International Business Management 10 (19): 4644-4652, 2016
ISSN: 1993-5250

Integrating Multiple Models for Definition of IT Governance Model for Banking ITGSM

[1]Cesar Pardo, [3]Felix Garcia, [3]Mario Piattini, [2]Francisco J. Pino,
[4]Sandra Lemus and [5]Maria Teresa Baldassarre
[1]Departamento de Sistemas, Facultad de Ingenieria Electronica y Telecomunicaciones,
Universidad del Cauca, Calle 5 No. 4-70, C.P. 190002 Popayan, Colombia
[2]Faculty of IDIS Research Group, Electronic and Telecommunications Engineering,
University of Cauca, Calle 5 No. 4-70, Popayan, Colombia
[3]Alarcos Research Group, Institute of Information Technologies and Systems,
University of Castilla-La Mancha, Paseo de la Universidad 4, Ciudad Real, Espana, Spain
[4]Superintendencia de Bancos de Guatemala, 9 Avenida 22-00 Zona 1,
Ciudad de Guatemala, Guatemala, America
[5]Department of Informatics, University of Bari, SER and Practices,
SPINOFF, Via E. Orabona 4, 70126 Bari, Italy

Abstract: The regulations, guidelines and procedures defined to give support to organizations as regards Information Technology play a crucial role when any organization wants to carry out good corporative government. In its quest to ensure the suitable control and management of activities, processes and procedures, the banking sector is currently subject to the implementation and adoption of multiple models and standards. However, there is no single model that provides a unified solution, allowing there to be integrated and overall improvement of the processes used in this context. In our desire to offer a proposal which provides an Information Technology Governance Model for Banking (ITGSM), we have integrated six models which are related to this context; these are: BASEL II, COBIT 4.1, RISK IT, VAL IT, ISO 27002 and ITIL V.3. We have taken into account the latest versions of the models. Moreover, considering that integration is an essential strategy for supporting the joining of multiple models in harmonization projects, we have defined a process to carry out out this purpose. This research intends to support banking organizations which are interested in introducing new processes, or improving their existing ones in specific areas such as maintaining IT governance, managing the investment of IT, IT risk, managing information security and the life cycle of IT services.

Key words: Integration, integration processes, information potential, management, management models, integrated business structure

INTRODUCTION

A couple of decades ago, lack of good practices for managing and leading the corporative processes and operations of the companies brought great problems and distrust in the way of working of bank systems and corporations. The lack of good practices extended to several subjects of corporative government such as risk management, return on investment and information security, amongst others. An example of the magnitude of the problems caused by the lack of suitable business practices may be seen in the report about security measures called CSI/FBI Computer crime security survey status, published by the Computer Security Institute (CSI) in collaboration with the Federal Bureau of Investigation (FBI).

In response to this issue, authorities and organizations such as the Information Systems Audit and Control Association (ISACA), the International Organization for Standardization (ISO) and the Bank for International Settlements (BIS), amongst others have defined a set of regulations, guidelines and action procedures concerning good corporative government and issues related to Information Technology (IT). These include COBIT, ITIL V3.0 (ITIL, 2010), RISK IT (ITGI, 2009), VAL IT (ITGI, 2008a), ISO 27002 (ISO, 2005a), ISO

Corresponding Author: Cesar Pardo, Departamento de Sistemas, Facultad de Ingenieria Electronica y Telecomunicaciones, Universidad del Cauca, Calle 5 No. 4-70, C.P. 190002 Popayan, Colombia

27001 (ISO, 2005), BASEL II (BIS, 2006), SARBANES OXLEY (Sarbanes and Oxley, 2002), COSO. The arrival of these reference models has enabled the performance of different markets, enterprises and corporations to be normalized, making it possible to incorporate practices into them, thus ensuring suitable: security, controls, risks management, investment management, transparency and confidence.

For the banking sector, corporative government models and IT standards have become a strong support. This is thanks to the fast propagation of Information Technologies in each one of the activities, services and business operations carried out within this context. Using a reference model has allowed them to acquire a feature that helps them be competitive. It also gives them an edge over their competitors as regards their daily activities. It is certainly true that the increased sophistication of the supporting technologies has allowed the banking sector to carry out the globalization of their financial services. It is nevertheless important to highlight that it has also contributed to increasing complexity in banking activities, thus augmenting their risk profiles (BIS, 2006).

With all the above in mind, it is obvious that the Banking sector is currently subject to the adoption of multiple regulations, models and standards (ITGI, 2007a). This fact means that a particular reference model may be chosen and implemented to give support to any one of the multiple needs at different hierarchic levels. However, the models chosen are applied separately which makes the associated costs such as in time and effort much greater than if the support had been given in an integrated way (Pardo *et al*., 2011). It is also the case that the individual definition of the operational objectives makes it difficult to have integrated leverage and implementation of the approaches that are institutionalized in an organization (Siviy *et al*., 2008a, b).

Some bodies, such as ISACA, ISO, amongst others, are currently working on establishing relationships between some models that are in widespread use and employed internationally, e.g., the analysis of the relationships between COBIT 4.1 with regard to other models such as ITIL V.3 and ISO/IEC 27002 (ITGI, 2008b; Pardo *et al*., 2011, respectively. However, it has not been possible to find a model which integrates the best practices that focus on supporting the compliance of different areas such as: maintaining IT governance, managing the investment of IT, the risks of IT, managing information security and the life of IT services. Given that there is no single proposal which unifies a set of best practices enabling different needs around the banking sector to be supported, this paper presents in detail the integration performed by a model called Information Technology Governance Model for Banking (ITGSM). This model sets out to help organizations especially in issues like the ones mentioned above. That help is made possible by the fact that ITGSM integrates the latest versions of models such as COBIT 4.1, Basel II, VAL IT, RISK IT, ISO 27002 and ITIL V3.

Literature review: On the basis of the results obtained from a systematic review performed about the existence of IT methodologies used to assess the banking sector as presented by Lemus *et al*. (2010), there was no IT governance framework found that applied to this sector. On the other hand, it was seen in the review that there are several studies which analyze the relationships between some models. The aligning of COBIT 4.1, ITIL V.3 and ISO/IEC 27002 for Business Benefit (ITGI, 2008c), Mapping between ITIL V.3 and COBIT 4.1 are just some examples. However, there was no integrated model which would harmonize multiple approaches and so support IT government. In that sense and taking the literature discovered as the starting point, the most important contribution of this article is the harmonization and integration of the best practices and standards that are subjects of this study. These are: COBIT 4.1, Basel II, VAL IT, RISK IT, ISO 27002 and ITIL V3. In addition, the harmonization strategy and integration process used for the harmonization of the models are set out.

Bearing in mind that space here is limited, a brief summary of the models involved with an outline of each approach is presented as follows.

BASEL II (BIS, 2006). This is a banking regulation of non-mandatory application. It is intended to guide financial organizations in maximizing the refinement of the measurement and management of risks, when calculating the capital that insures these risks.

COBIT 4.1 (ITGI, 2007b). This is a process model, constituted in such a way that it allows us to bring in and maintain control and governance of information. That meets the needs of top management in their quest to bridge the gaps that exist between business objectives and technological aspects.

VAL IT Framework 2.0 (ITGI, 2008a-c). The framework integrates a practical set of principles, processes, practices and guides of governance which help top managers, managers and leaders of the companies to optimize the delivery of value through investments in IT.

RISK IT (ITGI, 2009). This model addresses risk management in IT, integrated with enterprise risk management, ERM.

ISO 27002 (ISO, 2005b). This is a guide of best practices which describes the control objectives, along with recommended controls as regards information security. ITIL V3 (ITIL, 2010). This framework focuses on the administration of IT service lifecycle management.

MATERIALS AND METHODS

The integrated model: To support the management of the harmonization project and to manage to configure a suitable harmonization strategy to perform the harmonization of the models involved, a harmonization framework and the process that it proposes were used; a summary of these and their application with regard to this experience is presented by Pardo *et al.* (2013). A more detailed version of the harmonization process using SPEM 2.0 and edited with the EPF Composer is presented by Armonias. The main work of the implementation of this process was a harmonization strategy which was comprised of three stages and three techniques these are: homogenization, comparison and integration (Pardo *et al.*, 2009; Pino *et al.*, 2010), respectively. However, since the homogenization and comparison techniques have been presented in previous work and these have not suffered modifications, we are not going to go into them in detail. That being so and since the integration technique is being presented here for the first time, we devote this section to emphasizing and explaining this technique in depth.

Process of integration: The purpose of this technique is to provide a guideline which allows us to support the integration of multiple models step-by-step and ensure the reliability of the results obtained. In order to provide an ordered and systematic management of the people, activities and task involved, this technique has inherited the roles used in the harmonization strategy; these roles carried out the tasks described below.

Designing the integration: this activity involves the tasks: fixing the process entities to be integrated, based on the results obtained in the comparison; fixing the order of integration to follow (integration procedure) and defining an integration template.

Establishing integration criteria: this activity involves the establishing of rules of absorption or integration. It is necessary to define some criteria amongst the elements being integrated because this will allow more appropriate decisions to be made. That in turn will make it more possible to integrate the descriptions, recommendations or practices of the elements being integrated. These absorption criteria could refer to the following states: that the description of the element with less detail is supported and contained in the description of the element with greater detail or the description of the element with greater or less detail is not contained in the other element.

Carrying out the integration: this activity involves the tasks of carrying out an in-depth analysis of the descriptions of the process entities being integrated, carrying out a syntactic analysis if possible, resolving the discrepancies of integration and adaptation of the process entities under integration to take into account the absorption or integration criteria defined, verifying and validating these results:s

- Analyzing the results of the integration
- Presenting the integrated model

Figure 1 shows the activity diagram of the process for the integration technique which uses SPEM 2.0 notation and includes roles, activities and some work products.

The integration process described previously was followed and executed by two people, one person as performer and another as reviewer. In the next section the execution of the activities described by the process is described in greater detail.

Integrating the models: Before conducting the integration of the models, we have carried out the homogenization of

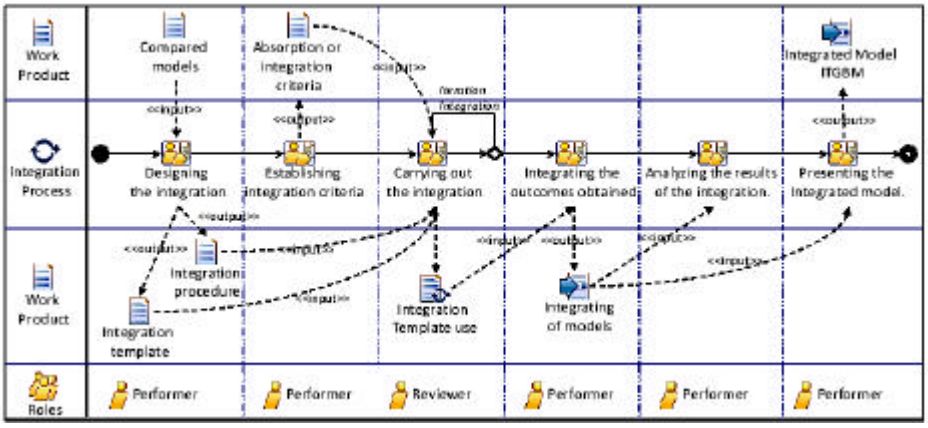

Fig. 1: Activity diagram of the process for integration

their process entities using a Common Structure of Process Entities (CSEP). A detailed summary of the homogenization technique and CSPE are presented by Pardo *et al*. (2009). The homogenization enabled the models' structures to be put in harmony and this made it possible to reduce the complexity of the comparisons. Before carrying out the homogenization, both processes and activities were process entities that were present in all models. In that sense, the performer and reviewer decided to carry out the comparison of the models to the level of these entities and guide the comparison in pairs of models as follows. First of all, the principles of BASEL II with the COBIT processes were to be compared and the principles that support these processes had to be discovered. This comparison was the basis for the definition of the integrated model. Other comparisons were performed following this. These took into account the first comparison between Basel II and COBIT 4.1. 5 comparisons were performed in all, between the following pairs: BASEL II and COBIT 4.1, VAL IT and COBIT 4.1, RISK IT and COBIT 4.1, ISO 27002 and COBIT 4.1 and ITIL V.3 and COBIT 4.1. In the first comparison 44 relationships (processes) were found; these have been reinforced from the comparisons with other models that is: VAL IT, RISK IT, ISO 27002 and ITIL. The definition of ITGMB is based on the integration of the set of comparisons of the models involved.

Establishing integration criteria: Once we identified the activities and/or procedures that supported the fulfilling of the purposes described in the 44 base-processes, we had to define how to integrate them. To do that, a set of integration criterion was established, defining rules and criteria of absorption and/or adaptation to follow in merging the descriptions of the process entities involved. Following the recommendations given by the integration process, these were organized into two categories according to their features. The rules and criteria of absorption and integration are presented below.

When the description of the procedure/activity with less detail is supported and contained in the description of the procedure/activity with greater detail. This issue involves taking into account the following.

When the procedure/activity of Model A offers a greater amount of description or detail than Model B, the procedure/activity of B could be absorbed by the procedure/activity of A.

When the procedure/activity of Model A offers an equal amount of description or detail to that in Model B, the procedure/activity of B could be absorbed by the procedure/activity of A. When the procedure/activity of Model A offers less description or detail than Model B, the procedure/activity of B could be absorbed by the procedure/activity of B.

When the description of the procedure/activity with greater or less detail is not contained in the other procedure/activity. This issue involves taking into account the following.

When the procedure/activity of Model A offers a greater amount of description or detail than Model B, the procedure/activity of B could be absorbed by the procedure/activity of A.

These rules and criteria were basic to being able to adapt and merge the descriptions of procedures/activities involved in each model. The definition of these rules and criteria were crucial to the fulfillment of the principles of operational risk defined in BASEL II. To apply these appropriately, it was fundamental for the person performing the application to have previous knowledge of the particular models involved, this person also needed to have experience in the banking supervision sector.

RESULTS AND DISCUSSION

Carrying out the integration: Using the results obtained in the comparison, the work group comprised by the performer and reviewer carried out the integration of the models that had been compared, at the level of their procedures and activities. The process of integration was thus defined and executed to support the joining of the sensitive process entities that were to be integrated. The process followed is the one presented previously in this section. This process made it possible to manage the activities involved systematically, reducing the complexity that comes about when the descriptions of each model are integrated.

To make the integration less complex, we used a one-to-one iterative and incremental procedure in the process. That is, the integration was performed on pairs of models. This procedure is iterative, because the execution of the integration is carried out on one model process first and then on the other in turn. It is also incremental because the integration template grows and evolves with the performing of each iteration, until it becomes a new/integrated process. Figure 2 summarizes the work performed in the integration step-by-step. The integrated model is organized

Template of the integration model:
Principles of BASEL II; process activities of the processes of each model:

- ID
- Description
- COBIT 4.1
- VAL IT
- RISK IT
- ISO 27002
- ITIL V.3

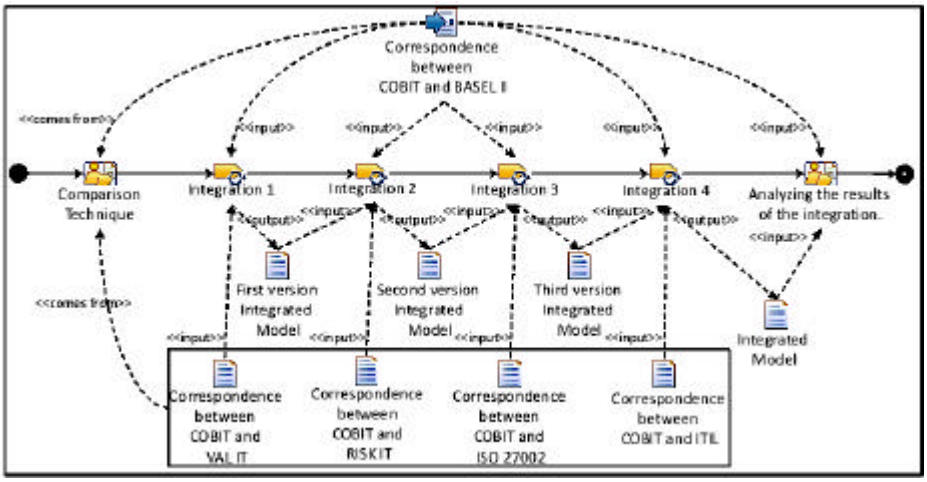

Fig. 2: Work performed to integrate the relationship between models involved

Table 1: Partial example of ITGSM

Princi. of		Process	Activities of the processes of each model				
BASEL II	ID	Description	COBIT 4.1	VAL IT	RISK IT	ISO 27002	ITIL V.3
1	2	Discover an IT risk management framework, then approve it and ensure it is fulfilled. The framework documents a commonly agreed upon level of IT risk also registering mitigating strategies and residual risk	PO9.1, PO9.2	IM1.2	RG1.5, RG1.7, RG1.8, RG3.3, RG3.4, RE1.1, RR1.3, RR3.4	Clauses 4.1, 5.1, 13.1, 14.1.1	SS9.5

It organizes the descriptions of the processes and activities of the models that give support to the processes and principles of Basel II that ITGSM gives support to. Table 1 shows an example as part of the integrated model.

Analyzing the results of the integration and presenting the integrated model: Taking the results of the activities performed and described in the previous sub-sections as his starting point, the reviewer performed an analysis of the outcomes of the integration to increase the reliability of the integrations. The integrated model was then presented to the stakeholders.

The new integrated model was called IT Governance Model for Banking (ITGMSB). Its structure which is made up of the 44 processes of COBIT related to the principles of operational risk defined in BASEL II. The activities related to those processes were identified from: analyzing the results obtained in the comparison of all of models and the analysis and identification of the activities needed to fulfill each purpose described in the 44 processes. Although, the first process structure identifies 44 processes, only 22 of them have been described in detail. That is because these were considered to be the basic processes that should be included in the first version of the model. In that sense, version 1.0 of ITGSM gives in-depth descriptions of the general purpose, the specific objective and the activities of 22 processes. ITGSM is presented by ITGI (2007a) where it is described fully. Because we cannot show the unified model here completely, due to the limited amount of space available, we present a summary which gives an outline of the structure, procedures and activities of ITGSM V1.0 as seen in Table 2.

A complete ITGSM process is shown in Appendix 1. It corresponds to process 2 of ITGSM; this is the process that is in charge of defining the best practices to support IT risk management. That task forms part of the necessary awareness and responsibilities of the board (it has been taken from (ITGI, 2007b). The table in Appendix 1 orders the process as follows: title of the process, principle of BASEL II that ITGSM fulfills, general purpose, specific objective and activities aimed at supporting approaches such as: IT governance, IT investment, specific IT risk management, management of information security and service lifecycle. The identification of the procedure/activity used in each model involved is also referenced.

IGTSM is expected to be useful to organizations that plan to adopt practices concerning IT Management, IT Government and Information Security Management through models such as BASEL II, COBIT 4.1, RISK IT, VAL IT, ITIL V.3 and ISO/IEC 27002. Figure 3 summarizes the approaches, subjects and models supported by ITGSM.

Table 2: Partial example of ITGSM

Process (PR) / Title of the processes	Activities of the processes of each model: IT governance	Management the IT investment	Specific risk management IT	Management of information security	Management the service lifecycle
PR 1					
P1: define the IT processes as well as the organization and relationships in IT which the management board should be aware of and responsible for	PO4.2, PO4.3	VG1.4, VG1.5, PM1	RG2.1	Clauses 5.1, 6.1, 6.2, 8.1.1, 8.2.1, 15.1, 15.2	SD2.4.2, SS6.1, SO3.2.4
P2: risk management of the ITS as part of what the management board should be aware of and responsible for	PO9.1, PO9.2	IM1.2	RG1.5, RG1.7, RG1.8, RG3.3, RG3.4, RE1.1, RR1.3, RR3.4	Clauses 4.1, 5.1, 13.1, 14.1.1	SS9.5
P3: provide TI governance as part of what the Management board should be aware of and responsible for	ME4.2	VG1, VG2.1, VG5	RG1, RG2	Clauses 5.1, 6.1.2, 10.1	SD3.10
PR 2					
P4: monitor and assess internal control as part of independent internal auditing	ME2.1, ME3.2	--NA--	RG1, RE2, RR1.2, RR1.3	Clauses 5.1, 6.1.8, 15.2, 15.3	--NA--
P5: ensure the that external requirements are fulfilled as part of independent internal auditing	ME3.1, ME3.3	--NA--	--NA--	Clause 15.1	--NA--
PR3					
P6: establish a strategic plan for IT as part of corporate risk management	PO1.2, PO1.4	VG1.5, VG2.1, VG4, PM1, PM6	RG1, RG2	--NA--	SS2.1, SS2.3, SS3.3, SS4.1, SS4.2, SS4.4, SS5.5
P7: determine the IT processes as well as the organization and its relationships as part of corporate risk management	PO4.1, PO4.8	VG2.4, VG2.6	RG1.2, RG2.4, RE1.1, RE3.1	Clauses 6.1, 6.2.1, 7.2, 8.1, 8.2, 8.3, 9.1, 9.2, 10.1.2	SS2.6, ST4, SO4
P8: communicate aspirations to the directors and management as part of corporate risk management	PO6.2, PO6.5	VG1.1, VG1.2, PM4.2, PM4.3, IM1, IM6, IM9	RG1.1, RG1.2, RG1.3, RG1.7, RG1.8	Clauses 5.1, 6.1.1, 7.1, 8, 9, 10.7.3, 10.8, 11, 12.3, 13.2	ST5.1, SO3.6
P9: manage quality as part of corporate risk management	PO8.1, PO8.6	--NA--	--NA--	--NA--	SS4, SD3, SD4.2, ST4.1,ST4.4,ST4.5, SO5, CSI4.1
P10: monitor and assess the IT effort as part of corporate risk management	ME1.1	VG5, PM5, IM9	RE3.6	Clause 10.10.2	SD3.6.5, SD4.2.7, ST4.5.8, SO4.2.8, SO5.1, CSI4.1.2, CSI4.3
PR4					
P11: evaluate and manage IT risk as part of the identification and evaluation of banking operation risk	PO9.3, PO9.4, PO9.5	PM4.1, IM1.2, IM2.2, IM5.1	RE1, RE2, RE3	Clauses 4.1, 4.2, 14.1	SD3.5, SD4.5, ST4.1, CSI5.6.3
P12: manage change as part of the identification and evaluation of banking operation risk	PO6.1, PO6.2, PO6.3, PO6.4, PO6.5	--NA--	--NA--	Clauses 10.1.2, 12.5.1, 12.6.1	ST4.2
P13: guarantee system security as part of the identification and evaluation of banking operation risk	DS5.1, DS5.2, DS5.3, DS5.4, DS5.5, DS5.6, DS5.7, DS5.8, DS5.9, DS5.10, DS5.11	--NA--	RR3.1, RR3.2, RR3.3	Clauses 5.1, 6, 8, 9, 10.1, 10.4, 10.6, 10.8, 10.9, 11, 12, 13, 15.1, 15.2	SD4.6, ST4.3, SO4.5, SO5
P14: manage the configuration as part of the identification and evaluation of banking operation risk	DS9.1, DS9.2, DS9.3	--NA--	RE3.1, RE3.2, RE3.3, RR2.1	Clause 7.1	ST4.3
P15: provide IT governance as part of the identification and evaluation of banking operation risk	ME4.1, ME4.5	VG1.1, VG1.4, VG1.5, VG2.1, VG5	RG1.1, RG1.2, RG1.3, RG1.4, RG1.8	Clause 6.1	SS3, SD3
P16: maintain and monitor IT risk as part of the monitoring of banking operation risk	PO9.6	VG5, PM5, IM9	RR1.2, RR2.2, RR3.2	Clause 10.1	SD4.5, ST4.6, CSI5
P17: monitor and assess IT effort as part of the monitoring of banking operation risk	ME1.2, ME1.3, ME1.4	VG5, PM5, IM9,	RE1.5, RR1.2	--NA--	SD3. SD4.2, ST4.5, SO5, CSI9.3
P18: monitor and assess internal control as part of the monitoring of banking operation risk	ME2.3, ME2.7	--NA--	RG1, RR1	Clauses 5.1, 6.1, 6.2, 10.1, 15.2, 15.3	--NA--
P19: provide IT governance monitor and assess IT effort as part of the monitoring of banking operation risk	ME4	VG1, VG2, VG5	RG1, RG2	Clauses 5.1, 6.1, 10.1	Core concepts, SS4, SD3, CSI4.3
P20: define IT processes, along with their organization and relationships as part of banking policy, process and procedure	PO4.1, PO4.4, PO4.5, PO4.8	VG2	RG1.1, RG1.2	Clauses 5.1, 6, 10.1, 15.2	SS4, SS5.4, SD3, SD4.1, ST4, SO4

Table 2: Continue

Process / Title of the processes	Activities of the processes of each model: IT governance	Management the IT investment	Specific risk management IT	Management of information security	Management the service lifecycle
P21: communicate aspirations and address management as part of the policies, processes and banking procedures	PO6.1, PO6.3, PO6.4	VG1	RG1, RG3,	Clause 6.1.1	ST4.1.3
P22: manage quality as part of banking policy, process and procedure	PO8.1, PO8.2	--NA--	--NA--	--NA--	SS4.4.4, CSI4, CSI5, CSI8
BASEL II					
The processes describe principles as well as general purpose and specific objectives	COBIT 4.1	VAL IT	RISK IT	ISO 27002	ITIL V.3

Nomenclature used to name some elements in the table: BASEL II: PR: Principle, COBIT 4.1: PO: Plan and Organize, ME: Monitor and Evaluate, DS: Deliver and Support, VAL IT: PM: Portfolio Management, IM: Investment Management, VG: Value Governance. RISK IT: RG: Risk Governance, RE: Risk Evaluation, RR: Risk Response, ITIL V.3: SD: Service Design, SS: Service Assets, SO: Service Operations, CSI: Continual Service Improvement, ST: Service Transition, NA: Not Applicable

Firstly, ITGSM should be useful in helping to understand the relationships identified between integrated models. This is because the model allows us to have continuous input of knowledge about the activities of the particular models that are related to the activities that ITGSM defines (Appendix 1). Thus, organizations will be able to know easily and at any time which activities they comply with according to Basel II, COBIT 4.1, RISK IT, VAL IT, ITIL v.3 and ISO/IEC 27002.

Secondly, since ITGSM keeps the relationships between its activities and the activities of the integrated models, it will be possible to carry out assessments of the integrated reference models separately or all together. That is to say, the assessments can be performed using an integrated assessment template with regard to ITGSM processes or we may assess the practices according to any one of the models integrated.

Thirdly, as the structure of the ITGSM takes a particular direction according to the specific approach of each model, it will be easy to carry out maintenance whenever international bodies provide new versions of the models integrated. Similarly, it will be straightforward to reflect the changes to the models in organizational processes.

Fourthly, ITGSM makes it possible for COBIT-registered organizations to adopt other approaches, e.g., a COBIT-registered organization that plans to adopt practices focusing on the management of information security can adopt the set of specific practices of ITGSM described on the basis of the ISO 27002 standard. In a similar vein, it is important to highlight that if an organization is interested in complying with banking regulations, the introduction of an activity of ITGSM is in response to the completion of a specific principle defined by BASEL II. Currently, ITGSM offers support to six principles of the 10 defined by BASEL.

Fifthly, since ITGSM organizes its activities according to a set of application approaches (which in turn depend on the particular approach of each model that has been integrated (Fig. 3), the organizations can bring in new processes or improve their existing ones by choosing a set of activities or specific approaches that are defined in ITGSM.

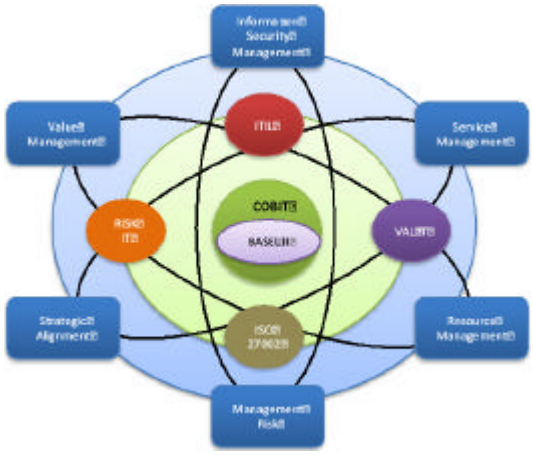

Fig. 3: Approaches and Models that ITGSM supports

CONCLUSION

This study has presented a unified model called ITGSM, which integrates and harmonizes at a low-level of abstraction the best practices (procedures/activities) of six models which are: BASEL II, COBIT 4.1, VAL IT, RISK IT, ISO 27002 and ITIL V.3. This model proposes a set of 22 processes can potentially help the banking sector, especially in issues such as: maintaining IT governance, managing the investment of IT, IT risks, managing information security and the life of services.

The integration process followed to integrate the models involved is also presented. This describes the activities performed to join the models that were harmonized. This technique is introduced here for the first

time and is part of the set of techniques defined in the ARMONIAS project. A framework has been developed in this project, along with elements to support the harmonizing and integrating of this case study and other harmonization projects such as ISO 27001 and ISO 20000 part 2 (Pardo *et al*., 2013).

The next step we plan to take is to release the second version of the ITGSM which will be able to integrate the remaining 22 processes. This will give support to the fulfillment of the principles of BASEL II that have not been addressed in this version. We would also like to comment that ITGSM will be validated by means of a case study from the viewpoint of banking supervision. We will do this by carrying out a diagnosis of a Guatemalan Bank's Technological Profile. Until now this diagnosis has been performed using only COBIT as a reference model. The results found will be used to strengthen the processes already existing in this sector and to confirm the efficacy of the proposed model. The conceptual relationships established between the two standards have been identified using the criteria and experience of the performer responsible for the analysis and comparison of models.

In future research, we will carry out an empirical study that allows there to be a mapping of the standards. To do that we will count on the opinion of several experts and/or practitioners involved in the use of ISO 27001 and ISO 20000 in some organizations. This validation would enable the correspondence between these standards to be checked, not only from a theoretical point of view but also from an empirical and practical standpoint.

ACKNOWLEDGMENTS

This research has been funded by the projects: ARMONIAS (JCCM of Spain, PII2I09-0223-7948), PEGASO/MAGO project (MICINN and FEDER, TIN2009-13718-C02-01), ARCA (CEC-JCCM of Spain and FEDER, HITO-2009-06). Cesar Pardo and Francisco J. Pino acknowledge the contribution of the University of Cauca where they work as an assistant professor and full professor, respectively.

APPENDIX

Appendix 1: process 2 of ITGSM

Activities		Models of Ref.
Activities aimed at IT governance (COBIT)		
Framework of IT risk management adopted	Ensure the establishment of a framework of IT risk management that is aligned to the framework of risk management in the organization	PO9.1
Establish risk context	Establish the context in which the framework of risk assessment should be applied	PO9.2
Actions to manage the IT investment (VAL IT)		
Develop an initial program of business concepts	Request the development of an initial business case concept to describe the results expected from the investments made and the key assumptions that must be considered, along with the risks that must be identified as well as potential impacts and mitigation strategies	IM1.2
Activities aimed at specific risk management IT (RISK IT)		
Approve IT risk tolerance	Management must approve the tolerance levels of IT-related risks, according to the thresholds for acceptance of business risk	RG1.5
Promote a culture of awareness of IT risk	Encourage the development and effective promotion of a culture of accountability of IT-related risks; this requires communication, organization and appropriate structures for implementation	RG1.7
Promote effective communication of IT risk	Encourage managers and IT executives to understand the actual amount of IT risk to help direct the appropriate resources to meeting IT risk, according to taste and tolerance	RG1.8
Considerations in business decisions include the IT risk	Ensure that IT risk assessment is considered in decisions within the organization	RG3.3
Accept IT risk	To complete the hazard mitigation projects or policies of exception, standards and operating procedures, review the report of the levels of residual risk, the risk mitigation options and projected costs; reduce potential risks from an expected cost-benefit analysis and lessen the effects of risk aggregation	RG3.4
Propose the establishment of a model for the registration of IT risk events	Apply the definition of a model for the collection, classification and analysis of multiple events related to IT risk	RE1.1
Order external evaluations of IT risk	Ask an outside expert to conduct a comprehensive assessment of IT risk and provide feedback for corrective action	RR1.3
Request post-mortem revisions of incidents related to IT	Order reviews to identify the root cause of IT-related incidents	RR3.4
Activities aimed at the management of information security (ISO 27002)		
Assessment of security risks	Promote assessments of risks to security, so as to be able to identify, quantify and prioritize risks in consonance with the risk acceptance criteria and objectives that are relevant to the organization	4.1
Promote and adopt the policy of information security	Approve information security policy at the organizational level and promote its implementation in line with business objectives, laws and regulations	5.1

Appendix 1: Continue

Activities		Models of Ref.
Promote the reporting of incidents in information security	Maintain a constant report of information security incidents, so as to be aware of these and deal with them properly	13.1
Management of business continuity	Include controls to identify and reduce risks; the overall process of risk assessment should limit the consequences of any harmful incidents and ensure the availability of the information required for business processes	14.1.1
Actions to manage the service lifecycle (ITIL V3)		
Consider and promote risk management in the delivery and support of IT services	Ask for management of risks to be considered in the management of the service lifecycle associated with the support and delivery of IT services	SS9.5

Title: IT risk management as part of the awareness and responsibilities of the board; one which reflects the principle of operational risk Basel II: the management board must know what the main aspects of operational risk for the bank are as a distinct risk category and they must approve and periodically review the framework used by the bank to manage this risk. This framework must provide a valid definition of operational risk throughout the enterprise and establish principles to define, assess, monitor and control or mitigate these risks. General purpose: support the assessment and management of IT risk, seeking the board of directors' approval by the of a framework of appropriate risk management; Specific objective: to know, approve and enforce a framework of risk management of IST which is applicable to the entire organization. The framework documents a common and agreed level of IT risks, mitigation strategies and definition of acceptable risk thresholds

REFERENCES

BIS., 2006. BASEL II: International convergence of capital measurement and capital standards: A revised framework, comprehensive version. Bank for International Settlements, Basel, Switzerland. http://www.bis.org/publ/bcbs128.pdf.

ISO., 2005a. Information technology-security techniques-Information security management systems-requirements. ISO/IEC 27001:2005. http://www.iso.org/iso/catalogue_detail?csnumber=42103.

ISO., 2005b. Information technology-security techniques-code of practice for information security management. ISO/IEC 27002:2005. http://www.iso.org/iso/catalogue_detail?csnumber=50297.

ITGI., 2007a. IT Control Objectives for BASEL II: The Importance of Governance and Risk Management for Compliance. ISACA, USA., ISBN-13: 9781893209381, Pages: 103.

ITGI., 2007b. COBIT® 4.1: Framework, Control Objectives, Management Guidelines and Maturity Models. IT Governance Institute, USA., ISBN-13: 9781933284729, Pages: 196.

ITGI., 2008a. Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for business benefit. IT Governance Institute (ITGI) and Office of Government Commerce (OGC), USA.

ITGI., 2008b. COBIT mapping: Mapping of ITIL V3 with COBIT 4.1. IT Governance Institute (ITGI) and Office of Government Commerce (OGC), USA.

ITGI., 2008c. The Val IT framework 2.0. IT Governance Institute (ITGI) and Office of Government Commerce (OGC), USA., pp: 207.

ITGI., 2009. Risk IT: Framework for management of IT related business risks. IT Governance Institute (ITGI) and Office of Government Commerce (OGC), USA. http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx.

ITIL., 2010. Information Technology Infrastructure Library version 3. http://searchcio.techtarget.com/definition/ITIL-v3.

Lemus, S.M., F.J. Pino and M.P. Velthius, 2010. Towards a model for information technology governance applicable to the banking sector. Proceedings of the 5th International Congress on IT Governance and Service Management: Proposals for Tough Economics Times, June 10, 2010, Madrid, Spain, pp: 1-6.

Pardo, C., F.J. Pino, F. Garcia and M. Piattini, 2009. Homogenization of models to support multi-model processes in improvement environments. Proceedings of the 4th International Conference on Software and Data Technologies, July 26-29, 2009, Sofia, Bulgaria, pp: 151-156.

Pardo, C., F.J. Pino, F. Garcia, M.P. Velthius and M.T. Baldassarre, 2011. Trends in Harmonization of Multiple Reference Models. In: Evaluation of Novel Approaches to Software Engineering, Maciaszek, L.A. and P. Loucopoulos (Eds.). Springer-Verlag, USA., ISBN: 978-3-642-23390-6, pp: 61-73.

Pardo, C., F.J. Pino, F. Garcia, M.T. Baldassarre and M. Piattini, 2013. From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies. J. Syst. Software, 86: 125-143.

Pino, F.J., M.T. Baldassarre, M. Piattini and G. Visaggio, 2010. Harmonizing maturity levels from CMMI-DEV and ISO/IEC 15504. J. Software Maintenance Evol.: Res. Pract., 22: 279-296.

Sarbanes, P. and G. Oxley, 2002. Sarbanes-Oxley act of 2002. http://www.soxlaw.com/.

Siviy, J., P. Kirwan, J. Morley and L. Marino, 2008a. Maximizing your process improvement ROI through harmonization. Software Engineering Institute, Carnegie-Mellon University, Pittsburgh PA., USA., March 2008.

Siviy, J., P. Kirwan, L. Marino and J. Morley, 2008b. The value of harmonizing multiple improvement technologies: A process improvement professional's view. Software Engineering Institute, Carnegie-Mellon University, Pittsburgh PA., USA., March 2008.