Managing Information Security Risk Using Integrated Governance Risk and Compliance

Mathew Nicho
School of Computing and Digital Media
Robert Gordon University
UK
m.nicho1@rgu.ac.uk

Shafaq Khan
College of Engineering and IT
University of Dubai
UAE
skhan@ud.ac.ae

M.S.M.K. Rahman
Xpert Governance Consultancy
UAE
msmkrahman@gmail.com

***Abstract*— This paper aims to demonstrate the building blocks of an IT Governance Risk and Compliance (IT GRC) model as well the phased stages of the optimal integration of IT GRC frameworks, standards and model through a longitudinal study. A qualitative longitudinal single case study methodology through multiple open-ended interviews were conducted over a period of four years (July 2012 to November 2015) in a retail financial institution. Our empirical study contributes to both academic research and practice in IT GRC. First, we identified the various building blocks of IT GRC domain from vertical as well as horizontal perspectives. Second, we methodologically demonstrated the gradual metamorphosis of the evolution of an IT GRC from a single ITG framework to multiple IT GRC building blocks. The journey thus throws light on the gradual staged process of attaining maturity in IT GRC by an organization. The resultant IT GRC model thus, guides managerial actions towards a better understanding of the positioning of IT GRC building blocks in an organization through the understanding of the interaction of vertical and horizontal domains. The results of the paper thus enable practitioners and academics to better understand and evaluate IT GRC implementation for effective governance, reduce risk and ensure compliance in organizations.**

Keywords*— *IT GRC, IT governance, IT risk management, IT compliance, risk management, IT GRC model, integrated IT governance model.

I. INTRODUCTION

IT security has become a significant focus of governance, risk and compliance to mitigate business risks [1]. However, implementing GRC in organizations can be difficult [2], as the concept needs to be demystified and further investigated [3]. Subsequently, there is a lack of scientific research on an integrated approach to governance, risk management and compliance [4, 5]. The financial sector being one of the most regulated industries around the world [6-10], as well as heavily dependent on IT [11] has been among the most intensive users of information technology [12]. Consequently, this dependency on IT by the financial sector requires them to have a more solid and broad IT governance framework [13]. Information technology plays a crucial role in the development of activities concerning banking organizations to achieve IT governance, while at the same time they give special consideration to the attainment of business objectives [14]. Issues generated by data protection, information privacy legislation, ethics and integrity regulations, IT governance (ITG) concerns, and regulations like Sarbanes Oxley Act has increased the scope of compliance imperatives [15]. In this regard, it was found that 90% of the organization in the financial sector have implemented, in the process of implementation and considering implementing IT GRC [16].

There is an ever-increasing demand for compliance in the information systems domain [2]. In this respect, internal control mechanisms play an important role in assisting enterprises to avoid risk [17]. Thus post 1990s, nationally and internationally, there has been greater focus by organizations on corporate governance and risk management [18]. This has forced organizations to comply with multiple and overlapping regulations resulting in major audit fatigue [19]. To manage the increasing business and operational risks inherent to competing in a complex global market, integrated GRC has become one of the most important business requirements for organizations [5]. Subsequently, GRC is considered an emerging topic in the business and information technology world [4]. Being critical for organizations, there is a need to support this by information and communication technologies (ICT) [20]. But the main challenge behind GRC concept is that the integration of these three areas (governance, risk and compliance) is generally dealt with in silos [21]. This leads us to the research question - ***How do organisations integrate and built an IT GRC model from a financial sector perspective?*** While our research question seeks to explore the answer for 'how', this further raises the question of 'what' IT GRC frameworks/standards/models/best practices (hereinafter referred to only as 'IT GRC frameworks' in this paper) to select and integrate. This paper thus aims to identify the IT GRC frameworks, as well the integration methodology leading to an integrated IT GRC model through a single case study.

978-1-5386-2752-5/17/$31.00 ©2017 IEEE

The rest of the paper is structured as follows. Section 1 provides the background to IT GRC and related concepts, while section 3 presents the different perspectives of IT governance to identify the IT GRC frameworks that have been proposed and used within the IT GRC domain. Section 4 presents the integrated IT GRC concept, while section 5 outlines the methodology of the empirical research. Section 6 presents the phased evolution of the IT GRC model followed by conclusion

II. Background Literature on GRC and IT GRC

A. GRC Defined

GRC is not a new concept since its components have been executed mostly in a fragmented manner, but the fact that organizations took a united perspective of this concept for creating added-value and realizing the competitive advantage, gave it a new perspective [20]. While GRC has come into increasingly common use, there is no proper universal understanding of the term or its objectives [22]. Thus, there is no single, commonly accepted definition of GRC [23]. From a process perspective, GRC describes different organizational activities, from arranging an annual (audit to the establishment of internal continuous control monitoring procedures, to set up roles and responsibilities in business processes and the system users, to data analytics procedures [3]. However, a holistic definition of GRC was given by [24, p.8] who defined it as:

"an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations, through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness."

An integrated holistic approach to GRC enables the organization to realize the value out of GRC framework implementations. First, GRC integrates a risk-based management approach that is proactive, effective, and can be used throughout an organization [2]. Second, GRC calls for a common infrastructure with collaborative processes to manage risks and is the product of 2002 Sarbanes- Oxley Act [25]. Third, GRC being cross-functional establishes a harmonized approach and communications network between existing mission-critical executives and departments [26] thus enabling seamless integration of GRC frameworks. Fourth, an integrated set of concepts covering governance, risk and compliance frameworks when applied holistically within an organization, can add significant value and provide competitive advantage [24]. But the main challenge behind GRC concept is the integration of these three areas (G, R and C) is generally dealt with in silos [21].

B. IT GRC

IT GRC being a subset of GRC with IT governance, IT risk management and IT compliance as the three main constructs [27], subsequently takes on the benefits of GRC with added IT oriented benefits (see fig. 1).

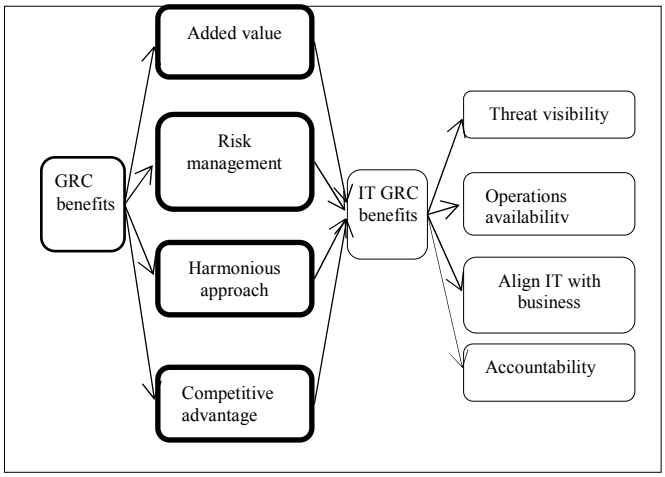

Fig. 1. Benefits of an integrated IT GRC model

An IT GRC approach integrates and automates the essential activities and promotes a level of visibility (threat) into effective and ineffective technical controls and gaps that threaten the confidentiality, integrity, and availability of key business operations and initiatives [19]. IT GRC ensures organizations not only to implement appropriate management techniques and methodologies to align business strategies and IT, but also controls the management of industry standards, technological risks, and regulatory compliance requirements facing IT organizations to ensure accountability [28].

C. IT GRC in Organizations

Despite the increased attention on GRC over the last few years, there is a lack of research on an integrated approach to GRC [27]. It has been argued that the GRC literature is limited [29], is a less researched field, and much of the information is yet to be aggregated [4]. Although there is a history of literature under the separate headings of governance, compliance and risk in various domains, there is little research covering the new integrated cross-domain, multi-jurisdiction, multi-disciplinary regulatory environment [30]. Subsequently, there is lack of scientific research on an integrated approach to governance, risk management and compliance [4, 5], as implementing GRC in an organization can be difficult [2]. Although companies are increasing their focus on GRC, most of them continue to have a fragmented and overlapping approach to GRC implementation [31]. Thus, while GRC provides a way to align governance, risk, and compliance in a more efficient and effective manner, presenting this framework to key stakeholders and non-practitioners in a simple manner is a challenging task [2]. This necessitates the need for an integrated IT governance model to address IS/IT challenges to the whole corporation [32]. It has been stated that the multiple compliance and risk endeavours result in silos operating isolated from each other [33]. Although practitioners have mapped the alignment between IT-related standards, this work

has rarely been reported in the academic literature [34]. Thus, in our view, not enough attention has been paid to the integration of disparate IT GRC frameworks to assist the wider academic and practitioner community. While, guidance has been given on how to use commonly used IT frameworks namely COBIT, ITIL and ISO17799 in conjunction [35] by practitioners and academics, a comprehensive methodology of integration covering relevant IT GRC frameworks is lacking.

III. FRAMEWORKS FOR IT GRC

The role of ITG frameworks is of relevance to IT GRC, since it is viewed as an approach to align IT with business [36-40]. Optimal integration of relevant IT governance frameworks thus ensures alignment of IT goals with business goals. Apart from the core benefit of alignment, IT governance consists of policies and procedures with appropriate controls for monitoring IT risks, controlling IT assets, compliance with laws and regulation and records management [41] thus encompassing the concepts of governance, risk and compliance. Hence, ITG frameworks provides the building blocks of an IT GRC model.

IT governance is implemented using ITG frameworks each having its own pre-defined set of ITG sub domains. A global survey revealed that external ITG frameworks used in the enterprise governance of IT as ITIL/ISO 20000, ISO 17799/ISO 27000, Six Sigma, COBIT, PMI/PMBOK, Risk IT, IT Assurance Framework, CMMI, ISO 38500, Business Model of Information Security, PRINCE 2, Val IT, TOGAF and COSO ERM [42] with each of them focusing on a different aspect of a company's IT [43]. From a practitioners perspective, the most commonly mentioned IT-related frameworks are the COBIT, ITIL, the Integrated Capability Maturity Model (CMMi), Six Sigma and the International Standards Organization (ISO) Standards number 17799 and 9000 [44]. Two frameworks commonly used for IT governance implementations are COBIT [45, 46]; and ITIL [47]. COBIT was developed to promote effective IT governance [48] while ITIL is a set of books describing best practices in several areas of service management [49] to promote efficient and cost-effective IT operations [50]. As frameworks, COBIT, ITIL and ISO 17799 are useful for the growth and success of an organization since an implementation of these ensures better ROI on IT investments, serves a guideline for compliance, reduces risks, optimizes costs and helps in benchmarking [7].

While generic ITG frameworks have been used in integrated ITG implementations, there are instances of using specific IT related models, like the software development life cycle (SDLC) used in the implementation of ITIL [51], and integrated with project management [52]. With multiple ITG frameworks to choose from, practitioners lack guidance on the selection of ITG frameworks for IT GRC.

IV. IT GRC INTEGRATION

Given the various ITG frameworks and best practices, finding the optimal mix for integrating and implementing ITG frameworks is a major challenge [53] due to their inter-relationships [54]. This difficulty of integration is influenced by many factors namely the complexity of implementing multiple frameworks simultaneously; the reduced learning curve for new hires; the conflicts among IT management, staff, and stakeholders created by differences in their interests regarding ITG framework adoption; the significant burden organizational change can place on staff, creating increased stress and reduced morale and productivity; and staff's need to manage ITG implementation through real work [54]. Other factors like terminology used by different frameworks [55] and costs involved [56] also pose challenges in this kind of integration.

Mapping/integrating relevant ITG frameworks has been recommended and done for various reasons by academics and practitioners alike due to 'benefits' gained, 'ease' of compliance, 'increased performance', being 'complementary' in nature, as an aid for 'regulatory' compliance, to provide 'synergy', for ensuring a 'comprehensive' solution, to provide 'strategic' direction, for 'harmonizing' the different frameworks, for 'added value' to align IT goals with business goals, and 'strategic direction' (see Table 1). In this respect, COBIT has been mapped from four up to ten IT related frameworks including COSO, ITIL, PMBOK, and TOGAF [57]. While a review of the existing academic and practitioner's literature on IT GRC provided generic integration of a few ITG frameworks, a methodology for a comprehensive IT GRC model encompassing relevant ITG frameworks is lacking. Hence, a methodological study of an actual phased implementation can provide best practices in this regard.

TABLE 1. MAPPING/INTEGRATING ITG FRAMEWORKS

Mapping/integrating of ITG frameworks	Reasons of Integration	Sour -ces
COBIT and PCI DSS 2.0	*Increased performance* and ease of *compliance*	[61]
COBIT, ITIL and ISO 17799	For achieving business *benefit*	[62].
COBIT and ISO 17799 (ISO 27000)	Reference frameworks for information security governance and to provide *synergy*	[63].
ITIL, COBIT and the standard, ISO/IEC 27002	For *comprehensive* IT management system	[64]; [65]
COBIT and Sarbanes-Oxley	*For* guidance in implementing *regulations*	[66]
COBIT, Balanced Scorecard and SSE-CMM	For a *strategic* Information Security Management (ISM) framework.	[67]
COBIT 4.1, Basel II, VAL IT, RISK IT, ISO 27002 and ITIL V3	To *harmonize* IT governance	[68]
ITIL V3 and COBIT 4.1	Complementary – to add value.	[47]

V. RESEARCH METHODOLOGY

IT GRC being a relatively recent topic with much of the existing information yet to be aggregated, an interpretive study is deemed suitable since, it has the potential to produce deep insights into the development and management of information systems phenomena [58]. Since deploying IT GRC involves change, the interpretive paradigm provides a deeper understanding of the underlying process of organizational change within the context of an information system [59]

through a single case study. In a single-case design approach, a case should be critical, extreme, unique or revelatory [60]. The case being unique, the single case study method was employed to explore the IT governance, frameworks/standards deployed as well as the methodology of integration. The data collection which is done through interviews does not follow any rigid pattern, as the questions are based on pre-determined (and emerging themes, where the responses can be subjective based upon the respondents or organizational context. This aids to understand the phenomenon from the point of view of the participants and the particular context [69].

VI. ANALYSIS OF FINDINGS

The study was conducted over a period of four years starting from July 2012 to November 2015 in a retail bank in the United Arab Emirates. All interviews were physically conducted at the bank's head office in Dubai at the office of the IT Strategy Manager (main respondent). The organization is one of the pioneer local banks in UAE started in the year 1969. It follows a very conservative approach in banking operations keeping in mind customer information and interests are protected to the maximum. In this regard we were given permission to interview only the IT Strategy Manager who in turn interviewed appropriate bank staff to get specific information, which was passed on to us during subsequent interview sessions. Thus, he maintained respondent anonymity throughout the interview sessions. The main respondent has 35 years of experience working at strategic levels in multinational banks in Asia. A total of eighteen interviews were conducted with the main respondent over the said period which were digitally recorded, transcribed and validated during subsequent sessions by the respondent. The corrected transcribed version was imported into the qualitative software NVIVO to extract the themes (nodes) based on chronology, domains, and ITG frameworks. In line with the interview sequence, the responses were categorized into five phases (phase 1 to 5) leading to the IT GRC model.

A. Phase – 1 (initiation 2004 – 2)

The initiation of the ITG implementation process started in the year 2004, where they migrated to a new core banking application system. This necessitated them to review and plan the service architecture which in turn prompted them to put IT controls in place For this in 2006 they hired a senior IT manager who was entrusted with the task of implementing an IT strategy with the aim of aligning IT goals with business goals. In this respect the IT strategy manager was entrusted with task of not only realigning the existing IT goals to business goals but also set new IT goals to achieve business goals:

B. Phase – 2 (planning 2006 - 2007*)*

In 2006, the management decided to implement best practices and standards in the IT department starting with service management for which the main reason given was to keep the systems live at any point of time. At that time, the senior IT manager acknowledged the role of an IT governance model in any 'integrated multiple implementations of best practices'. The bank has been following the traditional help desk approach where the focus was on helping the employees solve the IT issues rather than providing IT as a service. During the gap analysis process, the IT strategy manager selected ITIL framework as a method to implement IT service management (ITSM) concepts which required change in people, process and technology.

Three core areas of change: To initiate ITG implementation, the bank identified three core areas of change namely people, process and technology. According to the senior IT manager, change is required in three areas namely people, process and technology to start an integrated ITG implementation process. He further stated that people has an important role to play since they have to be knowledgeable to understand the process. This is followed by IT processes where each process related to information systems has to be defined. Technology, which encompasses frameworks and automated tools, provide a road map of best practices implementation. This is considered a cycle due to the dynamic change in IT and business where people need to be continuously updated and trained; the existing process need to redefined and/or new process defined, due to the periodic updates/versions in the technology. In this respect the bank follows the 90/10 rule where people and process consume 90 percent of the change management effort while technology consumes the rest 10 percent. When quizzed regarding the success of this model, the IT Strategy Manager replied:

"Implementing best practice means process (change) improvements, for efficiency. This is a major challenge where process involves people. Generally, many people find that it is easier to keep doing what has been done rather than implementing change which is human nature. Technology tools are an important aspect, but in order to be effective, they require qualified and skilled people. So, to make process to work effectively we need to acquire knowledge (what) and skills (how). This clarifies the 90/10 rule"

In an effort to impart awareness, trainings (leading to industry certifications) were conducted to facilitate people's skills and expertise. This was done while implementing/enhancing the processes based on best practices. As a monitoring mechanism, key performance indicators (KPIs) were assigned to people to measure the success criteria.

C. Phase – 3 (ITSM implementation 2007 - 2010*)*

For IT service management, the company has been following the traditional 'helpdesk' approach. This concept was changed to 'service desk' in 2007 as, according to the respondent help desk "is no more required, because we are not here to help. It should be a service desk, where, we should be providing service to people". ITIL was chosen as the framework as it takes care of the day to day IT operational activities. They implemented a service management tool, with a webpage where people can log in a request as well as report an incident where the service desk analysts can take action. Since people log in with their incidents they implemented incident management process. This was followed by the problem management process which involves analyzing the reported incidents to get into the root cause of the problems.

1) Certification as a Change Management Process: Involvement of people being a foremost requirement for any change management process, the company identified and conducted about five batches of ITIL training, leading to ITIL foundation certification to 52 employees. This gave an opportunity to those staff to understand IT service management processes. Through this method, the IT service management concept was sold to the employees which eventually motivated them to follow the concept. This process of involving and enriching the IT personnel helped them to understand ITIL best practice. To enhance the change management process, towards the middle of 2010, they sent seven people for project management institute (PMI) training and subsequent certification. According to the respondent, "change management and project management go side by side" which is one of the reasons for the parallel initiation of both. In the project management process, they had put all of the required documentation for each phases of the project management life cycle (PMLC).

2) The Push Approach Realizing the need for a driver to implement the numerous IT processes and IT controls, (towards the end of 2010), the IT Strategy Manager started planning for an integrated IT governance framework by following industry best practices. During this time, the IT department developed new policies and standard operating procedures for IT operations keeping the new ITG controls in mind. In this regard, respondent states that the "implementation of the integrated ITG framework is critical as it drives (push) the IT governance process which is the IT policy and IT operations, followed by the procedure for each and every IT process/control". Thus, policy governs the procedure and the procedure has the controls to operate (see fig. 2).

D. Phase – 4 (IT Governance Implementation 2010 - 2012)

During this phase, the organization focused their effort to implement an integrated ITG framework. Apart from the 'push' factor, another reason to follow an integrated ITG framework approach is to integrate quality management, service management, security management and project lifecycle management. These different but overlapping pillars form the support for the holistic IT governance framework. In order to execute the integrated ITG framework they developed and followed a strategic planning road map for guidance integrating business and IT.

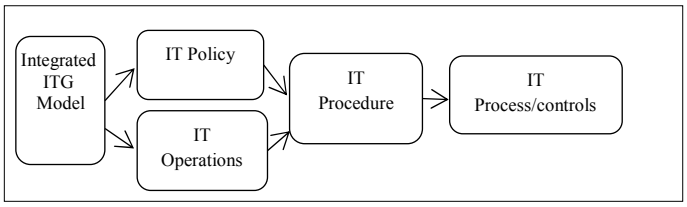

Fig. 2. Integrated ITG as a driver to implement the various IT processes/controls

1) The strategic planning road map. At the start of this phase, the strategic planning department analyzed the bank's business strategy to formulate the IT Strategic plan from a strategic level, the technical level, up to the staffing level using the bank's customized roadmap (see fig. 3) with inputs coming from business and IT. This was an exercise done to identify, evaluate and deploy relevant frameworks to embed into the proposed integrated ITG framework. Since the selection process involved only strategic level, this level has been expanded into six stages.

Strategic level: The strategic level stage involves the following sequential processes namely strategy development, business-IT alignment, developing a balanced score card, choosing an umbrella framework, selecting the supporting frameworks groups (pillars) and resulting in an initial integrated IT GRC model.

Stage 1- Strategy development: The initial phase of the IT strategic planning road map involved the development of the IS strategy where the management asked four questions namely 'why', 'what', 'how', and 'who'. Once the question, 'why' which clarifies the rationale for an IT strategy, was ascertained, the management proceeded to explore the question, 'what' which specifies the nature of strategy that needs to be created. This was followed by the 'how' question, which answers the nature of information technology, required to implement and protect the organizations information systems, which they termed it as the 'information technology strategy'. The last question, which is 'who' identified the target of the whole exercise which is to follow the management strategy.

Stage 2 - Business–IT alignment: As part of strategic alignment of objectives, the bank captured the strategic priorities (corporate objectives) from the top management, aligned the IS strategy with the strategic plan and allocated measurable goals and objectives in support of the IS strategy. This was followed by ongoing mutual discussion and understanding with the top management on the role of IT in support of this strategy. Since the use of the balanced scorecard approach has become an acceptable approach for evaluating IT performance [70] the management decided to introduce the balance scorecard (BSC) as a tool to measure the KPIs.

Stage 3 - Developing the balanced score card: This phase of the road map involved conceptualizing the alignment of business goals to IT goals. This was done by cascading the higher-level goals down to KPIs. The strategic mapping of BSC comprises of three fundamental strategic zones namely the strategic visionary statements, the strategic intent and the strategic alignment using derived KPIs, where the first two combine to create the strategic picture. Strategic visionary statements spell out the core goal, vision, mission group, SWOT statements, values, policies, and procedures. The strategic intent is a road map which provides the themes, perspectives, and objectives in a row-aligned flow chart. The strategic alignment zone using derived KPIs ensure that the objectives cascade into the BSC grid with user defined columns like KPI, KRA, measure, score and next review.

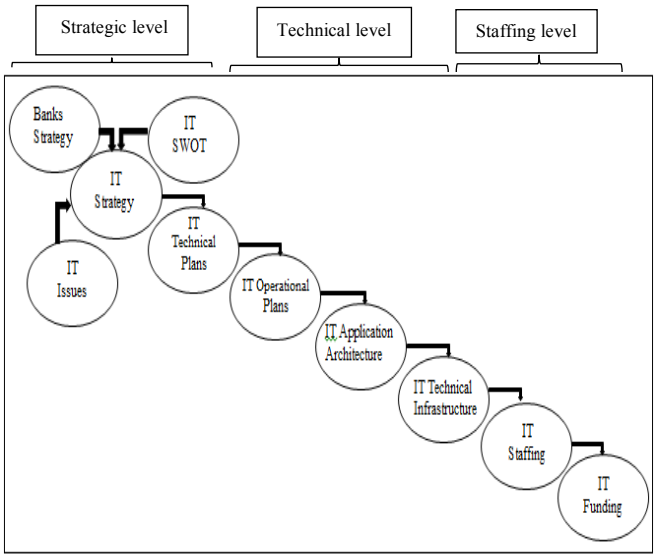

Fig. 3. The IT Strategic planning roadmap

Stage 4 - Umbrella framework: This involves selecting an umbrella framework to align relevant ITG frameworks into an integrated whole (fig. 4), for which COBOT was identified. COBIT is widely accepted and used internal control framework for IT [46, 71-74]. The framework describes several specific IT control and security processes that an organization can use to enhance its ability to achieve its business goals and to improve internal control [75].Moreover, it is considered to be the most appropriate control framework available to align information systems and business goals [76]. It cross-references all relevant, internationally recognized standards and frameworks such as ITIL, CMM, PMBOK, PRINCE 2, COSO, and ISO standards [77]. The bank thus selected COBIT as the IT governance framework model to act as an umbrella for the selected standards and frameworks due to the following reasons:

- they do have an annual COBIT audit from the Dubai government audit department,
- it covers all the domains of IT from corporate governance to align business and IT,
- provides the relevant control processes,
- allows a bottom up approach of implementation where the controls of the individual frameworks can be ultimately mapped up to reach the COBIT processes/controls/practices,
- it's a comprehensive governance model.

According to the bank, an umbrella framework aids in integrating the different IT GRC frameworks, standards and processes.

Stage 5 - Supporting Pillars: Since the bank had already implemented and got familiar with ITIL best practices, they proceeded to implement further two related standards, one quality standard and a project management framework namely ISO 20000, ISO27000-2005, ISO 9001 and PMBOK. The standards were chosen based on relevance, ease of

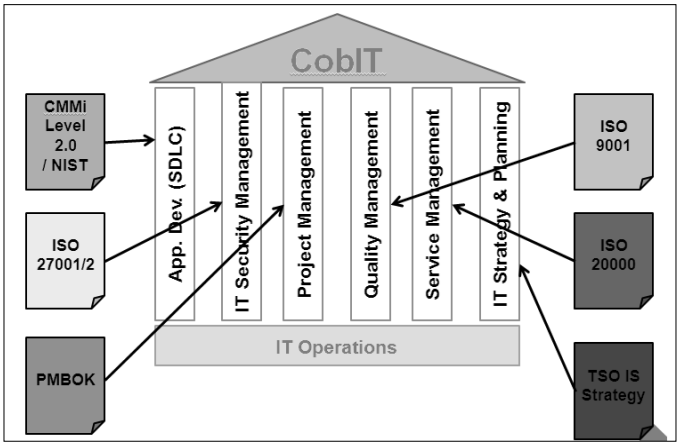

Fig. 4. The integrated IT governance model

implementation and gaining certification. From the bank's perspective, ISO9001 was the easiest to implement which was completed during the year 2010. Moreover, it provided them a foundation to build upon to reach the COBIT umbrella. Subsequently, ISO 20000 and ISO 27 K was implemented in parallel.

Stage 6 - Implementation: Using a bottom-up approach, the implementation started from the pillar and reached the top (COBIT) where respective IT processes/controls of the standards are selected, mapped with the respective IT processes (of the frameworks like ITIL) of COBIT. In the integrated ITG model, the bank started with quality management (aligned with ISO 9001) for which the reason given was its ease of implementation. This was followed by continuing the service management concept (aligned with ISO 20000) started in the previous phase and concurrently implementing security management (aligned with ISO 27000). The frameworks, standards and processes were enclosed as pillars subsequently named as management domains. In this regard, six management domains were identified namely application development, IT security management, project management, quality management, service management, and IT strategy & planning which are explained below:

2) Certification as a Change Management Process. The end of phase – 4 marked the emergence of the integrated ITG model which demonstrated not only 'building blocks' (what), but also the rationale as well as the integration methodology (how) of the integrated ITG model thus answering the second research question. The model encompasses two compliance frameworks namely COBIT (local government compliance) and PCI DSS (international). With the passing of the Executive Council Resolution No. 13 of 2012 – regarding the information in the Government of Dubai ("Dubai Information Security Resolution"), implementation of various industry standards like ISO/IEC 27001 and PCI DSS (for organizations handling with credit card data) is recommended for all organizations. While all the frameworks and standards are considered in ITG implementation to integrate processes, ISO 27K and PCI DSS form part of Dubai government regulatory requirements. In this respect, they started that "IT is a

customer service entity; quality is a mandatory process, while all the other processes are supportive".

The process frameworks overlap with other such that there is a considerable level of horizontal mapping between the controls of these frameworks, unlike management frameworks which are siloes by itself. From a vertical perspective, they have employed bottom up approach to map the management frameworks into the 210 COBIT 4.1 controls via the process frameworks.

Application development: This pillar encompasses software-development life cycle (SDLC), CMMI, PCI DSS (embedded into NIST), which was introduced at the end of the previous phase. According to the IT strategy manager "NIST being a very comprehensive framework, it can be used across all pillars, and we have deployed the NIST component for SDLC on our bank". While following the SDLC waterfall approach for developing and/or implementing software and IT projects, the bank realized the advantage of linking SDLC with the above frameworks. In this respect, they stated that "SDLC provides a discipline for IT development using the waterfall method where it streamlines the control process in software development". CMMI was used for benchmarking the process maturity in the SDLC and aligned to COBIT control processes because that was part of the SDLC requirement, and it helped them to assess the maturity level within the organization. Regarding security aspect of the SDLC, PCI DSS became mandatory and NIST was chosen for security within the SDLC. In this aspect the bank stated: "Even though PCI DSS is a regulatory requirement set by credit and debit card authorities namely VISA and MASTERCARD, Dubai government made it mandatory for the banking sector".

IT security management: According to the IT Strategy Manager "IT security management pillar is a requirement for ensuring security control standards for the entire ITG framework." Even though, the bank has its own security systems in place, they decided to follow ISO 27001 and ISO 27002 standards which were embedded into the bank's IT policies and procedures.

Project management: PMBOK was selected to aid in project management in 2007, where they put all of their PMO documents as a supplement followed by policies, standing operating procedures, template and user guides including the characteristic of each procedure. They decide to follow PMBOK rather than PRINCE due to its (PMBOK) widespread deployment in the Middle Eastern region which also gave them the benefit to benchmark against other banks.

Quality management: In the bank's ITG framework, all relevant frameworks and frameworks and standards have been integrated together through mapping to develop a governance framework. For any processes, quality being a primary requirement, ISO 9001 was selected to implement the baseline processes and related documents.

Service management: In this ITSM pillar, the chosen ITIL processes (aligned with ISO 20000 for certification) were incident management, change management, and problem management. The rationales for going for these processes were to manage and improve the service management process as priority.

IT strategy and planning: COBIT is an umbrella framework used by the bank for methodological alignment. Out of the specific standards and process frameworks deployed under the COBIT umbrella, technical standards order (TSO) was removed as other management processes were complementing each other. Towards the end of this phase, the bank implemented a complete business management system in place under the framework of COBIT and enterprise architecture using TOGAF 9 which covers the architecture aspects of IT governance controls, board and management expectations.

During the final stage of this phase a mapping of all included ITG frameworks was performed to integrate the relevant IT processes/controls of the ITG frameworks to link with relevant COBIT IT processes. It was during this time that the bank noticed that this integrated framework can be further improved through breaking down the pillars/domains into three inter-related components for clarification of the different components embedded in the pillars.

E. Phase – 5 (IT GRC Implementation 2012 – 2013)

The IT GRC model (Research question 1): During this phase, the bank further integrated ITG domains along with the governance, process and management framework, including best practices such as ITIL, and standards such as ISO, thus answering the 'what' and 'how' of the integrated ITG framework, thereby answering the main question resulting in the IT GRC model for the financial sector. In this phase, the organization transformed the integrated IT governance framework into an IT GRC model (fig. 5) providing a generic view of the frameworks and the integration between domains which provides guideline for practitioners to optimally position future frameworks, standards, models and best practices.

The bank got the impetus to further improve the integrated ITG framework into a generic IT GRC model due to the (1) dynamic and ever increasing compliance and regulatory environment in the financial sector (2) the emergence of new frameworks, standards, models and best practices, where they need to correctly position these ITG frameworks. In this regard the IT strategy manager stated "instead of developing implementation guidance for each and every emergent mandatory or voluntary compliance requirement, let us come up with a prescriptive method" so that people know "how to implement and where to position it", and the IT GRC model is the answer to this.

Phase 5 is a mature phase which elaborates the role of each domain and applicable related framework. In this bottom up approach, they started with the management framework, followed by the IT controls and processes, and gradually moving up each level until they reached and aligned with the COBIT IT processes and practices. In the IT GRC model all the pillars in the integrated IT governance remains, except the IT strategy and planning pillar. This was removed in the IT GRC model, as the bank realized that the whole methodology of the IT GRC is driven by IT strategy & planning.

Below the domains, the pillars were further differentiated to accommodate domain specific process, and management

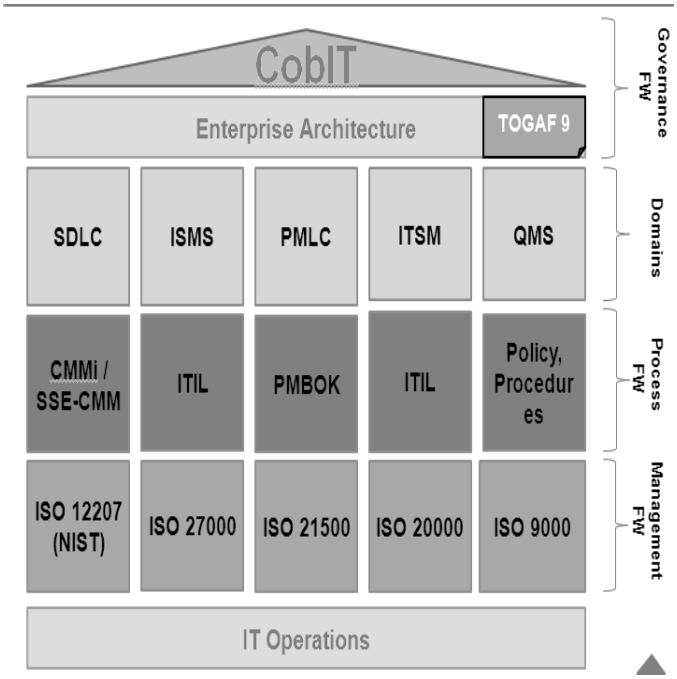

Fig. 5. The IT GRC Model (Retail banking sector)

frameworks. Since, GRC can be integrated horizontally and vertically [33], the vertically identified blocks represent the functional space of the IT domain, while the horizontal space provides the different perspectives of GRC.

Governance framework: The pillars were further differentiated into overall governance framework (identified in this model as COBIT and TOGAF). Enterprise architecture based on TOGAF 9 was introduced at this phase to develop a matured ITG framework and to govern the architecture of the IT infrastructure and related processes. Regarding the implementation of enterprise architecture, the bank is of the view that, they have decided to integrate the enterprise architecture concepts within the organization.

Domains: The identified domains are SDLC, information security management system (ISMS), project management life cycle (PMLC), ITSM and quality management service (QMS), process frameworks, and management frameworks. These domains relate to the functions within IT department of the bank.

Processes frameworks: Each domain we have to identify the process frameworks to define the processes. For example, SDLC we are using CMMI and SSE CMM. Similarly, for service management we are using the ITIL process framework.

Management frameworks: ISO is the management framework, where there are standard clauses and all the processes are aligned to these standard clauses, which can be monitored for improvement in plan-do-check-act (PDCA). It provides a complain perspective for the bank where all of these standards are externally audited.

IT operations: IT operations expectations are based on the functions of the IT Department and it operates as per defined processes which is in aligned to standards and best practices (see fig. 5). IT operations deliver IT services. IT operations

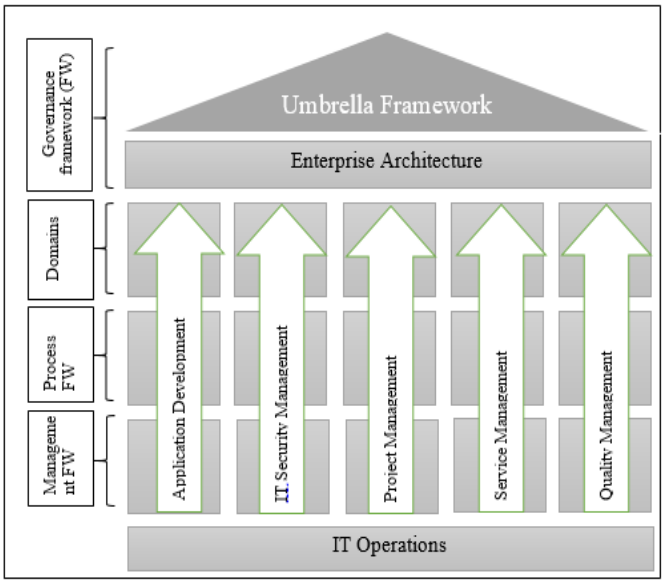

Fig. 6. IT GRC Model

is the execution part, while management direct the functions and control which explains the rationale for positioning IT operations below the management frameworks.

The pillars of the IT GRC model is similar to as described in section 5.4.2 except that in IT security management the security component evident in ITIL is mapped to the security functional space while the service component mapped to the service management functional space. The IT GRC model can be generically represented from a two-dimensional perspective (fig. 6) to illustrate the vertical and horizontal spaces. Being a bottom-up approach, the vertical space starts from the bottom and eventually maps up to the umbrella framework. It should be, however, noted that due to varying levels of overlaps of the functional spaces of the IT domain as well as the perspectives of enterprise GRC the different components of IT GRC buildings blocks may be represented in in more than one vertical or horizontal spaces

VII. Conclusion and Future Research Directions

Our empirical study contributes to both academic research and practice by reducing the gap between these two fields. The model guides managerial actions towards a better understanding of the positioning of IT governance frameworks in an organization through the understanding about the interaction of vertical and horizontal domains. From an academic as well as practitioner's perspective, this model provides a taxonomy to categorize relevant frameworks, standards, best practices and models into meaningful vertical and horizontal spaces. From an implementation perspective the journey throws light on the gradual staged process of attaining maturity in IT GRC by an organization. One of the unique features of the IT GRC model is its scalability as it can be expanded from a horizontal or vertical perspective taking into account major emergent themes and domains. Since our theoretical model explains the 'what', 'how' (process) and 'why' (reasons) of IT GRC implementation, we categorize the model under the type 2 theory of explaining and understanding

[78]. In this regard, our research enabled us to build validated theoretical constructs from case-based empirical evidence [79]. Accordingly, this contribution provides researchers and practitioners with guidance on the type of frameworks, standards, best practices and models to use in an ITG or integrated ITG or IT GRC implementations.

Being a longitudinal qualitative study, focusing on one organization has its own limitations, as such further studies in different sectors and cultures (internationally) are called for to validate and the model as well as generalize to a wider context. Another limitation we encountered is the restrictions on interviewing the members of the ITG, integrated ITG and IT GRC implementation team as all our queries were routed through the IT Strategy Manager to the staff of the IT department. Our interviews targeted only the staff of the IT department. Since, success and failure is a question of judgment, representing the different points of views of particular groups in an organization [80], we encourage researchers to examine the different views of stakeholders in the implementation process. Finally, due to privacy concerns, we were not able to get information on the specific IT processes/controls used in the various stages of IT GRC model. Taking the IT GRC model we encourage researchers to hypothesize and generalize the results through quantitative methods. While going through entire journey of the IT GRC implementation in the bank, one researchable topic that emerged is the development of a maturity model for IT GRC. Researchers are encouraged to delve into this new domain to come up with a maturity model for IT GRC implementation.

REFERENCES

[1] S. Bradley, "How to use analytics to enhance security," Risk Management, vol. 63, p. 14, 2016.

[2] J. Tadewald, "GRC Integration: A Conceptual Foundation Model for Success," Management Accounting Quarterly, vol. 15, p. 10, 2014.

[3] A. Papazafeiropoulou and K. Spanaki, "Understanding Governance, Risk and Compliance Information Systems (GRC IS): The Experts View," Information Systems Frontiers, pp. 1-13, 2015.

[4] N. Racz, E. Weippl, and A. Seufert, "A Process Model for Integrated IT Governance, Risk, and Compliance Management," in Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), 2010, pp. 155-170.

[5] P. Vicente and M. M. da Silva, "A Conceptual Model for Integrated Governance, Risk and Compliance," in Advanced Information Systems Engineering, 2011, pp. 199-213.

[6] F. R. Edwards, "Managerial Objectives in Regulated Industries: Expense-Preference Behavior in Banking," The Journal of Political Economy, pp. 147-162, 1977.

[7] D. C. Hardy, "Regulatory Capture in Banking," IMF Working Paper2006.

[8] P. G. Klein, "Information, Incentives, and Organization: The Microeconomics of Central Banking," in The Fed at One Hundred, D. H. a. J. T. S. (eds.), Ed., ed Switzerland: Springer International Publishing 2014.

[9] J. A. C. Santos, "Bank Capital Regulation in Contemporary Banking Theory: A Review of the Literature," Financial Markets, Institutions & Instruments, vol. 10, pp. 41-84, 2001.

[10] C.-C. Yang, "Evaluating the Performance of Banking Under Risk Regulations: A Slacks-Based Data Envelopment Analysis Assessment Framework," Expert Systems, May 2014, Vol. 31, No. 2, vol. 31, pp. 176-184, 2014.

[11] A. Joshi, L. Bollen, and H. Hassink, "An empirical assessment of IT governance transparency: Evidence from commercial banking," Information Systems Management, vol. 30, pp. 116-136, 2013.

[12] A. Farhoomand and M. Huang, "Does IT payoff? Strategies of Two Banking Giants," Communications of the Association for Information Systems, vol. 24, p. 47, 2009.

[13] S. D. Haes and W. V. Grembergen, "An Exploratory Study into the Design of an IT Governance Minimum Baseline through Delphi Research," Communications of the Association of Information Systems, vol. 22, pp. 442-458, 2008.

[14] S. M. Lemus, F. J. Pino, and M. P. Velthius, "Towards a model for information technology governance applicable to the banking sector," in Information Systems and Technologies (CISTI), 2010 5th Iberian Conference on, 2010, pp. 1-6.

[15] T. Butler and D. McGovern, "A Conceptual Model and IS Framework for the Design and Adoption of Environmental Compliance Management Systems," Information Systems Frontiers, vol. 14, pp. 221-235, 2012.

[16] ITGI, IT Governance Global Status Report. Rolling Meadows, Illinois: IT Governance Institute, 2008.

[17] H. Elbardan, M. Ali, and A. Ghoneim, "Enterprise Resource Planning Systems Introduction and Internal Auditing Legitimacy: An Institutional Analysis," Information Systems Management, vol. 33, pp. 231-247, 2016.

[18] P. McGee. (2001, 3). Integrating Governance, Risk and Compliance: Why and How. Available: http://search.informit.com.au/documentSummary;dn=907594378164023;res=IELBUS

[19] H. M. Kominars, "IT GRC Aims for Performance Gain: Auditors can Leverage an IT Governance, Risk, and Compliance Approach to Meet the Increased Demand for Assessing Risks and Controls," Internal Auditor, vol. 68, pp. 63-65, 2011.

[20] A. Shahim, R. Batenburg, and G. Vermunt, Governance, Risk and Compliance: A Strategic Alignment Perspective Applied to Two Case Studies: Springer, 2012.

[21] N. Mayer, B. Barafort, M. Picard, and S. Cortina, "An ISO Compliant and Integrated Model for IT GRC (Governance, Risk Management and Compliance)," in Systems, Software and Services Process Improvement, ed: Springer, 2015, pp. 87-99.

[22] M. L. Frigo and R. J. Anderson, "Strategic Risk Management: A Foundation for Improving Enterprise Risk Management and Governance," The Journal of Corporate Accounting & Finance vol. March/April, pp. 81-88, 2011.

[23] N. Marks, "Defining GRC," Internal Auditor, vol. February, 2010.

[24] N. Racz, E. Weippl, and A. Seufert, "A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)," in Communications and Multimedia Security, 2010, pp. 106-117.

[25] R. Banham. (2007). Is ERM GRC? Or Vice Versa? Available: http://www.treasuryandrisk.com/2007/06/01/is-erm-grc-or-vice-versa-

[26] P. Wechsler. (2007, The GRC Harmony. Treasury and Risk Magazine June.

[27] N. Racz, E. Weippl, and A. Seufert, "Integrating IT Governance, Risk, and Compliance Management Processes," in Proceedings of the 2011 conference on Databases and Information Systems VI: Selected Papers from the Ninth International Baltic Conference, DB&IS 2010, 2011, pp. 325-338.

[28] S. Schlarman, "What ITIL can Teach IT-GRC. " EDPACS: The EDP Audit, Control, and Security, vol. XL, pp. 8-18, 2009.

[29] K. Spanaki and A. Papazafeiropoulou, "Analysing The Governance, Risk And Compliance (GRC) Implementation Process: Primary Insights," in ECIS, Netherlands, 2013.

[30] A. O'Neill, "An action framework for compliance and governance," Clinical Governance: An International Journal, vol. 19, pp. 342-359, 2014.

[31] S. Steffee, "GRC Conundrum: Companies Struggle to Bridge the Gaps Among Governance, Risk, and Compliance Activities," Internal Auditor, vol. 69, pp. 11-13, 2012.

[32] N. Korac-Kakabadse and A. Kakabadse, "IS/IT Governance: Need for an Integrated Model," Corporate Governance, vol. 1, pp. 9-11, 2001.

[33] N. Racz, J. Panitz, M. Amberg, E. Weippl, and A. Seufert, "Governance, Risk & Compliance (GRC) Status Quo and Software Use: Results from a Survey Among Large Enterprises," Governance, vol. 1, pp. 1-2010, 2010.

[34] G. Ridley, J. Hartnett, and W. Jarern-Imakul, "Mapping Information Security Standards: A Counter-Terrorism Example," in ECIS, 2008, pp. 1370-1381.

[35] A. Hoekstra and N. Conradie, "CobiT, ITIL and ISO17799 How to Use Them in Conjunction," PriceWaterHouse presentation [On-line. Last accessed: February 11, 2004], 2002.

[36] W. V. Grembergen, S. D. Haes, and J. Moons, "Linking Business Goals to IT Goals and COBIT Processes," Information Systems Control Journal, vol. 4, pp. 18-22, 2005.

[37] W. V. Grembergen, S. D. Haes, and E. Guldentops, "Structures, Processes, and Relational Mechanisms for Information Technology Governance: Theories and Practices," in Strategies for Information Technology, W. V. Grembergen, Ed., ed London: Idea Group Inc, 2004, pp. 1-36.

[38] S. K. McGinnis, L. Pumphrey, K. Trimmer, and C. Wiggins, "Sustaining and Extending Organisational Strategy via Information Technology Governance," in 37th Hawaii International Conference on Systems Sciences, Hawaii, 2004.

[39] E. Wessels and J. v. Loggerenberg, "IT Governance: Theory and Practice," in Conference on Information Technology in Tertiary Education, Pretoria, South Africa, 2006.

[40] Q. Liu and G. Ridley, "IT Control in the Australian Public Sector: A International Comparison," in Thirteenth European Conference on Information Systems, Regensburg, Germany, 2005.

[41] S. Hamaker, "Spotlight on Governance," Information Systems Control Journal, vol. 1, pp. 15-19, 2003.

[42] ITGI, Global Status Report on the Governance of Enterprise IT (GEIT). Illinois: ISACA & IT Governance Institute, 2011.

[43] M. Niemann, J. Eckert, N. Repp, and R. Steinmetz, "Towards a Generic Governance Model for Service Oriented Architectures," in AMCIS, 2008, p. 361.

[44] L. Gerke and G. Ridley, "Towards an abbreviated COBIT framework for use in an Australian State Public Sector," in 17th Australasian Conference on Information Systems, Adelade, 2006.

[45] W. Brown and F. Nasuti, "What ERP Systems can Tell us about Sarbanes-Oxley," Information Management and Computer Security, vol. 13, pp. 311-327, 2005.

[46] B. Moeller, K. Erek, F. Loeser, and R. Zarnekow, "How Sustainable is COBIT 5? Insights from Theoretical Analysis and Empirical Survey Data," 2013.

[47] F. Stevens, "Frameworks for IT Governance Implementation," in Enterprise IT Governance, Business Value and Performance Measurement, N. S. Shi and G. Silvius, Eds., ed: IGI Global, 2011.

[48] M. Marrone, L. Hoffmann, and L. M. Kolbe, "IT Executives' Perception of CobiT: Satisfaction, Business-IT Alignment and Benefits," in Proceedings of the Sixteenth Americas Conference on Information Systems, Lima, Peru, 2010.

[49] M. Winniford, S. Conger, and L. Erickson-Harris, "Confusion in the Ranks: IT Service Management Practice and Terminology," Information Systems Management, vol. 26, pp. 153-163, 2009.

[50] W.-G. Tan, A. Cater-Steel, and M. Toleman, "Implementing IT Service Management: A Case Study Focussing on Critical Success Factors," The Journal of Computer Information Systems, vol. 50, pp. 1-12, 2009.

[51] C. E. Pollard, D. Gupta, and J. W. Satzinger, "Teaching Systems Development: A Compelling Case for Integrating the SDLC with the ITSM Lifecycle," Information Systems Management, vol. 27, pp. 113-122, 2010.

[52] M. Leih, "The impact of the Sarbanes-Oxley act on IT Project Management," Journal of Information Technology Theory and Application (JITTA), vol. 8, p. 4, 2006.

[53] B. Von Solms, "Information Security governance: COBIT or ISO 17799 or both?," Computers & Security, vol. 24, pp. 99-104, 2005.

[54] A. Cater-Steel, W.-G. Tan, and M. Toleman, "Challenge of adopting multiple process improvement frameworks," in Proceedings of 14th European conference on information systems (ECIS 2006), 2006, pp. 1375-1386.

[55] J. Wallhoff, "Combining ITIL with COBIT and 17799," Scillani Information AB, 2004.

[56] P. Năstase, F. Năstase, and C. Ionescu, "Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises," Economic Computation & Economic Cybernetics Studies & Research, vol. 43, p. 16, 2009.

[57] S. De Haes, W. Van Grembergen, and R. S. Debreceny, "COBIT 5 and Enterprise |governance of information Technology: Building Blocks and Research Opportunities," Journal of Information Systems, 2013.

[58] H. K. Klein and M. D. Myers, "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," MIS Quarterly, vol. 23, pp. 67-94, 1999.

[59] D. Silverman, "Qualitative Research: Meanings or Practices," Information Systems Journal, vol. 8, pp. 3 - 20, 1998.

[60] R. Yin, Case Study Research: Design and Methods, 2nd ed. Thousand Oaks: Sage Publications, Inc., 1994.

[61] P. Bankar and S. Verma, "Mapping PCI DSS v2. 0 With COBIT 4.1," COBIT Focus, vol. 2, 2011.

[62] G. Hardy, "Guidance on Aligning COBIT, ITIL and ISO 17799," Information Systems Control Journal, vol. 1, 2006b.

[63] B. v. Solms, "Information Security Governance: COBIT or ISO 17799 or Both," Computers and Security, vol. 24, pp. 99-104, 2005.

[64] S. Sahibudin, M. Sharifi, and M. Ayat, "Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations," in Second Asia International Conference on Modelling & Simulation, Malaysia, 2008.

[65] M. Gehrmann, "Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive Information Technology for Management in Organizations," Navus-Revista de Gestão e Tecnologia, vol. 2, pp. 66-77, 2012.

[66] P. Thibodeau. (2006, 15th May) IT Auditors Turn to COBIT for Sarb-Ox-Guidance. Computerworld. 9.

[67] J. E. Goldman and S. Ahuja, "Integration of COBIT, Balanced Scorecard and SSE-CMM as an Organizational & Strategic Information Security Management (ISM) Framework," ICT Ethics and Security in the 21st Century: New Developments and Applications, pp. 277-309, 2011.

[68] C. Pardo, F. J. Pino, F. García, M. Piattini, M. T. Baldassarre, and S. Lemus, "Homogenization, Comparison and Integration: A Harmonizing Strategy for the Unification of Multi-models in the Banking Sector," in Product-Focused Software Process Improvement, ed: Springer, 2011, pp. 59-72.

[69] B. Kaplan and J. A. Maxwell, "Qualitative Research Methods for Evaluating Computer Information Systems," in Qualitative Research Methods for Evaluating Computer Information Systems, J. G. Anderson, C. E. Aydin, and S. J. Jay, Eds., ed Thousand Oaks, California: Sage Publications, 1994, pp. 45 - 68.

[70] N. Mohamed and J. Gian Singh, "A conceptual framework for information technology governance effectiveness in private organizations," Information Management & Computer Security, vol. 20, pp. 88-106, 2012.

[71] L. A. Leon, D. M. Abraham, and L. Kalbers, "Beyond regulatory compliance for spreadsheet controls: a tutorial to assist practitioners and a call for research," Communications of the Association for Information Systems, vol. 27, pp. 541-560, 2010.

[72] P. Drews, M. Morisse, and K. Zimmermann, "Towards a Concept for Integrating IT Innovation Management into Business IT Management," 2013.

[73] J. Etzler, "IT Governance According to COBIT," Master of Science, KTH Department of Electrical Engineering, Royal Institute of Technology, Stockholm, 2007.

[74] J. Rouyet-Ruiz, "COBIT as a Tool for IT Governance: between Auditing and IT Governance," The European Journal for the Informatics Professional, vol. 9, pp. 40-43, 2008.

[75] D. S. Kerr and U. S. Murthy, "The Importance of the CobiT Framework IT Processes for Effective Internal Control over Financial Reporting in Organizations: An International Survey," Information & Management, vol. 50, pp. 590-597, 2013.

[76] G. Ridley, J. Young, and P. Carroll, "COBIT and its Utitlization: A Framework from the Literature," in 37th Hawaii International Conference on System Sciences, Hawaii, 2004, pp. 1-8.

[77] B. Summerfield. (2005, 9th September). EU Selects COBIT as an Auditing Standard. Available: http://www.certmag.com

[78] S. Gregor, "The Nature of Theory in Information Systems," MIS Quarterly, pp. 611-642, 2006.

[79] K. M. Eisenhardt, "Building Theories from Case Study Research," Academy of Management Review, vol. 14, pp. 532-550, 1989.

[80] Y. K. Dwivedi, D. Wastell, S. Laumer, H. Z. Henriksen, M. D. Myers, D. Bunker, et al., "Research on Information Systems Failures and Successes: Status Update and Future Directions," Information Systems Frontiers, vol. 17, pp. 143-157, 2015..