Journal of Management and Social Studies

Volume 2, Issue 2, February 2024, pp. 05-21

Copyright© 2023, CSTIJ Publication

homepages: http://cstij.org/

Toward a new integrated approach of information security management based on Governance, Risk and Compliance

Mounia ZAYDI[1], Bouchaib NASSEREDDINE[2]

[1] Faculty of Sciences and Techniques, Hassan 1st University, Settat, Morocco

[2] Faculty of Sciences and Techniques, Hassan 1st University, Settat, Morocco

*Corresponding author's E-mail: *1 zaydi.mounia@gmail.com, 2 nassereddine_bouchaib@yahoo.com*

ABSTRACT

The Information system security ISS has become the main lever of the world economy, is the key of value creation, and its inaccessibility has a technical, human and financial impact. Mastering this discipline lies by (1) securing information content against information system security risk (ISS risk management), (2) defining the stakeholders those contribute to its management and its control (ISS Governance) and (3) complying with the applicable laws, and regulations in force (ISS Compliance). ISS-GRC has emerged in the world of business and information technology remains a difficult subject to demystify. Researchers and professionals have studied this worldwide scourge from different perspectives. From an academic angle, studies have been made of the decision making's structures, impact factors and characteristics of the ISS-GRC. Professionals focused on the mechanisms and technical tools of the ISS-GRC. Despite research progress on ISS-GRC, this concept remains premature upon implementation and lack organizational involvement. To develop this approach, first it is essential to handle the three disciplines each as a separate entity, to analyze the existing studies of the integrated ISS-GRC. In a second level, authors have to explore the business benefits of their cohabitation, and then construct an integrated model of ISS-GRC and this all, by merging the three entities in a transverse way.

Keywords: Information system security, risk, ISS-Risk, ISS-Gov, ISS-GRC, and ISS-Compliance.

1. Introduction

Establishing a strategic vision of the relationship between ISS-governance, ISS-risk management and ISS -compliance with internal policies, laws and regulations, has become a critical concern for the Information Systems Department (ISD), which is currently the main lever of value creation and contribution to the overall organization performance. The ISS-Gov monopolizes this strategy and becomes more and more critical and urgent.

The main stakeholders involved in this approach are the executive management (EM), which designs the company's strategy, the ISD that ensures that it is operational, and the Head of Information Systems Security (CISO). Its role is to control information technological risks, but also to help improve the performance of business processes.

These stakeholders have a multitude of references, and methods of best practices namely, ISO 35800 and COBIT for the EM, ITIL for the ISD and the ISO27K family for the ISSR.

The goal is to merge these best security practices into a single integrated approach that will be translated into a framework for the ISS-GRC. This is to lower the cost of maintaining acceptable levels of security, to effectively assess and manage risks, to mitigate overall risk levels and to comply with applicable regulations.

In this research, the authors face a double challenge, on the one hand how to meet the needs of organizations for an integrated approach to cover their business and ISS needs, and this in terms of ISS-Gov governance, ISS-Risk and ISS-Compliance ISS-GRC, on the other hand, how to raise the automation issue of the various ISS-GRC processes. The rest of the paper is arranged as follows. Previous work on ISS-GRC proposed in the literature is discussed in Section 2. Section 3 describes the detailed description of the proposed methodology. Section 4 is devoted to the first phase of the methodology, which consists of identifying and classifying the different building blocks of the model. Section 5 deals with the analysis of the different components identified and the final proposal for each brick that will form the ISS-GRC unified model. Section 6 describes the final phase, consists of merging the different processes into a single process model, to build the desired integrated ISS-GRC approach. Section 7 for discussion. Finally, Section 8 presents conclusions and future research directions.

2. Literature Review

Recent studies on the GRC have identified the lack on scientific researches on a holistic and integrated approach to IT-GRC, especially on information system security (Χατζηπουλίδης, 2015). Although the field of GRC has been emerging, particularly in recent years, most of the frameworks developed so far cannot provide a clear view of the integrated ISS-GRC and its implementation. More specifically, these frameworks cannot provide guidelines for organizations with respect to the implementation of ISS-GRC processes. And how can they make benefits, by aligning the SSI infrastructure with their business objectives. In this sense, authors distinguish a few frameworks presenting models related to integrated GRC solution; however, it remains heavy to include the ISS processes. The Open Compliance and Ethics Group (OCEG) presents the OCEG GRC360 capacity model, consisting of 9 categories and 29 sub-elements,

each of which has sub-practices (oceg,2007), (Racz, Seufert, weippl, 2010). The model provides an overview of GRC practices and activities on the business process that affect strategy, business objectives in terms of governance, compliance and risk management; however, the model don't distinguish operational processes from managerial processes (Racz, Seufert, weippl, 2010). Mitchell (Mitchell, 2007) also proposes a framework to stimulate "principles-based performance," which is essentially the very first step in the GRC360 capability model. Rasmussen (Rasmussen, 2009) who refers to the “Corporate Risk and Compliance View” and proposes the OCEG capability model as a corporate architecture for GRC also discusses the OCEG capability model. And this without including the ISS-GRC activities. Paulus (Paulus, 2009), describes "GRC Reference Architecture" with a model that consists of four main phases: (1) requirement modeling, (2) status inquiry, (3) improvement of the situation, (4) crisis and incident management. Its model is considered easy to understand, but it does not include in-depth and basic analysis for the implementation of GRC, and it also neglect ISS processes. The "Strategic Framework for the GRC" (Frigo, Anderson, 2009) describes "policies and risk appetite" and these together broadly define common goals to add value and protect common processes associated with GRC practices from a business perspective. It can strategically help organizations manage their GRC initiatives; however, the framework mixes processes with organizational units and objectives and can sometimes be difficult to follow, especially for organizations that are not mature in terms of risk management. Tapscott (Tapscott, 2006) presents a new GRC approach, split into four core values for target organizations to achieve "trust," which remains the primary goal when adopting an integrated approach to the GRC. This approach, while easy to follow, doesn't translated into a process model that helps organizations gain a broader view of their GRC activities. Another research, conducted by PricewaterhouseCoopers (PwC, 2004), develops an operational model for the GRC without including those dedicated to the ISS; however, this model also mixes in each of the four stages that compose it, the organizational entities, the activities and relationships involved in these steps. This operational model (PwC, 2004) combined with the four core values presented by Tapscott (Tapscott, 2006) could develop essential tools to the analysis of the business GRC implementation process. Wiesche et al. (Wiesche, Schermann, Krcmar, 2011) presents a GRC framework linking GRC to accounting information systems, which gave rise to the "Framework for GRC IS Value Drivers". This framework is primarily in the area of accounting and not an ISS approach. In addition, Racz et al. (Racz, Seufert, Weippl, 2010) translates the GRC's definition into a "frame of reference for GRC research" that describes a definition in a figure that is the basis of research in the field of GRC business. (Gericke, Fill, Karagiannis, Winter, 2009) also present a framework for the GRC. The main objective of this framework is to analyze the GRC implementation with the situational method while identifying the fragments of the method. The method is divided into five categories: (1) conceptual, (2) strategic, (3) organizational, (4) technical and (5) cultural. The basis of this research is the deployment of the GRC solution, rather than the successful implementation of the GRC software. This framework will be used for the development of an integrated ISS-GRC framework. More recent research in the GRC’s area

includes the "Conceptual Model for Integrated Governance, Risk and Compliance" by Vicente and da Silva (Vicente, da Silva, 2011), which presents the key concepts and functions of the GRC, using OCEG MODEL (oceg, 2007). The conceptual model can be used to better understand the GRC integration and as a structural tool for the analysis framework of the establishment of integrated GRC process (Spanaki,Papazafeiropoulou, 2013). In conclusion, a set of references and models has been established for the GRC business, and sometimes IT-GRC, but none of them offers an holistic approach and incorporates for the IS security aspect. The models and standards used for the construction of these approaches are generally oriented business, economy, HR, IT-Business and in no case include the ISS processes.

3. Methodology

To carry out this research project, authors needed a structured methodology explaining, its different phases in order to establish the ISS-GRC integrated model. This model is broken down into three disciplines, respectively ISS-Risk Management, ISS-Compliance Management and ISS-Gov, and it is aligned with continuous improvement. The methodology applied in this paper covers 3 phases called, DIC (Delimit, Identify and Classify), SAP (Select, Analyze and Propose) and MAB (Merge, Adapt and Build) as demonstrated below (table1).The DIC phase consists of defining the scope of the study, identifying and classifying the existing references according to their category. At the level of the SAP phase, authors will choose the models that will build their model or propose them. In this case, for the project to be transversal, cyclical and consistent with continuous improvement, authors will propose a model for each category. Then they will start their merging in order to manage the overlaps, and this at the level of the MAB phase, once the fusion will be done correctly authors will have a concept well modeled and designed (phase CMD) that will allow them to move to the development phase of their application and its test, the latter will be the subject of another article.

Table 1: research methodology

Phase 1: DIC **I. Delimit, Identify and Classify (DIC):** 1. Identification of the scope and boundaries of the study; 2. Classification of ISS-GRC components; ISS-Risk Management (1), ISS-Compliance Management (2) and ISS-Gov (3). 3. Identification of related work for each discipline;
Phase 2: SAP **II. Select, Analyze and Propose (SAP):** 1. Process model proposed for the ISS-Risk Management brick; 2. Process model proposed for the ISS-Compliance Management Brick; 3. Process model proposed for the ISS-Gov brick by extending ISO 38500 standard.
Phase 3: MAB **III. Merge, Adapt and Build (MAB):** 1. Merging the ISS-Risk Management process with ISS-Compliance Management process; 2. Merging the ISS-Risk Management Process and ISS-Compliance Management Process with the ISS-Gov process. 3. Establishing the model of ISS-GRC: ISS-GRC Unified Model (ISS-GRCUM)

4. Finding

4 DIC phase

4.1 Identification of the scope and boundaries of the study

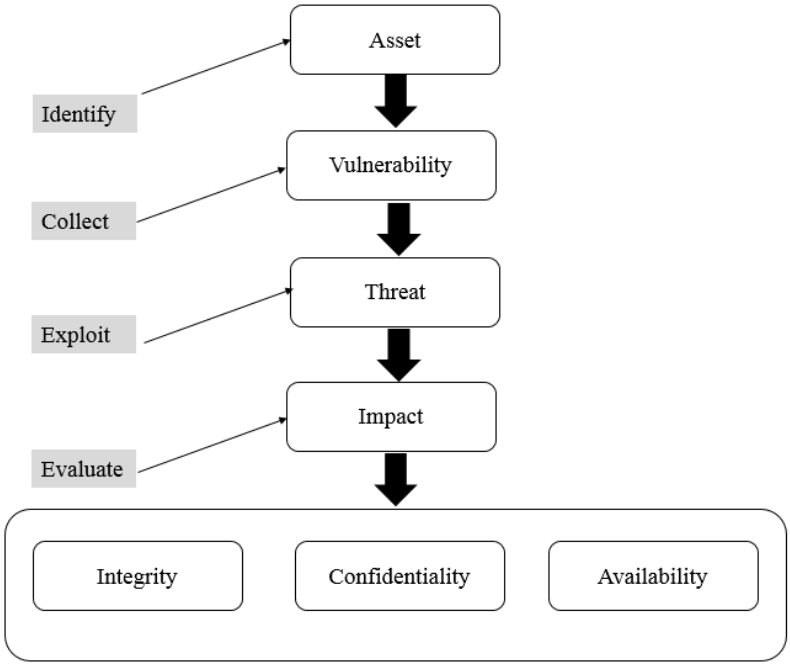
Nowadays, with the technological advances that the IT and business world knows, it is time for the organizations to focus on their activities of ISS-Gov, ISS-Risk and ISS-Compliance. Therefore, ensuring that their ISS supports their current and future GRC needs. ISS- GRC is not new but it is still a challenging subject of research. Main problem of the topic is to have the domains activities as integrated as possible. The limits boundaries of this paper will focus on the components of the ISS-GRC. And this, all by proposing the three models that will construct this framework.

4.2 Classification of ISS-GRC components

a. ISSRM

The risk defined as "a combination of the likelihood of damage and its severity" (Deodatis , Ellingwood , Frangopol , 2014). Definition of Information Security Risk: Is the possibility that 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 and necessary 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. It is this set that forms the IS [17, 18]. 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".

Figure 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 (Ross, Ronald, 2009).(3) The threat; defined by ISO 27002 (ISO/IEC 27002, 2013) 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 (acceptance, mitigation, refusal, transfer) (Bloch, Wolfhugel , 2013) to finally choose and put in place the necessary controls to reduce the risk to an acceptable level, we make recourse to the most recognized risk equation in the world of ISSRM(ISO/IEC 27005, 2013):

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 that support them for their operations. 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 expanded to also identify critical people, business processes and technology resources, understand why selected critical assets are required for operations, the fulfillment of the organization's mission and continuity operations.

b. ISSCM

The compliance component of information security plays a vital role in the organization's durability of any sector, especially in a data-driven world. Without adequate security, data breaches can occur, resulting in costly financial and commercial data loss, as well as leaks in stakeholders' confidential information. Such information breaches can sink business and ruin lives. To deal with, governments and regulatory organisms have put in place several safety regulations to help organizations improve their information security. Complying with these regulations allows to:

Improve security: IT security regulations improve organization security measures by defining basic requirements. This baseline maintains relatively constant levels of enterprise data security in the respective sectors.

Minimize losses: Improved security, in turn, prevents violations, which are costly for businesses. Many companies end up losing millions of dollars in sales, repair costs, and legal fees, all of which can be avoided with appropriate preventative measures.

Increase control: Enhanced security goes hand in hand with increased control. Prevent employee errors and insider stealing with increased accreditation systems while keeping an eye on external threats.

Maintain trust: Customers trust companies with their information. Honor this trust with improved security systems that protect their information.

Moreover, as this component is related by a multitude of laws, regulations and obligations that organizations must comply with; a non-exhaustive list cited below; organizations can design templates to centralize all of these terms into a unified database, making it easy to access, update, and apply.

GDPR: The General Data Protection Regulation, or GDPR, aims to protect citizens in the European Union (EU) from data breaches (Sgaglione, Luigi, Mazzeo, 2018).

HIPAA: An acronym for the Health Insurance Portability and Accountability Act, this bill puts in place several regulations about healthcare patients' data security (Madsen, Daniel,Masy, Miller, 2003).

FISMA: The Federal Information Security Management Act of 2002 treats information security as a matter of national security for federal agencies (Gikas, 2010).

GPG13: Alternatively known as Good Practice Guide 13, GPG13 is a U.K. general data protection regulation for business processes.

c. ISS-Gov:

ISS-Gov is the brick that will oversee the unified model of ISS-GRC, ISS-GOVUM that is the subject of this paper.

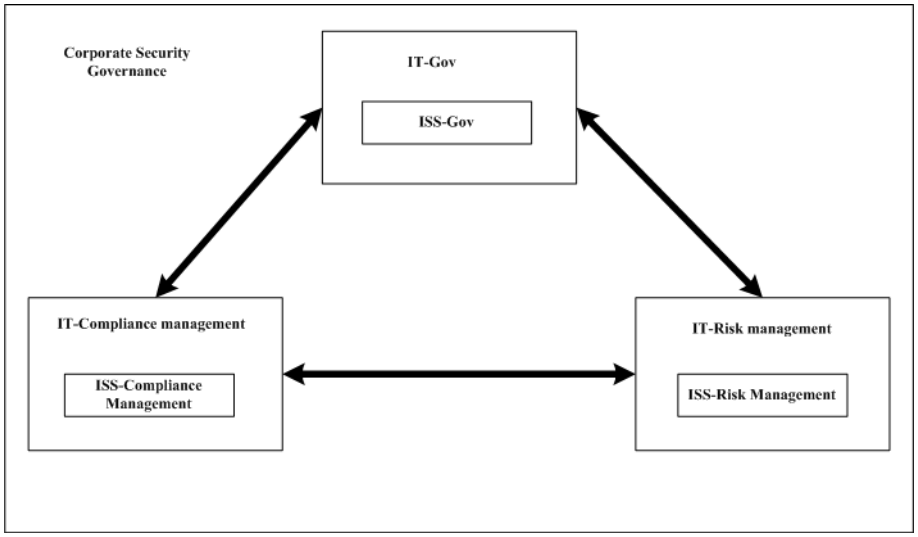
ISS-Gov is the system through which an organization directs and controls information security (ISO/IEC 38500, 2015). The ISS-Gov should not be confused with the management of information security ISM.

ISM is concerned with making decisions to mitigate risks; governance determines who is allowed to make decisions. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies. Governance ensures that security strategies are aligned with business goals and comply with regulations.

NIST describes the ISS-Gov as the process of establishing and maintaining a framework that ensures that information security strategies are consistent with corporate objectives, comply with applicable laws and regulations, and respect policies and internal controls. In an effort to manage, risk.

Governance of corporate security encompasses the IT-GRC, which contains the involved ISS-GRC processes as schematized below (figure 3).

Figure3: ISS-GRC subset of IT-GRC

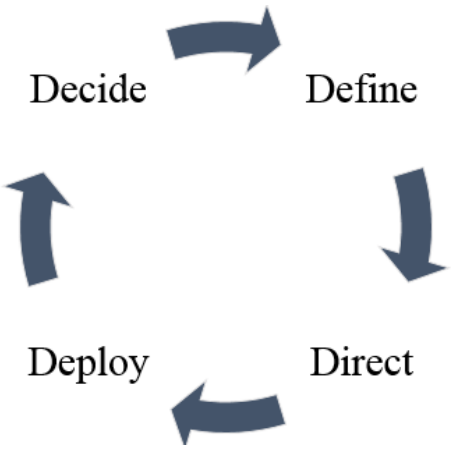


5 SAP phase

5.1 Process model proposed for the ISSRM brick

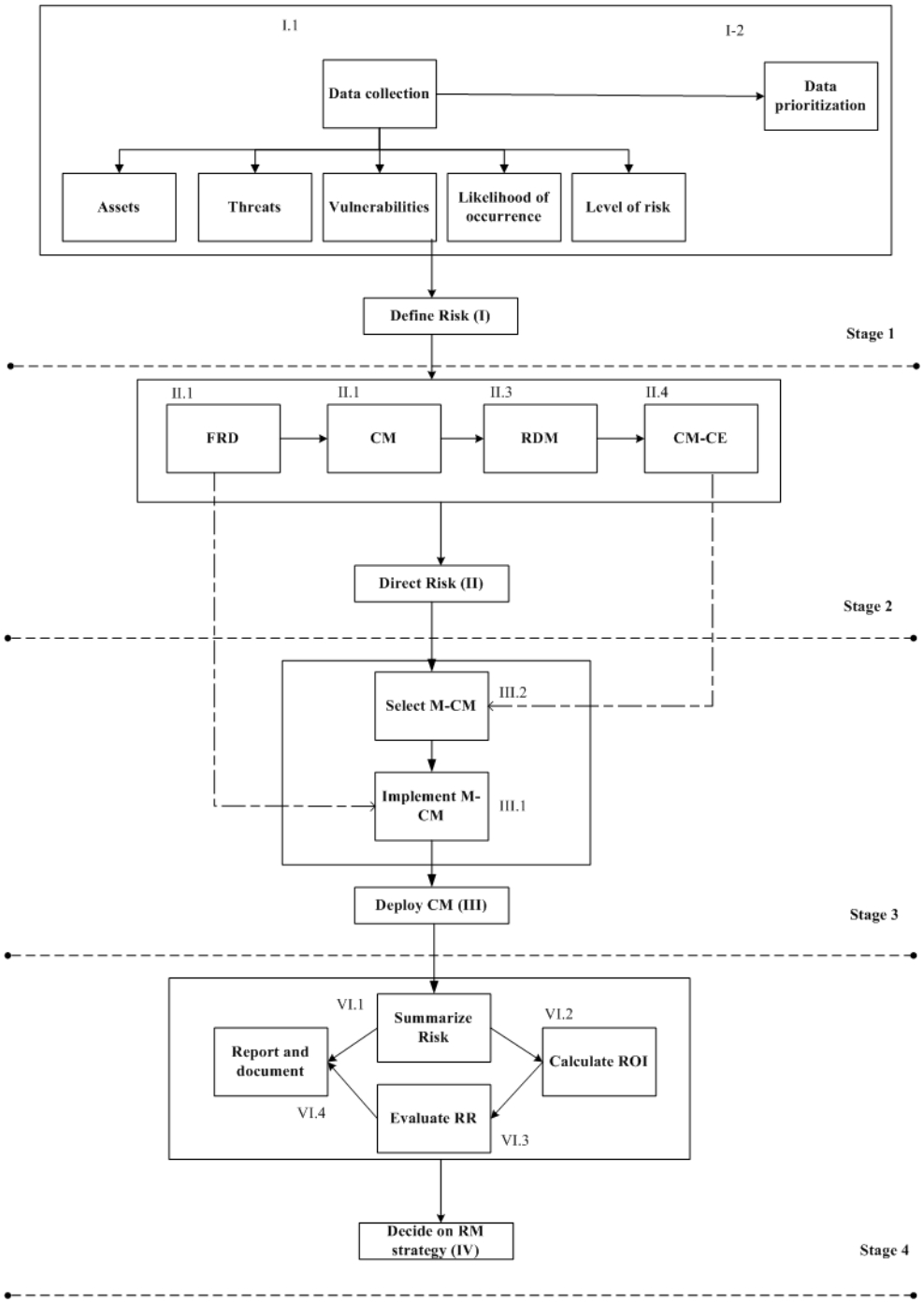
In this section, authors opt for the 4D-ISS model proposed in their previous work (Zaydi, Nassereddine, 2018), which will be part of the components of the future ISS-GRC model. This is an iterative process, aligned with the continuous improvement, broken down into four phases; each phase must be completed for the next one to begin (Figure 4).

Figure 4: Proposed model for ISS-Risk Management



The chosen model for this section will be 4D-ISS, which inherits a set of foundations of best practices in the ISSRM's field. The 4D-ISS model focuses on the quantitative category and it is broken down into four major phases (D1) Define risks and its different components. (D2) Direct them in terms of their priorities and criticality, define the functional requirements FRD to bring relevant treatment. (D3) Deploy the countermeasures CM and (D4) decide on the risk-management strategy that remains after the mitigation countermeasures M-CM implemented, in order to define the kind of threats that can be reduced, the residual risks when the risk mitigations are applied, to finally evaluate these controls in order to determine the degree of possible minimization RDM, and calculate the return of investment (ROI) of each risk mitigation. The 4D-ISS analysis model schematized below (Figure 5).

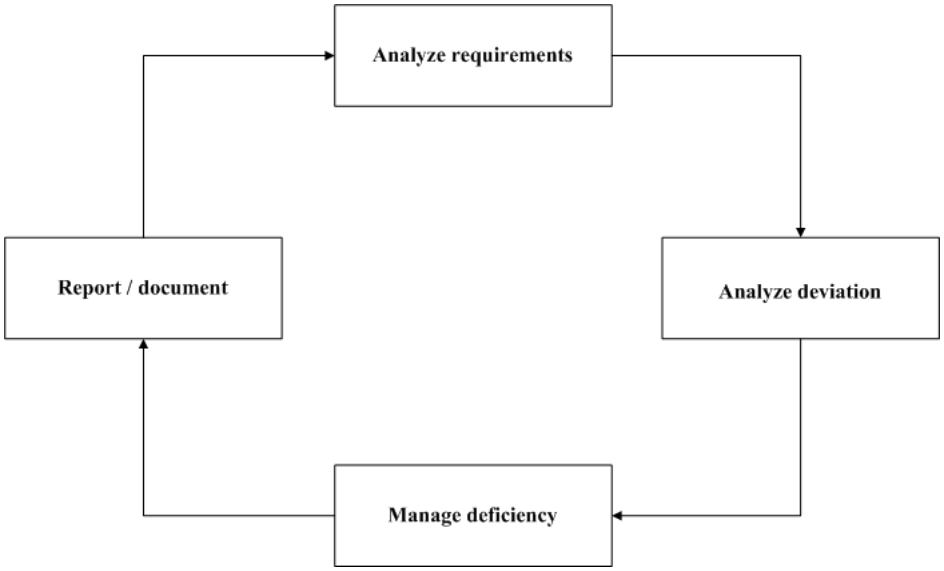
Figure5: 4D-ISS analysis model



5.2 Process model proposed for the ISSCM Brick

To deal with the heterogeneity of the laws of ISS, the distorted legislative between the developed and developing countries, authors opt for a generic process of ISSCM's brick, in this aims adaptability to different contexts and bodies, regardless of the legislation in force. To do this, the authors use the process model of Rath and Sponholz (Rath, Sponholz, 2009) described as follows (Figure 6).

Figure6: Proposed model for ISS-Compliance Management



This process model consists of (1) the identification of regulations, laws, contracts, IT operations obligations and internal policies, in order to create an internal regulatory database. This analysis can be done through internal and external audits, evaluations and security checks. The results (2) expose the shortcomings of management (3).

At this level, these shortcomings must be eliminated by improving, overhauling or creating new countermeasures. All these actions taken in the first three phases should be documented (4), and relevant information should be reported (4) to relevant stakeholders.

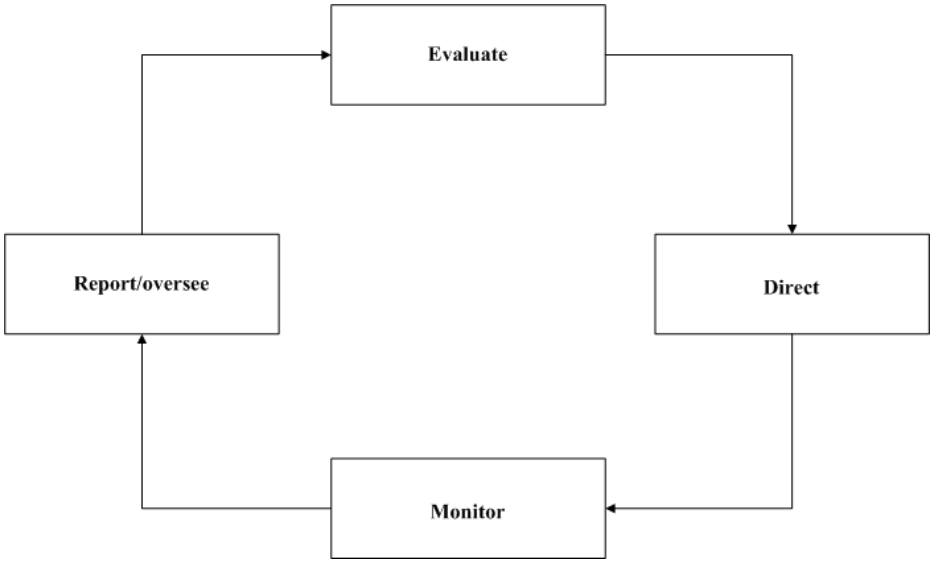
5.3 Process model proposed for the ISS-Gov brick

The ITG framework was developed in ISO / IEC 38500: 2015 (ISO/IEC 38500, 2015), and as the authors have (DIC phase, 5-2-c) emphasized that the ISSG is an integral part of ITG, as well as the project is aligned with the continuous improvement, the ISSG should be aligned with ISO / IEC 38500: 2015 (PwC, 2004). In this sense, the authors propose an extension of the ISO38500 standard that will be adapted and dedicated to the ISS-GOV process.

The model in question will inherit the 3 basic phases of the ISO38500, namely "direct" to guide the guidelines from the point of view of business strategies and risk management, "Monitor" to ensure the visibility of governance activities with measurable indicators, "Evaluate" to check and verify results. To include the ISS aspect, the authors take on consideration the fourth phase "Oversee and report" to audit governance processes and bring information back to the various stakeholders involved - proposed by Ohki et al. (Ohki, Harada, Kawaguchi, Shiozaki, Kagaua, 2009) (Figure 7).

In this sense, the authors homogenize the different processes of the three main components, which will facilitate their merging in the MAB phase.

Figure7: Proposed model for ISS-Gov



6 MAB phase

ISS-Gov, ISS-Risk and ISS-Compliance (ISS-GRC) are interdependent. The risk is to understand the probability of uncertainty. Compliance is about focusing on the policies and regulations that govern the target organization. Governance is essential for stakeholders to put in place processes and practices throughout the compliance process. A big challenge is to understand how much ISS-GRC integration can take place. By knowing where, is the ISS-risk and where ISS-risk management can carry the most affecting? It can highlight opportunities and avoid waste. ISS-risk management prioritize controls and compliance activities. Threats and vulnerabilities are fundamental elements of risk management. To cope with the legacy systems that put these processes in place on silo, organizations must begin to integrate them in a single and holistic way. In this part, the authors will explain the levels fusion of each element until the construction of the ISS-GRC final model.

6.1 Merging the ISSRM process with ISSCM process

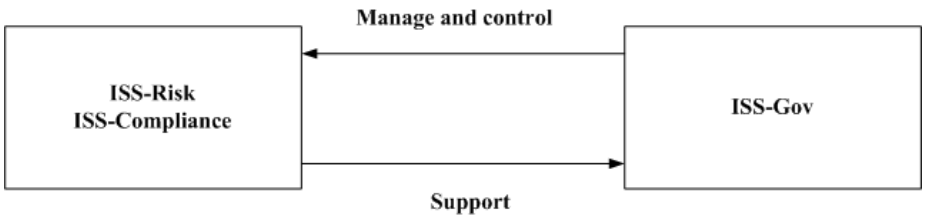
ISS risk analysis and its related processes are an integral part of compliance with different standards and laws.

For this reason, ISS risk analysis is closely linked to ISS compliance, hence the interest of starting with merging these two components.

6.2 Merging the ISSRM Process and ISSCM Process with the ISS-Gov process.

IT-Gov in general and ISS-Gov in the case of ISS-GRC represents a higher control level than ISS risk management and compliance processes, and this, if the organization is considered a cybernetic system (Lewis, Millar, 2009) , (Racz, Weippl, Seufert, 2010). The relationship of ISS-Gov and ISS-Risk and ISS-Compliance is shown below (Figure8).

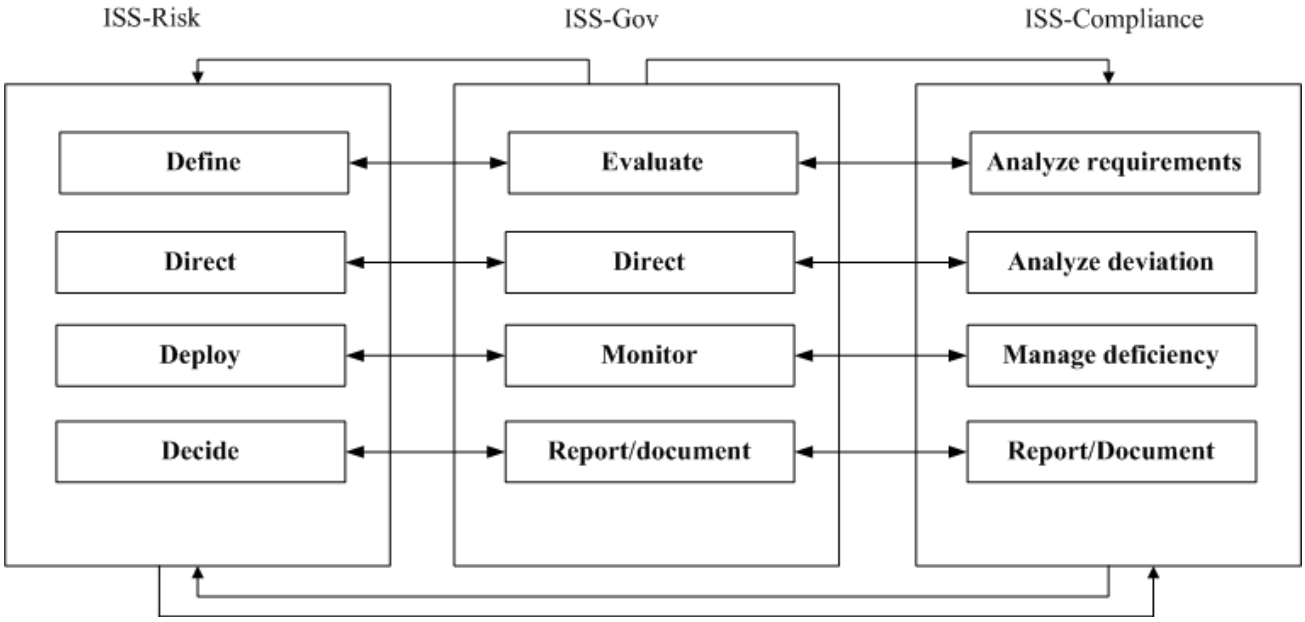
Figure8: Relationship between ISS-Risk, ISS-Compliance and ISS-Gov



6.3 Establishing the model of ISS-Gov: ISSGUM

Based on the selected components and merging their different processes, authors get the following model (Figure 9):

Figure 9: ISS-GRC unified model construction



5. Discussion & Conclusion

The ISS-Gov integration described in ISO 38500: 2015 with the inclusion of the fourth phase "report and document", the 4D-ISS model (by the ISS-Risk Management part) and the ISS-Compliance is doable. It is necessary to highlight several criticisms that can affect the methodology of this research. The choice of components of the proposed model (ISS-GRCUM) is justified by the fact that it is based on models derived from best practices in the areas of governance, risk management and compliance. The applicability of the theoretical model has not yet been proven in practice. This will be done at a later stage of the research once the model is developed and translated into a Framework. The model proposed in this document goes well beyond the existing GRC models presented in the “related work” section in various ways. First, integrated GRC models have so far been put in place without showing the path of separate disciplines to an integrated approach. It is a lack of both research and professional perspectives. For research, the logical deduction from the existing knowledge base is missing. For professionals, it complicates the management of change. This gap should be bridged by the approach applied in the construction of the proposed model. In addition, authors have explicitly developed this model for the ISS-GRC; however, the applicability of GRC existing models, present a complete lack of ISS processes inclusion. The authors attempted to facilitate the convergence of the IT-GRC with the ISS-GRC by selecting the 4D-ISS model, a generic model of IT compliance and an extended version of IOS 38500. Moreover, the role of ISS-Gov in

existing models was vast and inconsistent, while this model underline the relationship with the other components and shows how they fit together. Finally, it should be emphasized that the ISS-GOVUM model is based on existing standards and best practices, and follows a structured methodology for its development.

Conclusion and future work

In this article, the basic purpose of the authors is to propose an integrated and unified model for the ISS-GRC, based on existing good practices and in accordance with the ISO standards used. The proposed approach is broken down into 3 elements, the ISSRM, ISSCM and ISS-Gov, respectively, focuses individually on the extended IT-GOV standard (ISO / IEC 38500,2015), risk management (4D-ISS: 2018).) and the compliance management system (Rath and Sponholz model: 2014). The resulting model has been divided into two parts. First, a systematic bottom-up approach was followed to identify common activities between risk management and compliance management. Both standards can be combined by establishing the compliance management system based on the risk-related activities of the risk management process. Then, the overall part of the model was derived from the ISO / IEC 38500: 2015 model for the ISS-Gov. More future work will involve experimenting with the implementation of the ISS-GRC process model in an organization and comparing its effectiveness with ISS governance, ISS risk management and ISS compliance in silos, evaluating this theoretical approach to a practical way of applying these models in an integrated way.

References:

1. Α. Χατζηπουλίδης. 2015. “Enterprise management and software risk prediction based on security metrics.,”.
2. OCEG (2007). 2012. The 2007 GRC Strategy Study. Key findings report [Online] . Available from/ http://www.oceg.org/view/20056.
3. Racz, N., Seufert, A. and Weippl, E. 2010. A process model for integrated IT governance, risk, and compliance management. Proceedings of the Ninth Baltic Conference on Databases and Information Systems, pp. 155.
4. Racz, N., Seufert, A. and Weippl, E. 2010. Questioning the need for separate IT risk management frameworks. Konferenz Management, Compliance und Governance fur wiederstandsfahige Informationssysteme, Lecture Notes in Informatics (LNI), P-176, Informatik Proceedings, Band 2Springer LNI, 2.
5. Proceedings of the 21st European Conference on Information Systems.
6. Mitchell, S.L. GRC360. 2007. A framework to help organisations drive principled performance. International Journal of Disclosure and Governance, 4(4), 279-296.
7. Rasmussen, M. 2012. Foundations of GRC: Establishing an Enterprise View of Risk & Compliance. Corporate Integrity, Governance, Risk Manager and Compliance Research [Online]. Available from: http://grc2020.com/blog/establishing-an-enterprise-view-of-risk-compliance/.

8. Paulus, S. 2009. A GRC reference architecture. Kuppinger Cole Overview Report [Online]. Available from: http://www.kuppingercole.com/report/sp_overview_repo_grc_arch_051009 (2012).
9. Frigo, M.L. and Anderson, R.J. 2009. A Strategic Framework for Governance, Risk, and Compliance. Institute of Management Accountants.
10. Tapscott, D. 2006. Trust and Competitive Advantage: An Integrated Approach to Governance, Risk & Compliance. New Paradigm Learning Corporation [Online]. Available from: http://204.154.71.138/pdf/Trust-and-Competitive-Advantage.pdf. [25 November 2012].
11. PricewaterhouseCoopers. 2004. Integrity-Driven Performance. PricewaterhouseCoopers International Limited, Germany.
12. Wiesche, M., Schermann, M. and Krcmar, H. 2011. Exploring the contribution of Information Technology to Governance, Risk Management and Compliance (GRC) initiatives. ECIS 2011 Proceedings.
13. Racz, N., Seufert, A. and Weippl, E. 2010. A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC). Proceedings of IFIP CMS.
14. Gericke, A., Fill, H., Karagiannis, D. and Winter, R. 2009. Situational method engineering for governance, risk and compliance information systems. ACM. Philadelphia, Pennsylvania.
15. Vicente, P. and da Silva, M.M. 2011. A conceptual model for integrated governance, risk and compliance. Proceedings of the 23rd international conference on Advanced information systems engineering Springer-Verlag, Berlin, Heidelberg, pp. 199.
16. K. Spanaki and A. Papazafeiropoulou. 2013. “Analysing The Governance, Risk And Compliance (Grc) Implementation Process: Primary Insights,” ECIS Proc., pp. 1–12.
17. Deodatis G, Ellingwood BR, Frangopol DM, editors. 2014. Safety, reliability, risk and life cycle performance of structures and infrastructures. CRC Press.
18. Bloch L, Wolfhugel C. 2013. Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs. Editions Eyrolles.
19. Mayer N, Humbert JP. 2006. La gestion des risques pour les systèmes d’information. Magazine MISC.
20. ISO 27005 LOGICAL C. 2013. Information technology–Security techniques–Information security management systems–Requirements.
21. International Organization of Normalization. 2013. ISO/IEC 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management. ISO/IEC.
22. ISO/IEC 38500:2015: Information technology - Governance of IT for the organization. International Organization for Standardization, Geneva.
23. M. Zaydi and B. Nassereddine. 2018.“A new comprehensive Information System Security Governance framework A proposition of an Information system security risk management Unified process (4D-ISS),” pp. 1–16.

24. Rath, M. and Sponholz, R., 2009. IT-Compliance. Erfolgreiches Management regulatorischer Anforderungen. Berlin: Schmidt. Online verfügbar unter http://www. compliancedigital. de/978-3-503-12414-5.
25. E. Ohki, Y. Harada, S. Kawaguchi, T. Shiozaki, and T. Kagaua. 2009."Information Security Governance Framework," Work. Inf. Secur. Gov., pp. 1–5.
26. Lewis, E. & Millar, G.: The viable governance model – a theoretical model for the governance of IT. In: Proceedings of the 42nd Hawaii International Conference on System Sciences (2009).
27. N. Racz, E. Weippl, and A. Seufert, "A process model for integrated IT governance, risk, and compliance management.2010.
28. Ross, Ronald S. Recommended Security Controls for Federal Information Systems and Organizations [includes updates through 9/14/2009]. No. Special Publication (NIST SP)-800-53 Rev 3. 2009.
29. Sgaglione, Luigi, and Giovanni Mazzeo. "A GDPR-Compliant Approach to Real-Time Processing of Sensitive Data." In International Conference on Intelligent Interactive Multimedia Systems and Services, pp. 43-52. Springer, Cham, 2018.
30. Madsen, Elizabeth, Daniel R. Masys, and Randolph A. Miller. "HIPAA possumus." (2003): 294-294.
31. Gikas, Constantine. "A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards." Information Security Journal: A Global Perspective 19, no. 3 (2010): 132-141.