A formal qualitative risk management approach for IT security

Bessy Mahopo
School of Computing
UNISA
South Africa
49020056@mylife.unisa.ac.za

Hanifa Abdullah
School of Computing
UNISA
South Africa
Abdulh@unisa.ac.za

Mathias Mujinga
School of Computing
UNISA
South Africa
mujinm@unisa.ac.za

***Abstract* - Information technology (IT) security, which is concerned about protecting the confidentiality, integrity and availability of information technology assets, inherently possesses a significant amount of risk, some known and some unknown. IT security risk management has gained considerable attention over the past decade due to the collapsing of some large organisations in the world. Previous investigative research in the field of IT security have indicated that despite the efforts that organisations employ to reduce IT security risks, the trend of IT security attacks are still increasing. One of the contributing factors to poor management of IT security risk is attributed to the fact that IT security risk management is often left to the technical security technologist who do not necessarily employ formal risk management tools and reasoning. For this reason, organisations find themselves in a position where they do not have the correct approach to identify, assess and treat IT security risks. Employing a formal risk based approach in managing IT security risk assist in ensuring that risks that matter to an organisation are accounted for and as a result, receive the correct level of attention. Defining an approach of how IT security risk is managed should be seen as a fundamental task, which is the basis of this research. The objective of this paper is to propose an approach for identifying, assessing and treating IT security risk which incorporates a robust risk analysis and assessment process. The risk analysis process aims to make use of a comprehensive IT security risk universe which caters for the complex and dynamic nature of IT security. The research will contribute to the field of IT security by using a consolidated approach that utilises coherent characteristics of the available qualitative risk management frameworks to provide a stronger approach that will enable organisations to treat IT security risk better.**

Keywords: IT security risk management, IT security risk analysis

I. INTRODUCTION

The rapid growth of society's dependence upon Information Technology (IT) has precipitated a growing apprehension about the security and reliability of this fragile infrastructure [1]. Organisations and individuals always find themselves under pressure to stay abreast with the current technology in order to run their businesses or their lives whereby their IT systems are open to the Internet [2]. There is a tremendous amount of innovation involved with technology which introduces a great deal of complexity within the IT environment; resulting in a significant number of IT security risks [3]. IT security is a complex topic and evolves almost as fast as technology does [2].

While research in IT security has started giving importance to IT security risk management, the focus is still on the development of procedural guidelines and a few semi-automated methods [2]. Several issues remain unsolved including the need of sophisticated formalisation in the risk management reasoning [2]. In order to bridge this existing gap, IT security risk should be considered as just another risk that needs to be managed alongside all other business risks, rather than treating it as an independent technical concern [6].

For these reasons, a robust IT security risk management process is required in order to manage IT security risks to a tolerable level [3][6]. This paper therefore presents a process that was employed to define the proposed IT Security Risk Based (ITSRB) approach, which may used as a blueprint as well as a mechanism that can be applied by organisations to respond to IT security risk better.

This paper is divided into four sections. Section two presents a summarised view of a comparative analysis of five best practice frameworks chosen for this research. The frameworks were chosen because they inherently possess some of the important attributes which are deemed as vital for the definition of the proposed ITSRB approach. Section three presents the attributes derived from the best practice frameworks discussed in section two, with the objective of building up the foundation of the ITSRB approach. Section four presents the proposed ITSRB approach including its structure and features. Section five concludes this paper by highlighting important aspects that were used to define the ITSRB approach as well as the current challenges that the discussed frameworks possess, addressed by the ITSRB approach. The last section presents the references which were used in this paper.

II. COMPARATIVE ANALYSIS ON SOME OF THE BEST PRACTICE FRAMEWORKS FOR IT SECURITY

This section describes some of the common IT security frameworks used within the South African financial institutions [31][32]. It is important to note that there are many other IT security frameworks within the current body of knowledge developed by local governments within different European countries such as: Austrian IT Security Handbook,

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

Cramm Tool developed by British Central Communication and Telecommunication Agency, Dutch A&K Analysis, Ebios (Expression des Besoins et Identification des Objectifs de Sécurité) from France, ISAMM (Information Security Assessment & Monitoring Method) from Belgium, etc. [35].

The frameworks were reviewed at a high level to understand the different perspectives applied across the globe to manage IT security risk. A high level review indicated that, there are significant similarities when it comes to the risk management approaches applied for IT security, with shortcomings in other areas, but most of these frameworks were customized for local government requirements [35]. The interest of this study was limited to the frameworks commonly used within the South African financial institutions to ensure a focused scope that is exhaustive.

Although the selected frameworks discussed in this paper approach the subject of IT security differently, their ultimate goal is to reduce IT security risk to an acceptable level as per the organisation's risk appetite [30][32]. The analysis presented in this paper, explore the selected frameworks with emphasis on their strong characteristics which are leveraged off in defining the proposed ITSRB approach.

The frameworks selected are: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), International Organisation for Standardisation 27001/2 (ISO 27001/2), Control Objectives for Information and related Technology 4.1 (COBIT 4.1), Information Technology Infrastructure Library version 3 (ITIL v3) and Information Security Forum Standard of Good Practice (ISF SoGP). OCTAVE is an IT security risk management framework [14]. COBIT 4.1 and ITIL are categorised as IT governance frameworks even though COBIT 4.1 is more strategic and ITIL is more operational, both of them have IT security as sub-components [7][19].

Similarly, ISF SoGP and ISO 27001/2 are purely IT security governance framework with the objective of assisting organisations managing IT security adequately [5][38]. In principle, these selected frameworks have similar objectives with regards to IT security which is to safeguard the confidentiality, integrity and availability of information technology assets [30]. The primary differences about these frameworks lie in the approach followed in managing IT security risk [14]. Furthermore, these frameworks intrinsically possess the attributes that are proven as effective in managing IT security risk.

Table I provides a summarised view of the selected frameworks, with emphasis on the basic characteristics, key strengths and weaknesses.

Table I. THE IT SECURITY FRAMEWORKS

	Octave	ISO 27001/2	COBIT	ITIL	ISF
Focus	IT & info security risk	Info security for both IT and business	IT governance	IT service management	Info security & info risk
Applicability Level	Strategic	Tactical	Strategic	Tactical	Tactical
Basic Features	➢ Risk based ➢ Balances operational risk, security practices & technology ➢ Seeks accountability for assets, threats, vulnerability & impact	➢ Provides guidance on how to implement security controls ➢ Used as a model to build an ISMS ➢ Holistic risk-based view while enabling benefits from business opportunities	➢ Best practice processes for IT domains ➢ Consists of four core domains related to planning, building, running & monitoring of the IT environment ➢ Focus on people, process & technology	➢ IT services recognised as crucial & strategic assets ➢ Focus is on information collection, analysis & distribution ➢ Four lifecycle stages: service strategy, design, transition, operations and continual service improvement existing throughout the lifecycle	➢ Detailed or a high level security assessment ➢ Focus on security governance, requirements, controls, monitoring & improvement ➢ Enables compliance with other recognised frameworks (e.g. ISO 27001 & COBIT)
Key Strengths	➢ Systematic and context driven ➢ Involves junior staff up to executive management ➢ Self-directed workshop-based approach	➢ Provides an assurance or benchmark tool ➢ Can increase business & IT alignment ➢ Provides metrics to measure which security controls provide the largest return on security investment ➢ Uses tried & tested best practice guidance ➢ Ample guidance in how things should be done	➢ Can increase business & IT alignment ➢ Organises IT activities into generally accepted process model ➢ Highlight major IT resources to be leverage ➢ Provides control objectives to be considered	➢ Can increase IT user satisfaction ➢ IT services are explicitly defined & service levels are measured ➢ Improved decision making ➢ Can offer financial savings from reduced rework, lost time, improved resource management & usage ➢ improved time to market new IT products and services ➢ Can improve IT service availability because IT service levels are closely monitored	➢ Provides a detailed set of controls which covers the IT environment holistically ➢ Minimises the need to purchase additional repository of potential controls ➢ Seamless integration into an organisation because it is completely aligned with other globally recognised security frameworks

The idea behind presenting table I is to demonstrate some of the identified strengths derived from the selected frameworks which will be incorporated into the ITSRB approach. The four categories of frameworks which IT security frameworks may fall into are: strategic, technical, compliance and high-level guidelines [4].

For example, COBIT focuses on 'what' must be done rather than 'how' it must be done and is strong in providing high-level integration required in the cohesion of various IT security programmes [4]. Likewise, ITIL is more technical and detailed in nature and focuses on 'how' things should be done rather than the 'what' should be in place [4].

It can be seen in Table I that Octave and COBIT frameworks are applied at a strategic level while ISO27001/2, ITIL and ISF are applied at a tactical level. In finding a good approach, a combination of "what" and "how" as well as a combination of applicability levels (i.e. strategic, tactical and operational) should be aimed for. These principles form the selected frameworks, are also used to guide the ITSRB approach's principles.

III. ATTRIBUTES OF A GOOD IT SECURITY RISK MANAGEMENT APPROACH

The five attributes which are believed to make up a comprehensive and more effective IT security risk management approach are discussed in this section. These attributes have been derived through the detailed analysis of the IT security risk management frameworks discussed in section II of this paper.

A. ATTRIBUTE 1: Hybrid Approach

The first attribute essential for ensuring coverage of an organisation's IT security risk profile is a hybrid approach, depicted in figure I.

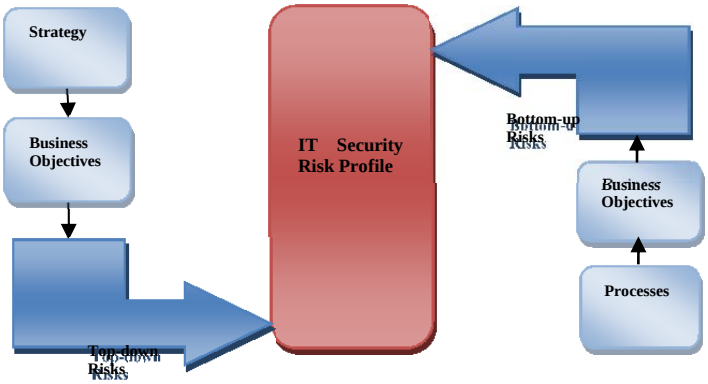

Figure I. the Hybrid Approach

Managing IT security risks requires the involvement of the entire organisation, from senior management to the most junior employee [19]. Figure I demonstrates that an approach employed to manage IT security risk should encompass risks from the strategic level down to the business objectives and processes, likewise the risks from the operational processes up to the business objectives and strategy [15]. Senior management is responsible for providing the strategic vision, goals and objectives of the organisation; mid-level management is responsible for planning and managing projects as well as processes; whereas the junior staff is responsible for carrying out operational activities [19].

A combination of a top-down approach and bottom-up approach in managing IT security risk provides a holistic view of the IT security risk profile, as depicted in Figure I.

The comparative analysis presented in section II also indicates that applying an IT security risk management framework only at a strategic level of an organisation, may leave out other significant IT security risks found at tactical and operational levels of an organisation [15].

The concept of a tiered risk management approach is recommended to ensure comprehensive coverage of IT security risks [19]. The tiered risk management approach is depicted in Figure II.

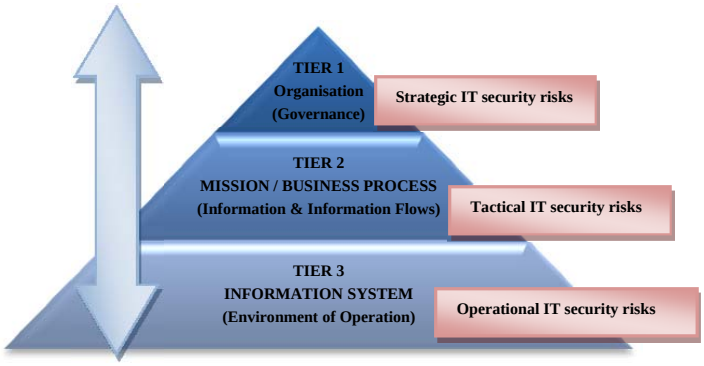

Figure II. Tiered risk management approach [19]

Figure II demonstrates that, the risks at tier one are strategic risks, then risks at tier two are tactical risks followed by risks at tier three which are operational risks. An approach employed to manage IT security risk should ensure coverage across all these tiers, as depicted in figure II. A comparative analysis on the frameworks discussed in section II also indicates that OCTAVE, ISO 27001, COBIT, ITIL and ISF all recommend involvement from senior management to the most junior employee of the organisation for risk management activities in order to ensure coverage of a holistic IT security risk profile.

Therefore, in order to ensure that the entire IT security risk landscape is incorporated during risk identification, the hybrid approach (i.e. combination of a top-down and a bottom-up approach) should be applied to identify and manage IT security risk.

B. ATTRIBUTE 2: Iteration

Treatment of any kind of risk should be an iterative process [21]. This attribute is also demonstrated in majority of the frameworks reviewed (i.e. Octave, ISO 27001/2, ITIL and COBIT).

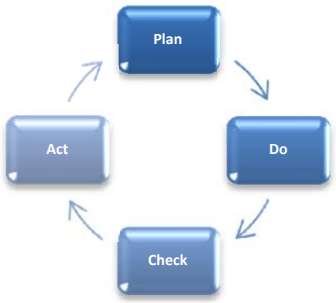

Figure III. PDCA model (PDCA, 2003)

(ISO/IEC 27001) further puts structure to the iteration by introducing the Deming cycle: Plan-Do-Check-Act model also known as the PDCA model as depicted in figure III. The PDCA model recommends that IT security initiatives must be planned, executed (i.e. do), monitored (i.e. checked) and maintained (i.e. act).

Therefore, an IT security risk management process should be an iterative process that is defined in a way which will lead

to a continuous improvement to an organisation's risk posture [3] [19] [21].

C. ATTRIBUTE 3: Responsibility Assignment

In identifying the responsibility of tasks for any process, the RACI (Responsible, Accountable, Consulted, and Informed) is an appropriate tool to be used [22]. The RACI model basically helps to simplify the responsibilities in a process by creating a two-dimensional matrix which shows the 'level of involvement' of functional roles in a set of activities, as demonstrated in table II [8] [22].

Table II. Example of a RACI model

Process Name	Role 1	Role 2	Role 3	Role 4
Process 1	R	A	C	I
Process 2	A	I	R	C
Process n	I	R	A	C

RACI is defined as follows:

R: Responsible refers to the individual(s) who owns the problem, activity or process [8] [22]. The responsible individual(s) executes that specific process [8]. Responsibility can be shared or delegated [8] [22].

A: Accountable refers to the individual who is liable [22]. The accountable individual(s) is responsible for approving the task before it can be used [8] [22]. Accountability cannot be delegated or shared [8] [22].

C: Consulted refers to the individual(s) who has the information and/or ability necessary to complete the specific process [8] [22]. These individual(s) will be consulted before a key decision is taken regarding the process or activity [8].

I: Informed refers to the individual(s) that must be notified about the results once an action has been taken [8]. Informed individual(s) are notified because the action(s) taken have some level of impact in their function [22].

The RACI model helps sort out the fundamental issues within a process where there is ambiguity in ownership of tasks [8].

Effective usage of the RACI model in a process will explicitly identify ownership, reduce duplication of effort and reduce misunderstanding [8] [22].The COBIT framework is the only framework out of the reviewed frameworks that recommends the use of a RACI model.

D. ATTRIBUTE 4: Input and Output

Both the ITIL and COBIT frameworks emphasise that a process as is a set of executable step(s) which has the primary objective of transforming input to output in order to achieve a known goal. A key and basic principle that is applicable to any process is the fact that it should have input and output [17]. It is important to note that any process is defined to achieve the one goal of transforming input to output [17].

Figure IV. A simple process model

The COBIT framework explicitly demonstrates the use of inputs and outputs in all its processes, whereas OCTAVE, ITIL, ISO27001/2 and ISF only emphasises the output components. For this reason, a good IT security risk management process should embody this principle.

E. ATTRIBUTE 5: Dynamicity

Prior to defining the security controls of an IT system, it is essential to enumerate the threats to the system in question in order to help system architects or designers to develop realistic and meaningful security requirements [27]. It is important to implement a risk approach that is vigorous so that risk can be treated in a proactive manner [26]. IT is dynamic and for this reason IT security threats also change quite often [28]. Therefore in order to achieve this principle it is important to define an approach that will periodically cater for the changing threats of the IT environment through a continuous monitoring exercise [22].

The above attributes, are the rudimentary and sourced from the various literature but are not all-inclusive enough to fully define an IT security risk management approach proposed by this research. The next section defines the proposed IT security risk management approach that is based on the discussed attributes.

IV. THE IT SECURITY RISK BASED (ITSRB) APPROACH

To ensure that the ITSRB approach integrates all the necessary elements to enable it to be more effective when it is applied in a real-world situation, the Kipling method is applied. The Kipling method is always recommended for use because it helps to explore the problem by probing the thinking of the problem solver with the questions: what, why, how, who, when and where [12].

In the same vein, the Kipling method was applied when defining the ITSRB approach. Before getting into the actual process of defining the ITSRB approach, the answers to the six questions asked by the Kipling method are discussed.

What is the ITSRB approach? The ITSRB approach is a proactive and dynamic method that aims to ensure that IT security risk is holistically managed, more effectively. In principle, the ITSRB anticipates to reduce the risks associated with confidentiality, integrity and availability of information and IT.

Why is the ITSRB approach defined?: The motivation behind defining the ITSRB approach was to formulate a

method which would assist in managing IT security risk thereby guaranteeing that relevant risk is addressed with adequate and effective controls, at the right time.

How will the ITSRB approach achieve its goal?: The ITSRB approach uses a combination of best practice IT security risk management frameworks and the threat modeling processes to ensure that risk emanating from both known and unknown threats in the IT environment is managed.

When is the ITSRB approach going to be applied?: A pragmatic tactic will be used when applying the ITSRB approach in order for it to add value. This is because the ITSRB uses a risk based approach; therefore its application will be guided by the nature of the risk.

Where will the ITSRB approach be applied?: The ITSRB approach will be applied within the IT environment of an organisation.

Who will use the ITSRB approach?: IT security professionals within any organisation can use the ITSRB approach.

A. Structure of the ITSRB Approach

It is common practice for frameworks to follow a structured life cycle, as highlighted in the comparative analysis section of this paper. Additionally, the "iteration" attribute as defined in section three of this paper highlights the importance of using a systematic process that is continuous for IT security risk management. Furthermore, it was previously stated that one of the objectives of this study is to re-use the best characteristics of the best practice frameworks in order to avoid re-inventing the wheel. Accordingly, the ITSRB approach will not deviate from this practice and will adopt the PDCA model as well as the "Iteration" attribute. Figure V presents the four phases of the ITSRB approach based on the PDCA model.

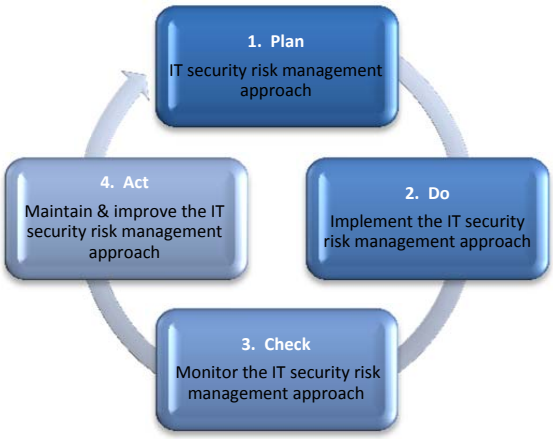

Figure V. Structure of the ITSRB approach

Plan refers to establishing the proposed IT security risk management approach. **Do** refers to the activities involved in implementing and operating the proposed IT security risk management approach. **Check** refers to the process of monitoring and reviewing the IT security risk management approach. **Act** refers to the process of maintaining and improving the IT security risk management approach which involves maintaining the IT security controls.

B. Features of the ITSRB Approach

The four phases of the ITSRB approach will each have a number of features which will be used to guide the approach. The features of the ITSRB approach will be used to ensure that the target audience that make use of this approach have an idea of exactly what will be required from them to manage IT security risk within their organisations. The features of the ITSRB approach will also align to the attributes defined in section III of this paper.

The features of the ITSRB approach are defined as follows:

- **Phase**
  As per figure V, the ITSRB approach has four phases based on the PDCA model. This implies that it goes through different phases in order to achieve its goal. A phase basically refers to one of the sub-processes or stages of the ITSRB approach.
- **Objective**
  Objective refers to the aim of each ITSRB approach's phases. The objective describes what each phase intends to do.
- **Target audience**
  Target audience refers to the person(s) which each phase of the ITSRB approach is beset at. The different target audiences will be categorised according to their work responsibilities as demonstrated in figure II of this paper.
- **Frequency**
  Frequency is the rate of occurrence that a specific phase should be conducted. The frequency that is specified in the ITSRB approach is the minimum frequency, therefore, any additional executions of phases will not cause any concerns.
- **Process Model (i.e. Input, Process, Output)**
  The process model provides the input elements, the process that will be used to transform the input elements and the output elements.
- **Tools**
  Tools refer to the existing frameworks, processes, documents or technologies that can be used in order to execute the process within a specific phase.
- **RACI**
  RACI is for responsibility assignment. RACI shows who will be responsible for what within each phase.

The ITSRB approach is presented from table III – table VI.

Table III. Phase 1 of the itsrb approach

PHASE 1	**PLAN** THE ITSRB APPROACH			
OBJECTIVE	The objective of this phase is to define and develop an IT security risk management plan that is fit for purpose for a specific organisation. The plan basically provides a view of what IT security controls are in the IT environment versus what IT security controls need to be in the IT environment (i.e. for software, hardware, procedures, networks, people and procedures).			
FREQUENCY	Annually			
TARGET AUDIENCE	➢ Strategic Management ➢ Tactical Management			
PROCESS MODEL	**INPUT**	**PROCESS**		**OUTPUT**
	➢ Organisational strategy (Objectives) ➢ IT strategy ➢ Previous IT security risk register (if it exists) ➢ Previous IT audit report (i.e. IT security audits) ➢ Previous IT security incidents	➢ Map each organisational strategy and IT strategy objective to an IT security principle (i.e. confidentiality, integrity and availability) ➢ Define IT security requirements for each strategic objective and assess which IT security controls exist and which do not exist. ➢ Use the COBIT control objectives to conduct a gap analysis to assess which controls exist within the IT environment and which ones do not exist. ➢ Define the IT security risk appetite (i.e. This information should be sourced from the senior executive who is in charge of the IT environment like a chief information officer (CIO)) ➢ The gaps identified from the strategic objectives as well as the gaps identified from the COBIT framework should be added as inherent IT security risks within the IT security risk register. ➢ Define Key Risk Indicators (KRIs) including the associated thresholds. KRI data are normally sourced from people in the tactical management tier (e.g. CIO's direct reports). ➢ Define the controls for each identified risk, assess the each controls' adequacy and effectiveness. ➢ Assess the risk once the controls have been taken into consideration, and record the residual risk as the risk that is tracked on a regular basis in the IT security risk register.		➢ IT security strategy ➢ IT security risk appetite ➢ IT security risk profile ➢ IT security risk register
TOOLS	➢ Workshops (Senior & tactical management) ➢ Spreadsheets ➢ Word documents	➢ COBIT ➢ OCTAVE ➢ RCSA (Risk & Control Self-Assessment) and KRIs		➢ Centralised document management application (e.g. Microsoft SharePoint)
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

Table IV. Phase 2 of the itsrb approach

PHASE 2	**DO:** IMPLEMENT THE ITSRB APPROACH			
OBJECTIVE	The objective of this phase is to put the ITSRB approach into effect within a specific organisation. Implementing the ITSRB approach will enable IT security professionals to prioritise implementation of the necessary IT security controls as per the organisation's risk profile.			
FREQUENCY	Quarterly			
TARGET AUDIENCE	➢ Tactical Management ➢ Operational Management			
PROCESS MODEL	**INPUT**	**PROCESS**		**OUTPUT**
	➢ IT security risk register ➢ IT components (i.e. information, hardware, software, procedures, networks, people) ➢ Previous IT security incident report	For each risk within the IT security risk register: ➢ Identify and define each IT component(s) affected by each risk ➢ Decompose each identified IT component ➢ Categorise the identified sub-components (i.e. High\Med\Low based on business criticality) ➢ Identify current threats for each IT sub-component ➢ Document the threats for each IT sub-component ➢ Select IT security controls for each IT sub-component commensurate with the threat ➢ Plan the implementation of the IT security control(s) as per the IT budget. ➢ Prioritise implementation basing the decision on the risk impact to the business and IT operations. ➢ Implement IT security control(s) for each IT sub-component as the per the implementation plan. ➢ Assess the IT security control(s) for each identified asset and update the IT security risk register on a regular basis. ➢ Monitor the IT security control(s) for each identified asset		➢ IT security risk register (updated) ➢ IT security threat landscape
TOOLS	➢ Focused workshops \ meetings with IT management (i.e. CIO's direct reports, their sub-ordinates) and other relevant operational staff. ➢ Spreadsheets ➢ Word documents	➢ ITIL and ISO 27001 ➢ OCTAVE ➢ RCSA, Management Actions, KRIs and Operational losses		➢ Centralised document management application (e.g. Microsoft SharePoint)
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

Table V. Phase 3 of the itsrb approach

PHASE 3	**CHECK:** MONITOR THE ITSRB APPROACH			
OBJECTIVE	The objective of this phase is to monitor the adequacy and the performance of the ITSRB approach. Performing this phase will assist the organisation to reflect on how the ITSRB is doing thereby highlighting the good and the bad IT security risk areas for the IT environment.			
FREQUENCY	Monthly			
TARGET AUDIENCE	➢ Tactical Management ➢ Operational Management			
PROCESS MODEL	**INPUT**	**PROCESS**	**OUTPUT**	
	➢ IT security risk register	For each risk within the IT security risk register: ➢ Assess the adequacy and effectiveness of the IT security control(s) taking into consideration the IT security incidents associated with each risk as well as the key risk indicators ➢ Record the performance of the KRIs ➢ Record any operational losses for each risk which materialised during that specific month ➢ Update the Management Actions ➢ Update the residual risk ➢ Develop an IT security risk report which provides both a summarised view and a detailed view of the IT security risk profile. Update the IT security report on a monthly basis. ➢ Record any generic areas of improvement of the ITSRB approach and also include them in the IT security monthly report	➢ IT security risk register (updated) ➢ IT security monthly report	
TOOLS	➢ Focused workshops \ meetings with IT management (i.e. CIO's direct reports, their sub-ordinates) and other relevant operational staff. ➢ Spreadsheets ➢ Word documents	➢ RCSA, Management Actions, KRIs and Operational losses.	➢ Centralised document management application (e.g. Microsoft SharePoint)	
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

Table VI. Phase 4 of the itsrb approach

PHASE 4	**ACT:** MAINTAIN AND IMPROVE THE ITSRB APPROACH			
OBJECTIVE	The objective of this phase is to assess the performance of the ITSRB approach by identifying areas of improvement and then implementing the corrective actions.			
FREQUENCY	Bi-annually			
TARGET AUDIENCE	➢ Strategic Management ➢ Tactical Management			
PROCESS MODEL	**INPUT**	**PROCESS**	**OUTPUT**	
	➢ IT security monthly report ➢ IT security strategy ➢ IT security risk appetite ➢ IT security risk profile ➢	➢ Assess the trend of the IT security risks for six months and update the IT security risk profile ➢ Review the IT security risk appetite and update it (i.e. Take guidance from the CIO & direct reports) ➢ Review if the goals within the IT security strategy are being met. ➢ Create a progressive report providing a view of the progress on the activities involved with regards to delivering against the IT security strategy. Define a generic plan of the activities which still need to be performed and record them in the organisation's action plan for IT security. ➢ Present the report to strategic and tactical management	➢ IT security progress report (bi-annual) ➢ Action plan for IT security	
TOOLS	➢ Centralised document management application (i.e. spreadsheets, word documents, etc.)	➢ Spreadsheets ➢ Word documents ➢ Power-point presentations ➢ Etc.	➢ Meetings with strategic and tactical management	
RACI	**IT Security Professional**	**CIO & Direct Reports**	**Risk Management**	**Internal Audit**
	Responsible	Accountable	Consulted	Informed

V. CONCLUSION

This paper presented the process that was taken to define the ITSRB approach. A comparative analysis of five best practice frameworks was presented and discussed in section two of this paper. The objective of presenting the frameworks was to highlight the key strengths that were used in defining the ITSRB approach. Section three presented the important attributes derived from best practice IT security frameworks discussed in section two of this paper. The objective of section three was to provide the good attributes as found in various literatures which would be used as basic principles of the ITSRB approach. The last section presented the proposed ITSRB approach, including its structure and features. The section provides the detail of how the ITSRB approach can be used for IT security risk management within an organisation.

A. *Deficiencies addressed by the ITSRB Approach*

It is demonstrated in table I that the selected frameworks have different shortcomings, some of which are addressed by the ITSRB approach. At a high level, the ITSRB approach addresses the following aspects:

- **Organisational-wide view** [33]: Attribute 1 discussed in section III ensures that a comprehensive view of the IT security risk profile is captured within an organisation from the operational level up to the strategic level.
- **Slow response and Reactiveness** [36]**:** Attribute 2 and attribute 5 discussed in section III emphasises the importance of threat modeling which ensures that new threats are iteratively considered to ensure that a risk based approach is followed. This enables organisations to be more proactive.
- **Accountability** [19]: Attribute 3 discussed in section III emphasises the need for explicitly documenting responsibilities when processes are executed.
- **Knowledge Management** [34]: The ITSRB approach emphasises the importance of capturing tacit knowledge in the risk management process to ensure that continuity in the process. This is demonstrated in all the phases of the ITSRB approach.

REFERENCES

[1] K.J. Soo Hoo, "How Much Is Enough? A Risk-Management Approach to Computer Security", 2000.

[2] J. Krichene, "Managing Security Projects in Telecommunication Networks", Engineering School of Communications, SUP'COM, November 2008.

[3] M. Ketel, " IT security Risk Management", ACM-SE'08, March 2008.

[4] J. Furner, and K. Cheney, "HP Project and Portfolio Management Center Briefing", Hewlett-Packard Development Company, USA , 2008.

[5] ISO 27001, International Standard for Information Security, ISO/IEC 17799:2005, "Information technology — Security techniques — Code of practice for information security management", January 2007.

[6] S. Foley, "Security Risk Management using Internal Controls", Department of Computer Science, University College Cork Ireland, *WISG'0, November* 2009.

[7] IT Governance Institute 2008a, "Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit", IT Governance Institute, USA, 2008.

[8] S. Banacorsi, "What is a RACI "[Homepage of 6sixsigma.com], [Online]. Available: http://6sixsigma.com/index.php/Six-Sigma-Articles/RACI-Diagram.html [2011, 10/22], 2011.

[9] IT Governance Institute 2008b, "Cobit Mapping: Mapping of IT v3 With Cobit 4.1", IT Governance Institute, USA, 2008.

[10] IT Governance Institute 2007a, "Cobit 4.1", IT Governance Institute, USA, 2007.

[11] King III code, 2009.

[12] R. Kipling, "Just so stories", Double Day Page Edn.First Edition. 1902.

[13] P. Panda, "the OCTAVE Approach to Information Security Risk Assessment", ISACA Journal, Volume-4, 2009.

[14] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE® Approach, Networked Systems Survivability Program", Carnegie Mellon, Software Engineering Institute, Pittsburgh, PA 15213-3890, August 2003.

[15] M.S. Saleh, and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management", Applied Computing and Informatics, vol. 9, pp. 107-118, 2011.

[16] A. Taylor, D. Alexander, A. Finch, and D. Sutton, "Information Security Management Principles - An ISEB Certificate", The British Computer Society, pp. 1 – 37, ISBN 978-1-902505-90-9, 2008.

[17] A. Calder, "Information Security and ISO 27001: An Introduction, IT Governance Green Paper", Infosec-and-ISO27001v3-uk, February 2013.

[18] The IT Governance Institute, ITGI, "Framework-Control Objectives-Management Guidelines – Maturity Models", ISBN 1-933284-72-2, 2007.

[19] P. Nastase, F. Nastase, and C. Ionescu, "Challenges generated by the implementation of the IT Standards ITGI, ITIL V3 and ISO/IEC 27002 in enterprises", The Bucharest Academy of Economic Studies, July 2009.

[20] P. Hill, and K. Turbitt, "Combine ITIL and COBIT to Meet Business Challenges", BMC Software, May 2006.

[21] National Institute of Standards and Technology (NIST), "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach", Gaithersburg, MD 20899-8930, February 2010.

[22] R. Langner, "The RIPE Framework: A Process-Driven Approach towards Effective and Sustainable Industrial Control System Security", Langner Communications Whitepaper, Langner Communications GmbH, 2013.

[23] IRM, "A structured approach to enterprise risk management". The Public Risk Management Association. London: 1-18. Available: http://www.theirm.org/documents/SARM_FINAL.pdf, 2010.

[24] M. Smith, and J. Erwin, "Role & Responsibility Charting (RACI)", Project Management Forum p. 5, 2005.

[25] www.businessdictionary.com/definition/process.html 2014

[26] V. Gandotra, A. Singhal, and P. Bedi, "Threat-Oriented Security Framework: A Proactive Approach in Threat Management", University of Delhi, India, Elsevier Ltd, 2012.

[27] S. Myagmar, A.J. Lee, and W. Yurcik, "Threat Modeling as a Basis for Security Requirements". National Center for Supercomputing Applications (NCSA). University of Illinois at Urbana-Champaign, 2005.

[28] M. Jouini, L. Rabai, and A. Aissa, "Classification of security threats in information systems". 5th International Conference on Ambient Systems,2014.

[29] R. Winter, and J. Schelp, "Enterprise Architecture Governance: The Need for a Business-to-IT Approach", University of St.Gallen. Institute of Information Management, ACM: p548 – p552, 2008.

[30] F. Ajibuwa, "Data and Information Security in Morden day Businesses", Atlantic International University, 2008.

[31] J. Amsenga, "An Introduction to Standards Related to Information Security". Proceedings of the ISSA 2008 Innovative Minds Conference, 2008.

[32] R. Maphakela, "A Model for Legal Compliance in the South African Banking Sector - An Information Security Perspective", Nelson Mandela Metropolitan University, 2008.

[33] J. Webb, A. Ahmad, S. Maynard, G. Shanks, "A situation awareness model for information security risk management", ScienceDirect, Computers & SecurityElsevier Ltd, 2014.

[34] P. Shedden, R. Scheepers, W. Smith, A. Ahmad, "VINE: Incorporating a knowledge perspective into security risk assessments", Vol. 41 Iss 2 pp. 152 – 166, 2011.

[35] https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-manage

[36] D. Utin, M. Utin, J. Utin, "General Misconceptions about Information Security Lead to an Insecure World." , Information Security Journal: A Global Perspective 17, no. 4: 164-169, 2008.

[37] P. Panda, "the OCTAVE Approach to Information Security Risk Assessment", ISACA Journal, Volume-4, 2009.

[38] M. Chaplin, J. Creasy, "Information Security Forum (ISF) Limited. The ISF Standard of Good Practice", 2011.