISBN: 978-988-14049-0-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

C. "Direct" in the 4D-ISS process

Now comes the time to address the most important risks by identifying appropriate actions to minimize them. In the previous phase, the security risk management team identified the assets, potential threats, vulnerabilities that could be exploited, and the existing controls that would protect these resources. Based on the results of the "Direct" phase, we get to choose an appropriate action to conduct each risk, define the functional requirements (instructions describing the functionalities required to mitigate the risks), propose the controls that are more likely to minimize the level of risks, evaluate these controls in order to determine the degree of possible minimization of the risks associated to the assets identified, estimate the costs of each proposed control and then select the final solutions to be implemented from the analysis costs.

D. "Deploy" in the 4D-ISS process

During this phase, the minimization risk managers use specified controls during the "Direct" phase. The success of this phase lies in the holistic approach minimization risk used when implementing control solutions.

Those managers must take into account the specifics of the entire IT system, all functional business units or even the entire company when planning, acquisition and deployment of risk minimization solutions.

E. "Decide" in the 4D-ISS process

In the "Decide" phase, the security risk management team must provide a formal summary of the current state of risks to which the organization is exposed. The company continues to conduct business activities alongside the risk management cycle. Therefore, the progress of risk minimization can be evaluated in action aiming at reducing the risks on the company to an acceptable level. During this phase, the security risk management team prepares the "Safety Risk Assessment Sheet", or a summary of the risks to the organization, that can communicate the project's progress to people involved. The evaluation sheet also verifies that the concept of risk management has been integrated into IT processes.

V. Conceptualization and Modeling of 4D-ISS Process

Before proceeding with the 4D-ISS process, the organization must assess its maturity level according to ISSRM. Without a formal strategy or process managing information security risks, it will face many difficulties implementing all aspects of the process at once. Even organizations with formal strategies and guidelines that are already well integrated by most of its collaborators are sometimes slightly out of date. Therefore, an assessment of the degree of maturity of the target organization, in terms of risk management is paramount. In this sense, the organization has the free choice to personalize a grid evaluation, or to make use of a framework, in this case, COBIT [20], Table 2, represents the five levels proposed by the latter in order to evaluate maturity according to ISSRM.

In the case where the organization is still relatively inexperienced, it is best to display the implementation of the process over several months, for example, by controlling it within a silo; functional business unit mastered; until several cycles completed. Once the effectiveness of the process is demonstrated through this pilot program, the security risk management team can then progressively extend it to other silos and then adopt it across the entire organization.

Any participant in the implementation of the 4D-ISS process, must be aware of the problem posed by the security of its information system, and should be able to position itself precisely while taking into consideration the various issues that revolve around its current security situation, in particular, (a) the definition of the expected objectives of the IS security of their organization and their communication to the collaborators, (b) the designation of the IS Security Officer (ISSO) status,(c) the identification of the IT vulnerabilities and the evaluation of the corresponding financial losses,(d) the choice of maximum threshold of the accepted risk that can't impact negatively the organization's sustainability, and finally in case of unavailability (c) he must be able to determine the time required to recover normal activity.

A. Discussion

The concept of "integrated ISS risk management" is one of the main elements in assessing the maturity of the organization in terms of information security.

It is from this perspective that we seek to model a coherent, methodical and well-structured process, that allows later an integration into another process that will ensure the compliance of the IS of the organization holding this process.

The purpose is to design a governance process model of the ISS, which covers all functional aspects of the organization, which will ultimately be converted into a framework.

We are in the process of defining the key processes of this model, which are the risk management, the compliance and the actual governance of the ISS.

The definition of the first process is complete, it has been called 4D-ISS, its Eligibility conditions and the actors involved in its implementation are well defined. The test of its effectiveness will be the subject of a study case that will cover a field that is different from what is usual with all current GRSI methods and standards.

Our experiment will be at the level of higher education, more precisely the scientific research units in Morocco.

Next, we will define a compliance process that will be merged with the 4D-ISS process. Its purpose is to check that the latter is applied in compliance with applicable legal, regulatory and contractual requirements as well as with the policies and regulations of scientific research. Then after we plan to add a 4th dimension that is the "technology intelligence" in a transversal way, in order to intervene at the level of the three pillars as we have already published [22].

ISBN: 978-988-14049-0-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

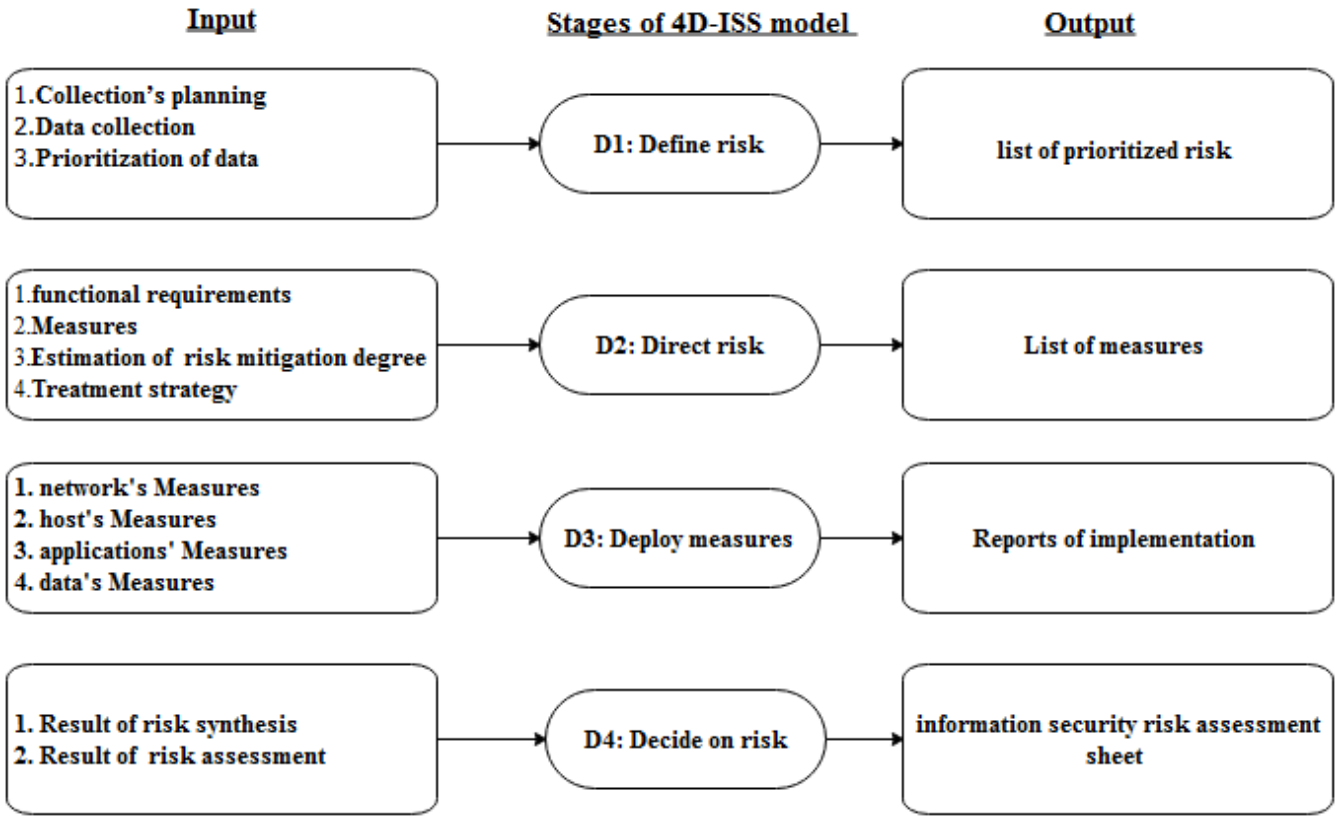

Fig. 3. ISS- Risk management Methodology flowchart

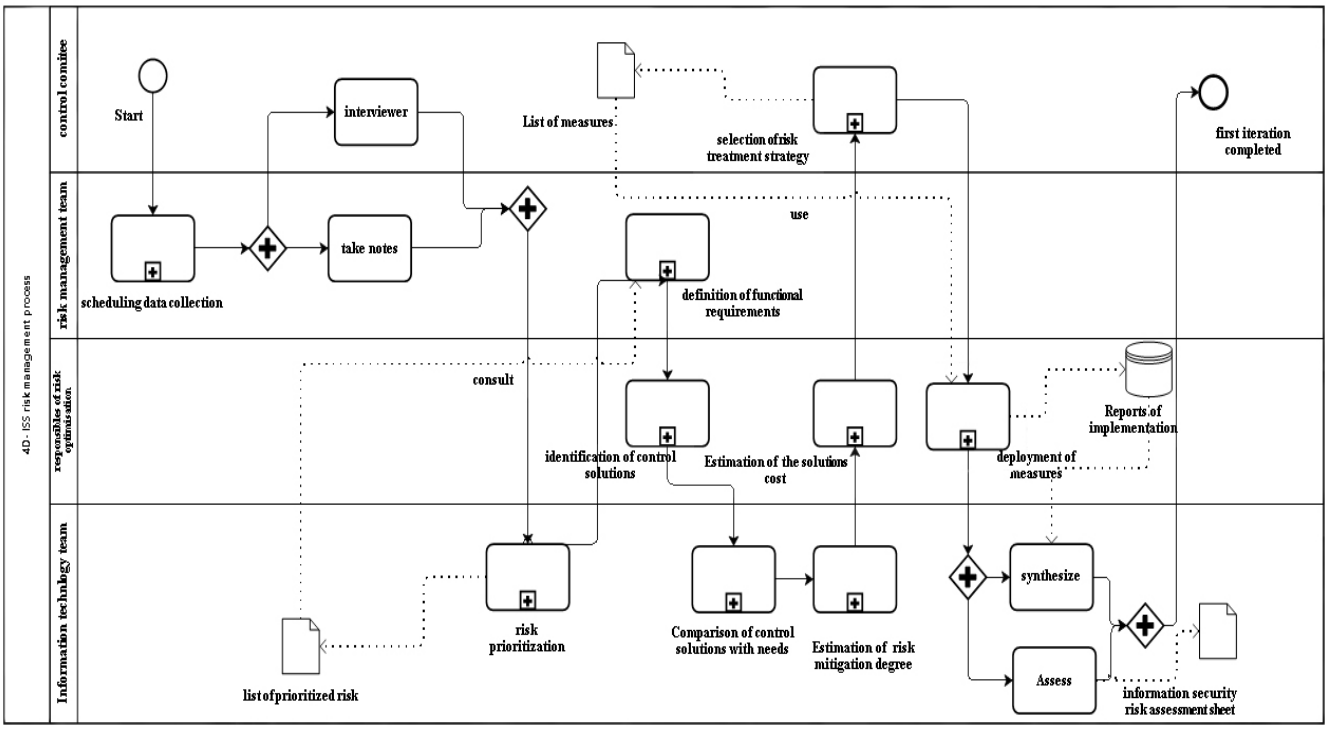

Fig. 4. Collaboration diagram of 4D-ISS process

ISBN: 978-988-14049-0-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

VI. CONCLUSION AND FUTURE WORK

At this level, 4D-ISS is a proactive approach designed to help organizations of all sizes to protect themselves against the risks of ISS that can lead to performance degradation. Our 4D-ISS process allows an organization to conduct its business in the most cost-effective manner, giving a clear and consistent program to organize and classify its resources, keeping its risk level to the minimum. The tangible results of this process will be displayed once these controls are in place, which will reduce the risks to an acceptable level. The acceptable level of risk and the adopted approach to risk management vary from one organization to another. Many risk management models are used today; there is no ideal solution. Each model requires a compromise between precision, resources, time, complexity and subjectivity. An organization needs to invest in a safety risk management program involving the implementation of a reliable and concrete process, and the definition of roles and responsibilities to be able to prioritize, take the necessary actions to minimize risks and address critical vulnerabilities and threats that may jeopardize its business activities.

The next stage of this project is to automate the 4D-ISS process, to integrate it into the intranet of the target institution to automate the asset mapping and collect, their values as well as their owners and, then after a test will be planned for the integration. the second phase of the project focuses on the proposal of a generic process; it's will be the second brick of our ISSG framework; consists of ensuring compliance to contractual obligations, law and reglementation, finally we will built our ISSG framework.

REFERENCES

[1] Sokovic M, Pavletic D, Pipan KK. Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS. Journal of achievements in materials and manufacturing engineering. Nov 1; 43(1):476-83, (2010).

[2] Deming WE. Elementary principles of the statistical control of quality: a series of lectures. Nippon Kagaku Gijutsu Remmei; (1950).

[3] ISO /CEI 27001, “Information technology — Security techniques — Information security management systems — Requirements,” (2013).

[4] Band, I., Engelsman, W., Feltus, C., Paredes, S.G., Hietala, J., Jonkers, H., Massart, S.: Modeling Enterprise Risk Management and Security with the ArchiMate®. Language, the Open Group (2015).

[5] Barateiro, J., Antunes, G., Borbinha, and J.: Manage Risks through the Enterprise Architecture. In: 45th Hawaii International Conference on System Science (HICSS), pp. 3297–3306 (2012).

[6] ISO 31000: Risk management—Principles and guidelines. International Organization for Standardization, Geneva (2009).

[7] Mayer, Nicolas. "Model-based management of information system security risk." PhD diss., University of Namur, (2009).

[8] Leitch, M., 2010. ISO 31000: the new international standard on risk management. Risk analysis, 30(6), pp.887-892 (2009).

[9] Innerhofer-Oberperfler, F., Breu, R.: Using an Enterprise Architecture for IT Risk Management. Presented at the Information Security South Africa 6th Annual Conference (2006).

[10] Ertaul, L. and Sudarsanam, R. Security Planning Using Zachman Framework for Enterprises (2005).

[11] Sherwood, J., Clark, A., Lynas, D.: SABSA ® Enterprise Security Architecture (2010).

[12] Goldstein A, Frank U. A language for multi-perspective modelling of IT security: objectives and analysis of requirements. In International Conference on Business Process Management (pp. 636-648). Springer, Berlin, Heidelberg, (2012).

[13] Goldstein A, Frank U. Components of a multi-perspective modeling method for designing and managing IT security systems. Information Systems and e-Business Management. 14(1):101-40, (2016).

[14] Lund MS, Solhaug B, Stolen K. Model-driven risk analysis: the CORAS approach. Springer Science & Business Media; (2010).

[15] Deodatis G, Ellingwood BR, Frangopol DM, editors. Safety, reliability, risk and life cycle performance of structures and infrastructures. CRC Press; (2014).

[16] V. Lalanne, “ Gestion des risques appliquée aux systèmes d’information distribues,” (2013).

[17] Bloch L, Wolfhugel C. ‘IT Security : Principles and Methods for IT Directors, CISOs and Administrators ‘, ‘Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs’. Editions Eyrolles; 2013 May 15.

[18] ISO 27005 LOGICAL C. Information technology–Security techniques–Information security management systems–Requirements (2013).

[19] Mayer N, Humbert JP. ‘Risk Management for Information System’, “La gestion des risques pour les systèmes d’information”. Magazine MISC. (2006).

[20] C. Cabanillas, M. Resinas, and A. Ruiz-cort, “in BPMN Models Using RACI Matrices,” pp. 56–57, 2012.NIST Homepage, https://www.nist.gov, last accessed 2016/10/27.

[21] Mayer N, Humbert JP. La gestion des risques pour les systèmes d’information. Magazine MISC. (2006).

[22] Zaydi, M. and Nasserddine, B., Information system security governance: Technology intelligence perspective. In Advanced Communication Systems and Information Security (ACOSIS), International Conference on (pp. 1-6). IEEE (2016).