CRITICAL SUCCESS FACTORS FOR THE IMPLEMENTATION OF AN OPERATIONAL RISK MANAGEMENT SYSTEM

M.D.Gibson*, J. Young*

Abstract

Operational risk has become an increasingly important topic within financial institutions resulting in an increased spend on operational risk management solutions. While this is a positive approach, evidence has shown that information technology implementations have tended to have low rates of success. Research has highlighted that a series of defined critical success factors could reduce the risk of implementation failure. Twenty-nine critical success factors were identified by means of a literature review and confirmed by a questionnaire that was distributed to an identified target group within the South African financial services community. Reponses to the questionnaire revealed that 27 of the 29 critical success factors were deemed important and critical to the implementation of an operational risk management system.

Keywords: Critical Success Factors, Operational Risk, Risk Management Systems, Strategy, Governance, Information Technology

*PO Box 392, Unisa, Pretoria, 0003
Tel.: +971 (0) 50 1098 082
**PO Box 52 185, Wierda Park, Centurion, Pretoria, South Africa, 0149
Tel.: +27 12 429 3010; +27 83 307 6265
Fax: +27 86 695 3324
Email: youngj@unisa.ac.za

Introduction

Operational risk has become an increasingly important topic within financial institutions of late. A series of high-profile cases as well as increased regulation around the measurement and management of operational risk have prompted an increase in the level of sophistication with which operational risk is managed. To support the management of operational risk, software vendors have developed sophisticated applications to manage the full operational risk management life cycle. This has resulted in an increased spend by financial service organisations on operational risk management solutions. While this move is positive, evidence has shown that Information Technology (IT) implementations generally have high failure rates, jeopardising the success of the investment in any operational risk management solution. It is estimated that about one-third of all IT projects either fail or are abandoned, and around 40 per cent of application development projects are cancelled before completion (Randeree & Ninan 2009).

The Standish Group (2009) identified that 32 per cent of IT projects were considered successful, having been completed on time, on budget and with the required features and functions. A further 24 per cent were considered failures, having been cancelled before they were completed, or having been delivered but never used. The remaining (44 per cent) were considered challenged meaning that they were either over time or over budget, or completed with fewer than required features and functions. The Standish Group (2009:3) defines a successful project as the ability to complete and operationalise the project, on-time, on-budget, meeting features and functions as specified.

One of the probable reasons for these high failure rates is the large number of areas of expertise that must be managed during and throughout the project implementation. Project managers not only need to grasp technical issues, for example, system development and process re-engineering, but also master the human and organisational aspects, such as change management and end-user involvement. Practitioners and researchers have begun to identify these areas and commonly refer to them as critical success factors (CSFs).

Rockart (1979:83) describes a critical success factor as the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organisation, in other words the few key areas where things must go right to ensure a positive outcome for the business.Rockart (1979:86) also argues that the process of identifying CSFs helps to

ensure that these factors receive the necessary attention.

Cooke-Davies (2002:186) describes success factors as those inputs to the management system that lead directly or indirectly to the success of the project or business. The focus of this paper is based on a system implementation-type project, to identify the CSFs that can lead to the successful implementation of that system, more specifically, an operational risk management system.

Literature review

Research into the literature revealed that, while several types of IT implementations had defined CSFs, it seems that none had been done for the implementation of an operational risk management system (ORMS). To address this shortcoming it was argued that a series of CSFs were required to ensure a successful implementation of an operational risk management system. In order to ensure insight into the complexities involved in an ORMS implementation, it is important to first gain an initial understanding of enterprise risk management (ERM) and operational risk management.

For all types of organisations, there is a need to understand the risks being taken when seeking to achieve objectives and attain the desired level of reward. The Institute of Risk Management (IRM) (2010), states that an organisation needs to understand the overall level of risk embedded within their processes and activities. As such, it is important for organisations to recognise and prioritise significant risks and to identify the weakest critical controls. A successful ERM initiative can affect the likelihood and consequences of risks materialising, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004:2) states that ERMis a process:

- effected by an entity's board of directors, management and other personnel;
- applied in a strategy setting and across the enterprise;
- designed to identify potential events that may affect the entity; and
- to manage risk to be within its risk appetite to provide reasonable assurance regarding the achievement of entity objectives.

Ding (2009a:8) defines ERM as a risk management philosophy and approach which adopts a top-down, organisation-wide approach to managing the entire universe of risks. In addition, Ding (2009a) also states that ERM not only covers point risks, such as, operational risk, credit risk, market risk, legal and compliance risk, but also considers the broader risks like strategic, reputational, political, environmental and key people risks.

Risk management is a process that is underpinned by a set of principles. It also requires the support by a structure that is appropriate for the organisation and its external environment or context. A successful risk management initiative should be proportionate to the level of risk in the organisation (as related to the size, nature and complexity of the organisation), aligned with other corporate activities, comprehensive in its scope, embedded in routine activities and dynamic by being responsive to changing circumstances (IRM 2010).

Considering the many risks faced by a business, operational risk can be viewed as a central point at which other risks interface with the business and, if mismanaged, can lead to significant losses. The Basel Committee for Banking Supervision (BCBS) defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Explicitly excluded from this definition are systemic risks, strategic and reputational risks, as well as all indirect losses or opportunity costs. The BCBS (2004) states that operational risk is inherent in every business and support activities, in other words, operational risk can occur anywhere and anytime in any business environment.

In June 2006, the BCBS released the International Convergence of Capital Measurement and Capital Standards, which contained the definitive proposals on capital charges for operational risk under Basel II (BCBS 2004). The Basel Committee however refrained from dictating explicit methodologies for calculating operational risk capital charges towards a more qualitative approach to the management of operational risk. In their final proposals, the Basel Committee stressed the importance of qualitative standards for banks that prefer to use the advanced measurement approach (AMA) for management of their operational risks. The Basel Committee, however, states that an ORM system must be “conceptually sound and implemented with integrity” (BCBS 2004:3), but gives little guidance as to what such a system might actually look like.

Over the last few years, in order to support financial institutions in meeting their Basel II regulatory requirements, along with the automation of the operational risk management process, operational risk management systems have become increasingly sophisticated and important tools (Ding 2009b).

An operational risk management system (ORMS) is a broad term used to describe software designed for the management and monitoring of operational risk within an organisation. Gartner

(2009) defines an operational risk management system as a combination of two primary technologies, namely operational risk engines (OREs) and qualitative risk self-assessments (QRSAs).

According to Gartner (2009), an ORE involves the following:

- it incorporates a tool for the measurement of potential losses that are due to inadequate operations;
- it supports event reporting;
- it calculates economic and regulatory risk capital for operational risk;
- it runs scenarios of potential risk exposures to quantify operational risk;
- it fits statistical distributions to internal and external loss data;
- it links cause and effect to determine key risk indicators;
- it conducts fault tree analysis; and
- it creates qualitative rankings and balanced scorecards for operational risk.

Gartner (2009:64), furthermore defines a QRSA, as a software application that provides the ability to identify operational risk exposures, and then links controls, risk weightings, audit findings and losses to those exposures. QRSA tools focus on qualitative, process-based management of operational risk and typically support risk policy definition and controls, including an organisational framework; business process identification; as well as mapping, evaluation, audit and certification functions. Information related to loss events and key risk indicators are captured, reported, and escalated through a workflow functionality to the appropriate level of management for regulatory reporting.

To start identifying a list of CSFs for an ORMS, IT, ERM and Enterprise Resource Planning (ERP) implementations as well as operational risk in general were researched to determine a baseline and categories for potential CSFs relevant to an ORMS implementation. Strauss and Corbin (1990:15) state that with respect to the naming of a category, "it is usually the one that seems most logically related to the data it represents, and it should be graphic enough to remind you quickly of its referent". Accordingly, the categories and category descriptions for CSFs are depicted in Table 1 below that were obtained from the literature.

Table 1. Categories of critical success factors

Category name	Category description
Strategy	All CSFs related to the support of the strategic direction of the system implementation project
Pre-project planning	All CSFs related to the pre-project planning phase of a system implementation project
Scope	All CSFs that relate to the scope of a system implementation project. The Project Management Institute (PMI) defines scope as "the work that must be performed to deliver a product, service, or result with the specified features and functions" (PMI 2008:444).
Project resources	All CSFs that relate to the project resources who are involved with a system implementation project
Project management	All CSFs that are related to the project management of the system implementation project. The PMI defines project management as the application of knowledge, skills, tools, and techniques to project activities to meet the project requirements
Performance monitoring	All CSFs that are related to the performance monitoring of a system implementation project. The PMI defines performance monitoring as those processes required tracking, reviewing and regulating the progress and performance of the project, identifying any areas in which changes to the plan are required, and initiate the corresponding changes(PMI 2008:444).
Decision-makers' support from senior management	All CSFs that are related to the key stakeholders and decision-makers involved with a system implementation project
Governance	All CSFs related to the governance of a system implementation project
Change management	All CSFs that are involved with the change management effort throughout the organisation undergoing a system implementation project
Communication	All CSFs related to both the internal and external communication between all stakeholders involved in the system implementation project
Data	All CSFs related to the application data required for a system implementation project
Application	All CSFs related to the application being implemented as part of the system implementation project
Architecture	All CSFs related to the solution architecture for the system being implemented
Internal audit	All CSFs related to internal audit's role within a system implementation project

At the same time twenty-nine potential CSFs relevant to the implementation of an ORMS were identified as part of the same literature review and are listed in Table 2 in no particular order.

Table 2. Critical Success Factors

Number	Critical Success Factor
1	Common understanding between business and IT of the risk strategy
2	Defined risk appetite
3	Well defined and documented Operational Risk management policies, processes & procedures
4	Clear, realistic goals and objectives (around the ORMS and what the implementation will achieve)
5	A clear implementation strategy
6	Business Unit and IT involvement in pre-project planning (Business Unit involvement in early planning phases)
7	A clearly establish project scope (clear and fixed statement of requirements along with smaller project milestones)
8	Ensure that the ORMS implementation is enterprise wide
9	Ensure adequate budget for project resources (to cover in addition to the direct project costs, costs associated to project team performance incentives, e.g. project bonuses)
10	A cross functional team consisting of the right mix of external consultants and internal staff
11	Full-time (dedicating 100% of their time to the project) team members (assuming that they are adequately skilled)
12	Have an experienced project team with the right mix of business and technical skills
13	Assign responsibility (to one or several individuals for delivery of the project)
14	Have a competent project manager (both in terms of skill and leadership ability)
15	Have effective monitoring/control throughout the implementation lifecycle (strong/detailed plan kept up to date throughout the implementation lifecycle along with ensuring that risks are addressed/assessed/managed)
16	Have specified measures of project success (predefined metrics to track and monitor the project's success against, e.g. 40% decrease in a particular process time)
17	Have a project Sponsor/Champion from top management (having the CRO, or equivalently empowered decision maker, driving change along with active top management support throughout the implementation lifecycle)
18	Have a documented and agreed project team structure (reflecting clearly defined roles & responsibilities throughout the organisation as they relate to the project team along with a defined project steering committee)
19	Have a defined and documented organisational structure (an organisational wide structure documenting interdepartmental roles/reporting lines that reflecting the ORMS projects relationship/impact on this structure)
20	Ensure effective Change Management (focusing on User/Client involvement throughout the implementation process along with adequate training)
21	Ensure targeted and effective communication (management of expectations at all levels along with communication among key stakeholders and continuous project progress communication)
22	Ensure that Operational Risk related data is available, in a single data repository
23	Have a documented Data Model (Conceptual, logical and physical data model for all data related to an ORMS)
24	Have minimal customisation to the ORMS software (aligning the business processes to the software)
25	Ensure that the ORMS interfaces with legacy systems and other applications
26	Conduct system testing prior to implementation
27	Have a vendor with past experience in a similar implementation
28	Have flexible and configurable architectural framework (architectural design of the ORMS solution)
29	Have Internal Audit control throughout implementation (the involvement of the Internal Audit department throughout the implementation lifecycle)

Each CSF can be allocated to a CSF category, reflected in Table 3.

Table 3. Allocation of CSFs to CSF categories

ID	CSF Category	CSF
1	**Strategy**	
1.1		Well-defined and documented operational risk management policies, processes and procedures
1.2		Common understanding of risk strategy between business and IT
1.3		Define risk appetite and tolerance
2	**Decision-makers' support from senior management**	
2.1		Project sponsor/champion from top management
		CRO required to drive change
		Active top management support throughout the implementation life cycle
		Empowered decision-makers
3	**Governance**	
3.1		Documented and agreed project team structure
		Creation of a project steering committee
		Clearly defined roles and responsibilities throughout the organisation (operational risk-related)
3.2		Defined and documented organisational structure
4	**Data**	
4.1		Data availability, migration, consolidation and cleaning
4.2		Data model
5	**Communication**	
5.1		Targeted and effective communication
		Management of expectations at all levels
		Communication among key stakeholders
		Project progress communication
		Organisational adaptation/culture/structure
6	**Change management**	
6.1		Effective change management
		User/client involvement
		Training provision (budget, resources)
		End-user training
7	**Project resources**	
7.1		Experienced and adequately skilled project team
		Team should have both business and technical knowledge
7.2		Adequate budget
		Adequate compensation and incentives
		Linking output to management compensation
7.3		Full-time team members
7.4		Cross-functional team consisting of a mix of consultants and internal staff
8	**Scope**	
8.1		Clearly established project scope
		Clear and fixed statement of requirements
		Smaller project milestones
8.2		Enterprise-wide implementation
9	**Project management**	
9.1		Responsibility assigned
9.2		Competent project manager
10	**Application**	
10.1		System testing prior to implementation
10.2		Vendor support and past experience
10.3		Interfaces with legacy systems and other applications
11	**Architecture**	
11.1		Flexible and configurable architectural framework
12	**Pre-project planning**	
12.1		Clear realistic goals and objectives
12.2		Business unit and IT involvement in pre-project planning
		Business unit involvement in early planning
12.3		Clear implementation strategy
13	**Performance monitoring**	
13.1		Effective monitoring/control throughout the implementation life cycle
		Strong/detailed plan kept up to date throughout the implementation life cycle
		Risks addressed/assessed/managed
		Maintaining initial project scope
13.2		Specified measures of success
14	Internal audit	
14.1		Internal audit control throughout implementation

In order to determine the critical importance of the identified CSFs for the implementation of an ORMS, the following research methodology was used.

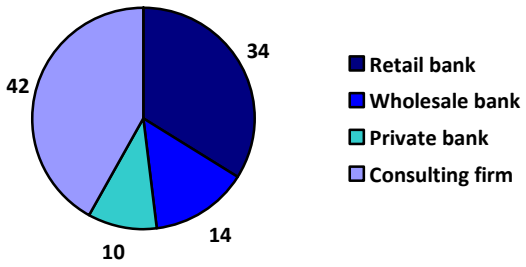
Research Methodology

Research was carried out, via a questionnaire, to validate the list of 29 CSFs by confirming how critical and important each CSF was in relation to an ORMS implementation project. The questionnaire was distributed to an identified target group within the South African financial services community. The target population for the South African financial services industry comprised of the six main largest South African banks. The reason for deciding on this target audience was based on the South African Reserve Bank's statistical information of 2011. According to this information, these banks together constitute approximately 90 per cent of the South African banking market (by assets) and are considered to be the most sophisticated financial services organisations in the industry in terms of information technology maturity.

In addition to the identified financial services institutions, IT consulting firms were also considered in the target population, as they are often contracted by the financial services institutions to play a role in the implementation process. Thus, it was assumed that these firms would have a considerable amount of experience and expertise in implementing an ORMS.

A total of 52 questionnaires were completed, which represents a 68% response rate. Responses across all business-type categories were received, however, analysis of the results (Figure 1 below) indicated that the majority of respondents were from IT consulting firms and retail banks, which represented 42 per cent and 34 per cent respectively.

Figure 1. Respondents business type summary



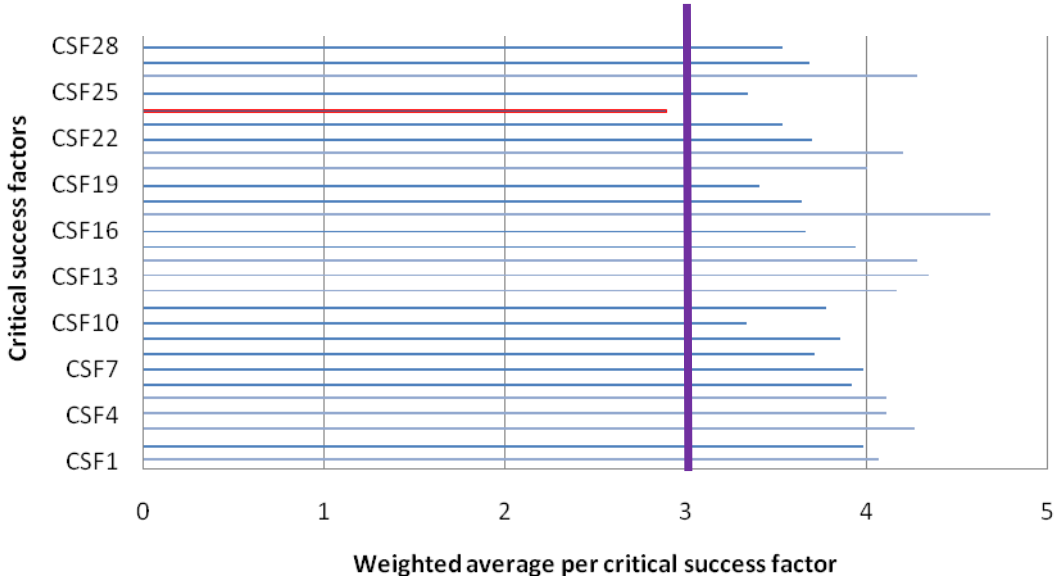
To determine the significance of the 29 identified critical success factors, the respondents were asked to rate, via a Likert scale (Table 4 below), each CSF from "neither critical nor important" to "extremely critical and important".

Table 4: Likert scale rating and description

Value	Likert scale description
1	Neither critical nor important
2	Important not critical
3	Somewhat critical and important
4	Critical and important
5	Extremely critical and important

Reponses to the questionnaire (Figure 2 below) revealed that 27 out of the 29 critical success factors were deemed important and critical to the implementation of an operational risk management system.

Figure 2. Significance of critical success factors

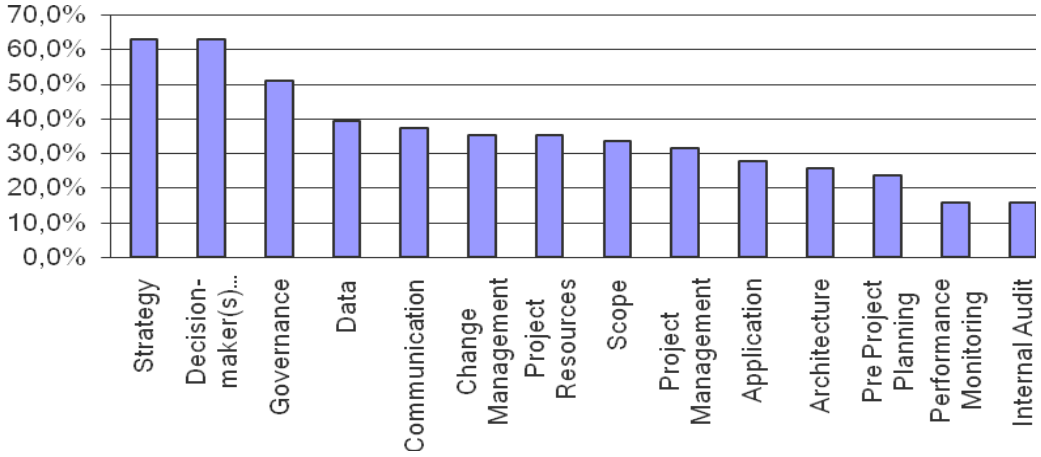


For a CSF to be considered, the average response had to be at least "somewhat critical and important". CSF 24, *minimal customisation to the ORMS software*, in Figure 2 above, was not considered as critical with only 19% of respondents indicating that this was critical and important. The majority of respondents (45%) were of the opinion that this was somewhat critical and important, with 26% being of the opinion that this was important but not critical. Only 6% of respondents thought that this was neither critical nor important. With the majority of respondents considering this CSF as less than somewhat critical and important, CSF 24 was not considered as a CSF in the implementation of an ORMS.

CSF 29, *the importance of having internal audit control throughout the implementation*, in Figure 2 above, was found to be important but not critical by 30% of the respondents with another 30% considering this as somewhat important and critical. Only 29% considered this as being critical and important as well as extremely critical and important. As the majority of respondents considered this CSF as less than somewhat critical and important, it was not considered as a CSF for the implementation of an ORMS.

The questionnaire also determined the priority of the 14 identified CSF categories (originally defined in Table 1 above). Figure 3below presents the cumulative results of the prioritised CSF categories as per the respondents' feedback. The majority (62.7%) of the respondents confirmed that the most important factor categories of an ORMS were *strategy and decision-makers' support from senior management*. This indicated that the respondents recognised the strong need to have a definite and well-defined strategy around implementing an ORMS as well as support from senior management in order to execute a successful implementation of an operational risk management system.

Figure 3. Prioritised critical success factor categories



Based on the response, the 27 identified CSFs along with the prioritised CSF categories were combined to produce a list of prioritised CSFs with associated categories (Table 3above).

The cumulative results from the questionnaire enabled the CSFs and their respective categories to be ranked in order of importance and criticality. There are several conclusions that can be drawn from the results of the questionnaire. These conclusions are grouped below in order of priority according to the 14 identified CSF categories discussed in the section above.

As a general observation, the highest prioritised CSF categories and CSFs tended to be those that influenced or impacted the implementing firm at an organisational level, while the lower prioritised categories and CSFs were found to impact and influence theORMS project environment. As an example, *strategy*, *decision-makers' support from senior management* as well as *governance*, tend to influence and be managed at an organisational level and were thus found to be the top three prioritised CSF categories. *Architecture*, *pre-project planning*, *performance monitoring and internal audit* are all project-specific, and were found to be the lowest prioritised CSF categories. The results seemed to indicate that for an implementation to have the highest probability of success, CSFs that affect the organisational level must first be examined and in place before concentrating on more operational and project-level CSFs.

Other key observations resultant from the literature review and in order of priority according to the empirical analysis, are discussed below:

Strategy

- Having *well-defined and documented operational risk management policies, processes and procedures* was identified as the most important critical success factor to enable a successful ORMS implementation. This is possibly because the existence of these documents is usually considered as a starting point for the implementation process. Documented policies, processes and procedures enable the team involved to clarify with management how the new system will complement the existing way of handling operational risk, and where it will deviate. By identifying specifications and variances upfront, the project team is able to adequately scope and plan for the implementation and ultimately increase the probability of success.
- A *common understanding of the risk strategy between the business and the IT department* will ensure that the solution that is developed will meet the business' needs. It is also important that a mutual understanding of the risk strategy be maintained throughout the implementation in order to ensure alignment of the ORMS to the overall risk strategy.
- A *defined risk appetite and tolerance* will allow for the ORMS to be correctly calibrated. The risk appetite and tolerance will define the operational risk that the bank is prepared to tolerate and will thus have a direct impact on how the system that manages and monitors the operational risk is implemented and calibrated.

Decision-makers' support from senior management

- Having *a project sponsor/champion from top management* is vital to provide the right level of support behind the project. Typically, sponsorship of an ORMS implementation from a business perspective will fall under the risk and/or finance department. As such, the CRO/CFO should provide full support to drive the required change. Active support from top management throughout the implementation life cycle will ensure that decisions are made in a timely manner and that the implementation team receive the required support. All decision-makers involved in the project should be adequately empowered in order to affect the

change and decisions at the level where it is required.

Governance

- A *documented and agreed project team structure along with clearly defined roles and responsibilities throughout the organisation for all stakeholders involved with the ORMS implementation* is crucial to ensure that all parties involved are aware of their role within the implementation. Establishing a project steering committee prior to the commencement of the project allows for a single project governance body to be established with the role of guiding, reviewing and approving all critical milestones and issues that arise during the project. The project steering committee should consist of senior managers and executives who have a direct interest in the ORMS implementation.
- A *defined and documented organisational structure* allows the project team to assess possible areas within the organisation that will be impacted by the implementation. Once an understanding has been established, the project team can adequately prepare and manage the stakeholders within these areas. It was noted in the analysis of the results that banks that have implemented an ORMS found it more critical and important to define and document the organisational structure for the ORMS implementation than compared to banks that did not have an ORMS or who did not plan to implement an ORMS. This finding is in line with the view of having a defined and documented organisational structure prior to implementation.

Data

- The *data required* to set up and run the ORMS should be available prior to starting the implementation. Once the data has been identified, the data needs to be consolidated, verified and migrated into the new ORMS.
- A *data model*, which defines the relationships between disparate data entities within the operational risk environment, should be developed prior to implementation. Having a defined data model will allow for easy integration between the data source systems and the new ORMS. When examining the respondent types, it was noted that a documented data model was considered more critical and important by organisations that were planning on implementing an ORMS than those that did not have an ORMS or were not planning to implement an ORMS. This finding is in line with the view of having a defined data model prior to implementation.

Communication

- Project communication must be addressed by *targeting the correct stakeholders by delivering the correct message* at the right time and in the right format. Throughout the project, the expectations of key stakeholders involved in the implementation must be managed through effective communication. This typically takes the form of frequent project progress communications to all identified stakeholders and is usually adapted to the style, structure and culture of the organisation.

Change management

- Any new system implementation brings a fair degree of change to an organisation. *Effective change management* is important to ensure that all affected parties understand the impact of the change and the way it affects their work. By establishing adequate training prior to the implementation, the organisation can begin to manage the change that a new ORMS will bring by adequately training and familiarising the end-users with the new features and functions of the ORMS.

Project resources

- The *implementation team should consist of experienced and adequately skilled team members who have a balance of both business and technical knowledge*. This is important when gathering business requirements to implement an IT system that will be owned and operated by the business. Having a team with both business and technical knowledge will enable an ORMS to be implemented that meets both the needs of the business while still being technically sound.
- An *adequate project budget* should be set aside to incentivise and link the project teams' compensation to the outcome of the project. Providing a performance bonus tied to the successful outcome of the project will drive the delivery team to provide their best efforts during the implementation.
- Ideally, the *project team should consist of full-time team members with a cross-functional mix of consultants as well as internal staff*. The implementation of an ORMS will require a dedicated and focused team who should be full time involved in the project. The project team should also consist of a mix of cross-functional consultants (with a wide range of skills) as well as internal departmental team members to provide the organisational perspective needed to successfully implement the ORMS.

Scope

- The *scope of the ORMS implementation should be clearly established prior to the project commencing*. The scope should include a fixed statement of requirements and should be organised within a project plan with frequent project milestones.
- The scope of the implementation should be *enterprise-wide*. With operational risk affecting

the entire organisation and not just a department or subsidiary, an implementation should be targeted across the enterprise. This would also create efficiencies and synergies across the organisation by means of common and standardised ways of handling and managing operational risk.

Project management

- *Responsibility for managing the project should be assigned* and made clear to all involved stakeholders before commencing with the project. Typically, a project manager will be assigned responsibility for the delivery of a project. The project manager is one of the most critical team members throughout the implementation and thus a competent project manager should be selected. The project manager's primary responsibility is to ensure that the project is delivered on time, on budget and against the defined scope. Once the project manager has been assigned, this should be communicated to all stakeholders in order to promote accountability for the delivery of the implementation.

Application

- The application should be *tested prior to implementation*. Application testing should focus on the stability and usability of the ORMS application as well as attempt to uncover any performance issues. Having a properly tested system prior to implementation will support the adoption of the system by end-users and will play a key role in determining the success of the overall implementation.
- The vendor implementing the ORMS should have *experience in implementing* and should provide support throughout the implementation life cycle.
- If required, the selected ORMS should be interfaced with the organisation's *legacy systems* in order to ensure that the data required to support the ORMS is available and in the required format. This requirement is typical of organisations with a fragmented application landscape in which several applications contain data needed by the ORMS.

Architecture

- A *flexible and configurable IT architectural framework* should be developed to support the ORMS implementation. With a flexible and configurable IT architecture, the complexity and cost of an ORMS implementation should be reduced by capitalising on unified architectures, scalable solutions and automated services. This should have a positive impact on the probability of having a successful ORMS implementation.

Pre-project planning

- *Clear realistic goals and objectives* should be set prior to the project commencing. By establishing the objectives of the project upfront, the expectations of all stakeholders involved can be managed throughout the project life cycle. A set of clear goals and objectives can also be used to drive out more detailed project planning as well as establish a reference point against which project progress can be assessed.
- *Business units* impacted by the implementation as well as the IT department should be involved early in the pre-project planning phase. This will ensure that all stakeholders are afforded the opportunity to understand the impact that the ORMS will have on their department as well as on their role throughout the implementation.
- A *clear implementation strategy* should be developed and laid out prior to the start of the project. The implementation strategy should provide more in-depth insight into how the ORMS will be implemented and by whom. The strategy should also focus on defining known risks and issues as well as mitigation strategies to address these before the project commences.

Performance monitoring

- *Effective monitoring and control* of the project is necessary throughout the implementation life cycle with a strong and detailed plan being kept up to date. Project risks should be identified, assessed and managed frequently as part of the monitoring and control life cycle.
- *Project success metrics* should be defined up front in order to measure, as part of the monitoring and control life cycle, whether the project is delivering the intended benefits.

Internal audit

- Due to the fact that the category of *internal audit* was found to be non-critical for a successful implementation of an ORMS, it can be considered as not applicable at this stage.

Conclusion

In most countries across the globe, the global financial crisis showcased certain inadequacy of the current financial services industry regulation as well as the inability of industries to successfully detect and prevent the risk exposures. Some of the most severe losses that were experienced during the crisis could be attributed to operational risk failures.

With the introduction of Basel II, the field of operational risk received a boost in terms of the development of tools and strategies. The emergence of operational risk management systems provided much needed support to the management and monitoring of operational risk within an organisation; however there have been challenges in realising these benefits with difficult and often failed ORMS implementations. It was thus determined that an identified list of critical success

factors relevant to an ORMS implementation was needed in order to increase the probability of successfully implementing an ORMS system.

Through a review of the literature and survey on CSFs, the study identified a set of 27 success factors that were considered as critical and important for the implementation of an ORMS. The prioritisation of the success factors along with their corresponding categories provided insight into which CSFs were the most important and should be regarded as a priority when implementing an ORMS. CSFswhich could influence the organisation were identified as the most critical and important with CSFs around strategy, support from senior decision makers and governance being of the highest importance for an ORMS implementation. This finding indicated that broader organisational topics needed to be addressed prior to the actual ORMS implementation taking place.

The remaining CSF categories and associated CSFs all pertained to the ORMS implementation project. CSFs around data, communication, change management, project resources, project scope, project management, software application, IT architecture, pre project planning and project performance monitoring were identified as being critical and important to the implementation of an ORMS.

The identification of the CSFs should provide future ORMS stakeholders with the ability to improve the probability of implementing an ORMS successfully. The identified CSFs should also allow for the efficient allocation of scarce organisational and project resources against the identified CSFs most likely to influence the success of the implementation.

The results from this research should lay a foundation upon which to build the understanding of the CSFs affecting an ORMS implementation. In addition to this research further areas for investigation could be to determine whether:

- the identified CSFs extend across industries; and
- how the size of the implementing organisation affects the identified CSFs.

The adoption of these and other identified CSFs should increase the probability of a successful implementation of an operational risk management system by serving as a guideline during the project management process.

References

1. Basel Committee on Banking Supervision (BCBS). (2001). *Sound practices for the management and supervision of operational risk*. BCBS Publications No. 86. Bank for International Settlements (December). www.bis.org/publ/bcbs86.htm [Accessed 6 May 2010].
2. Basel Committee on Banking Supervision (BCBS). (2004). *International convergence of capital measurement and capital standards: A revised framework*. BCBS Publications No. 107. Bank for International Settlements (June). www.bis.org/publ.bcbs107.htm [Accessed 6 May 2010].
3. Basel Committee on Banking Supervision (BCBS). (2006). *Basel II: International convergence of capital measurement and capital standards: A revised framework-comprehensive version*. BCBS Publications. No. 128. Bank for International Settlements (June). www.bis.org/publ/bcbs128.htm [Accessed 6 May 2010].
4. Cooke-Davies, T. (2002). *The "real" success factors on projects*. International Journal of Project Management, 20:185-190.
5. COSO (Committee of Sponsoring Organizations of the Treadway Commission). (2004). Integrated framework: *Executive summary*. *Enterprise Risk Management*. Available: http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf. [12 August 2010].
6. Ding, C. (2009a). *Enterprise operational risk management, compliance, and governance solutions*, USA: Celent Research, 3 - 45. Available: http://www.celent.com/ [Accessed 2 February 2010].
7. Ding, C. (2009b). *Risk governance and the board*, USA: Celent Research, 3 - 38. Available: http://www.celent.com/ [Accessed 2 February 2010].
8. IRM. (2010). *A structured approach to enterprise risk management*. The Public RiskManagement Association. London: 1-18. Available:http://www.theirm.org/documents/SARM_FINAL.pdf [Accessed 10 February 2010].
9. IT Cortex. (2001). *Failure rate: Statistics over IT projects failure rate*. Available: http://www.it-cortex.com/Stat_Failure_Rate.htm [Accessed 2 March 2010].
10. Project Management Institute (PMI) (2008). *A guide to the project management body of knowledge (PMBOK)*, fourth edition. Project Management Institute, Inc, 2008, Pennsylvania, USA.
11. Randeree, K. & Ninan, M. (2009). *Leadership and teams in business: A study of IT projects in the United Arab Emirates*. International Journal of Managing Projects in Business, 4(1):28-48.
12. Rockart, J.F. (1979). *Chief executives define their own data needs*. Harvard Business Review, March/April: 81-93.Available: http://hbr.org/1979/03/chief-executives-define-their-own-data-needs/ar/1 [Accessed 9 June 2010].
13. Strauss, A. & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park, CA: SAGE, 2008. 63-66. SAGE Research Methods Online, doi: 10.1177/1049732305285972 [Accessed 17 June 2011].
14. The Standish Group. (2009). *Chaos Report*, USA, 2 – 13 Available: USA. http://www.marketresearch.com/Standish-Group-International-v2514/ [Accessed 3 Mar 2010].