

## **CHAPTER 5: CONCEPTUAL ENTERPRISE RISK MANAGEMENT IMPLEMENTATION MODEL AND PROPOSED ENTERPRISE RISK MANAGEMENT IMPLEMENTATION ASSESSMENT TOOL**

### **5.1 INTRODUCTION**

At this stage of the study, the requirements of theoretical objectives 1 (Describe the ERM domain in terms of the scope and definition of ERM, ERM adoption drivers, and the perceived value proposition of ERM implementation) and theoretical objective 2 (Identify and document the barriers to ERM implementation) were addressed by the systematic literature review and the results were described in Chapter 2.

Theoretical objective 3 stipulates the exploration of the use of organisational design models and the principles of continual improvement as the theoretical frameworks for the conceptual ERM implementation model. The aforementioned was discussed in detail in Chapter 3 and the necessary recommendations were also contained within the discussion.

The problem statement essentially refers to the fact that there are several barriers to ERM implementation. This was confirmed with the phase 1 questionnaire (part of phase 1 of the empirical portion of the study) that was sent to primary and secondary risk stakeholders in South African organisations. The aforementioned questionnaire also confirmed certain elements of the ERM domain in a South African context which satisfied the requirements for empirical objective 1 (refer to Section 1.4.3). The results were discussed in Chapter 4 (refer to Section 4.5).

Chapter 5 commences with the detailed description of the conceptual ERM implementation model (required by theoretical objective 4 – refer to Section 1.4.2) by identifying:

- The building blocks of the conceptual ERM implementation model with the focus on continual improvement;
- Addressing the key requirements of the ERM implementation model based on the recommendations of ISO 31000: Risk management principles and guidelines (ISO, 2009b), ISO 31010: Risk management – Risk assessment techniques (ISO, 2009c), Guide 73: Risk management vocabulary (ISO, 2009a), and the King III Code on Governance (IODSA, 2009); and
- Clarifying the derived deliverables and the purpose of the deliverables.

After proposing the conceptual ERM implementation model, the chapter proceeds with a proposed ERM implementation assessment tool (theoretical objective 5 – refer to Section 1.4.2) to determine the level of implementation and the degree of formality of ERM implementation within any South African organisation, operating within any industry.

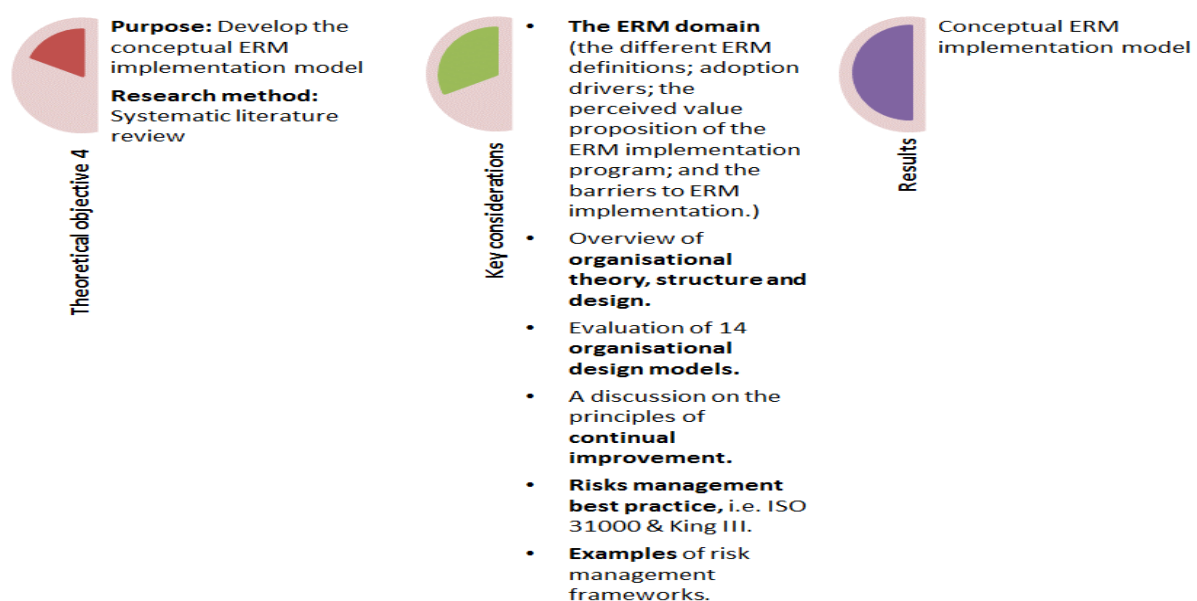
## 5.2 THE CONCEPTUAL ENTERPRISE RISK MANAGEMENT IMPLEMENTATION MODEL

It is imperative to reiterate that the main objectives of the conceptual ERM implementation model are to:

- Provide risk stakeholders with a standardised ERM implementation model that they can use to facilitate the implementation of the ERM program;
- Reduce the barriers to ERM program implementation;
- Improve the allocation of scarce risk resources;
- Establish a common risk language within the organisation; and
- Contribute to the academic literature regarding the misalignment between ERM program design and organisational design principles (refer to Section 3.2, 3.3 and 3.4); a practical approach to ERM implementation by utilising a model and an assessment tool (refer to Section 5.2) and to stay true to a practice-based ERM model development and validation process (refer to Chapter 5).

Figure 5.1 describes the purpose, research method, key considerations and results for this part of the study.

**Figure 5.1: Purpose, research method, key considerations and results**



**Source:** Researcher's own compilation.

The conceptual ERM implementation model will consist of the design and structuring of the ERM model (detailed by building blocks 1-4); and the implementation, monitor and review, as well as the continual improvement thereof (building blocks 5-7).

Due to the constraints of the allotted capacity of this thesis, the researcher will explain all seven building blocks that make up the foundation of the conceptual ERM implementation model. However, the researcher will only use Building block 1 of the conceptual model to explain the process that was undertaken to include the requirements (refer to Section 5.2.2), derived deliverables (refer to Section 5.2.3) and the purpose of each deliverable (refer to Section 5.2.4) within the model. All the detail associated with these aspects of building blocks 1–7 is tabled in Addendum A.

### **5.2.1 The seven building blocks**

Section 1.3 describes the three areas of concern that falls within the scope of this study. To address the aforementioned, an organisational design model (Weisbord's Six-box model), and the continual improvement model (the Deming cycle) was used as the theoretical frameworks for the design of the building blocks of the conceptual ERM implementation model. It was done intentionally to address the misalignment between the principles of organisational design and ERM program design (Martin & Power, 2007; Arena et al., 2010; Bromiley et al., 2014). This was then populated with the requirements, deliverables, and the purpose of these deliverables from Guide 73: Risk management vocabulary (ISO, 2009a), ISO 31000: Risk management principles and guidelines (ISO, 2009b), ISO 31010: Risk Management – risk assessment techniques (ISO, 2009c), and the King III Code on Governance (IODSA, 2009) in order to clarify the ambiguity surrounding the concept practice-based ERM (Arena et al., 2010; Arena et al., 2011; Mikes & Kaplan, 2013).

The alignment between Weisbord's Six-box model, the Deming Cycle and the risk management best practise requirements is illustrated in Table 5.1.

**Table 5.1: Conceptual ERM implementation model - building blocks**

| Building blocks                             | Theoretical frameworks |                                                         | Level 1 best practice requirements | Level 2 best practice requirements |
|---------------------------------------------|------------------------|---------------------------------------------------------|------------------------------------|------------------------------------|
|                                             | Deming cycle           | Weisbord organisational design model                    | Source                             | Source                             |
| I. Get permission.                          | Plan                   | Purpose, Leadership                                     | ISO 31000                          |                                    |
|                                             |                        |                                                         | King III                           |                                    |
|                                             |                        |                                                         | King III                           | King III                           |
|                                             |                        |                                                         | King III                           | King III                           |
|                                             |                        |                                                         | ISO 31000                          |                                    |
| II. Establish the tone of the organisation. | Plan                   | Leadership, Relationships                               | ISO 31000                          | King III                           |
|                                             |                        |                                                         |                                    | ISO 31000                          |
|                                             |                        |                                                         | King III                           |                                    |
| III. Design the rules of the game.          | Plan                   | Purpose, Relationships, Structure, External environment | ISO 31000                          | ISO 31000                          |
|                                             |                        |                                                         |                                    | ISO 31000                          |
|                                             |                        |                                                         |                                    | ISO 31000                          |
|                                             |                        |                                                         |                                    | ISO 31000 / King III               |
|                                             |                        |                                                         |                                    | ISO 31000                          |
|                                             |                        |                                                         |                                    | King III                           |

| Building blocks                      | Theoretical frameworks |                                                                                | Level 1 best practice requirements | Level 2 best practice requirements |
|--------------------------------------|------------------------|--------------------------------------------------------------------------------|------------------------------------|------------------------------------|
|                                      | Deming cycle           | Weisbord organisational design model                                           | Source                             | Source                             |
| III. Design the rules of the game.   | Plan                   | Purpose, Relationships, Structure, External environment                        | ISO 31000                          | ISO 31000                          |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | ISO 31000 / King III               |
|                                      |                        |                                                                                | ISO 31000                          | ISO 31000                          |
| IV. Develop the risk infrastructure. | Plan                   | Helping mechanisms, Relationships, Rewards                                     | ISO 31000                          | ISO 31000                          |
|                                      |                        |                                                                                | King III                           | King III                           |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                | King III                           | King III                           |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                | ISO 31000                          |                                    |
|                                      |                        |                                                                                | ISO 31000 / King III               |                                    |
| V. Implementation.                   | Do                     | Leadership, Structure, Relationships, Helping Mechanisms, External environment | ISO 31000                          | ISO 31000                          |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                | ISO 31000                          | ISO 31000                          |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                | ISO 31000                          | ISO 31000                          |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | King III                           |
|                                      |                        |                                                                                |                                    | ISO 31000                          |
|                                      |                        |                                                                                |                                    | King III                           |

| Building blocks             | Theoretical frameworks |                                      | Level 1 best practice requirements | Level 2 best practice requirements |
|-----------------------------|------------------------|--------------------------------------|------------------------------------|------------------------------------|
|                             | Deming cycle           | Weisbord organisational design model | Source                             | Source                             |
| VI. Monitor & review.       | Check                  | Rewards                              |                                    | King III                           |
|                             |                        |                                      | King III                           | King III                           |
|                             |                        |                                      |                                    | King III                           |
|                             |                        |                                      |                                    | King III                           |
|                             |                        |                                      |                                    | King III                           |
|                             |                        |                                      |                                    | King III                           |
|                             |                        |                                      |                                    | ISO 31000                          |
|                             |                        |                                      |                                    | ISO 31000                          |
|                             |                        |                                      |                                    | ISO 31000                          |
|                             |                        |                                      |                                    | ISO 31000                          |
| VII. Continual improvement. | Adjust                 | PDCA                                 | King III                           | ISO 31000                          |
|                             |                        |                                      |                                    | King III                           |
|                             |                        |                                      |                                    | ISO 31000                          |

Source: Researcher's own compilation.

The main objective and details regarding each building block will be explained in the next sections.

#### 5.2.1.1 Building block I: Get permission

The main objective of this building block is to formalise the *instruction* and *permission* for the design and implementation of an ERM program within the organisation, and to establish *leadership* of the ERM implementation model.

The **instruction** can be triggered by a business event, such as due diligence for a merger or acquisition, or by a regulatory or legal requirement, such as the Companies Act (Companies Act, 2008). The ERM project sponsor is tasked to prepare a business case document to explain the benefits and value-add proposition of an ERM implementation program to the decision makers within the organisation.

The business case document should then be presented at the relevant forum/committee for **approval**. At this stage of the process, in the absence of a formalised board risk committee, the presentation will be made at the board meeting, the executive committee meeting or another appropriate decision-making committee. Proof of the request will be the business case

document, a board/executive committee/other committee agenda item and the minutes of the relevant committee meeting where the decision will be recorded.

The next step is to establish *leadership* or board risk oversight by preparing the terms of reference for the board risk management committee or by revising the audit committee charter to include risk oversight. The scope, objectives, roles and responsibilities for risk management must then be documented in the risk management policy.

#### **5.2.1.2 Building block II: Establish the tone of the organisation**

The *tone of the organisation* in a risk context proposes that a culture of “everyone is responsible for risk management” has to be established within the organisation. This implies that every employee, from top management through to the lower level employees, displays responsible behaviour and makes risk-based decisions. This also recommends aspects such as: a common risk language is used to create risk awareness and establish a risk culture within

the organisation; a formalised risk awareness strategy and program for all the levels within the organisation; a formalised escalation process for dispute resolution within the organisation in which the board will be informed of disputes concerning, and cases of narrow avoidance of disasters associated with risk events. The aforementioned deliverables will fulfil the seven best practice requirements from ISO 31000 (ISO, 2009b) and King III (IODSA, 2009). These requirements will be discussed in Section 5.2.2.

By the end of employing building block 1 and 2 of the ERM implementation model within the organisation, ERM program design and implementation has been *instructed*, *approval* has been obtained, *leadership* established and the correct *tone of the organisation* has been created. In order to implement an effective ERM program, the *rules of the risk game* must then be developed and communicated throughout the organisation.

#### **5.2.1.3 Building block III: Design the rules of the game**

ISO 31000 (ISO, 2009b) contains detailed requirements with regards to the design of the risk management framework or, in simpler terms, *the rules of the risk game*. The different elements are: (1) establish an internal, external and risk management context and define the risk criteria; (2) develop a risk management policy; (3) formalise the risk governance framework; (4) integrate risk management into business operations; (5) align risk management and strategic objectives; (6) determine risk management performance indicators that align with performance indicators of the organisation, (7) develop internal reporting and communication guidelines and (8) develop external reporting and communication guidelines.

The only rule for the risk management process is that it should be *standardised* for the entire organisation. Consequently, the purpose of this building block is to establish the foundation and standardised guidelines for ERM within said organisation. The result is a description of the risk world within which the organisation operates by identifying internal and external stakeholders; describing the external environment and the internal value chain; having gained an understanding of the purpose of the organisation from the organisation's strategic plan and then in answer to the aforementioned, developing a risk management policy, risk governance framework, internal communication and reporting guidelines; as well as external communication and reporting guidelines. Culminating in designing a standardised risk management process which has to be used by the entire organisation.

At this stage in the model, the *instruction* to develop an ERM program has been formalised, *permission* has been granted, *leadership* has been established, the *tone of the organisation* has been established and the *rules of the risk game* have been defined. The next building block will expound the risk infrastructure needed to implement an ERM program within the organisation.

#### **5.2.1.4 Building block IV: Develop the risk infrastructure**

At this stage, the ERM program requires *physical infrastructure* for implementation. The main objective here is to identify the people, processes, systems, budget, committees, tools and models necessary to efficiently and effectively implement the ERM program within the organisation. The result is a matrix of identified risk owners, risk champions and other risk stakeholders; a list of operational processes that has to integrate with the risk management process; a systems requirements document that lists existing organisational systems where risk data can be sourced from and also describes the need for risk recording, risk monitoring and risk reporting systems; a risk management plan where the budgetary requirements are captured; a committee structure that will result in risk-based decision-making and handle the escalation of risk issues; the tools and models to record, manage and monitor risks and standardised templates to be used by all the risk stakeholders.

This concludes the design and structuring phase of the ERM implementation model. As previously stated the collective name for building blocks I to IV is the ERM program. The next section focusses on the implementation of the different elements of the conceptual ERM program.

#### **5.2.1.5 Building block V: Implement the enterprise risk management program**

This building block is divided into two sections: *the risk management framework* and the *risk management process*. With regards to the **risk management framework**, ISO 31000 (ISO, 2009b) and King III (IODSA, 2009) recommends that: (1) decisions need to be made with regards to the appropriate timing and strategy for implementation; (2) regulatory and legal compliance with regards to risk should be ensured; (3) risk tolerance levels and risk appetite statements must be formalised, communicated to the relevant departments/divisions and it must be implemented; and (4) regular risk awareness and training sessions must be held for all the levels of employees. With regards to the **risk management process**, ISO 31000 (ISO, 2009b), ISO 31010 (ISO, 2009c) and King III (IODSA, 2009) recommend that: (1) the internal and external stakeholders have to be identified, risk communication plans have to be finalised and the relevant risk reports have to be populated and distributed to the relevant risk stakeholders; (2) the internal, external and risk management context of the organisation or the specific division/department/project has to be established; (3) the key risks for the organisation (top-down process) and for the different divisions/departments/projects (bottom-up process) have to be identified, analysed and evaluated; (4) the risks with the highest risk score have to be treated in accordance with the approved risk controls and risk treatment options.

The successful implementation of the ERM program will depend on the clarity and transparency regarding the design; quality of relationships between internal and external risk stakeholders and the ERM department, and whether there are clear communication guidelines. At this point, the ERM program has been designed and implemented. The next step will describe the purpose of the monitoring and review activities associated with the ERM program.

#### **5.2.1.6 Building block VI: Monitor and review the enterprise risk management program's performance**

Monitoring and review activities should be explicitly included in the ERM implementation model. According to ISO 31000 (ISO, 2009b), the organisation's monitoring and review processes should encompass all aspects of the risk management process. This is to ensure that all the controls are effective and efficient in both design and operation; to obtain additional information to improve risk assessment; to intentionally document and analyse lessons learnt from events (including near-misses), changes, trends, successes and failures; to be conscious of changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and to identify emerging risks.

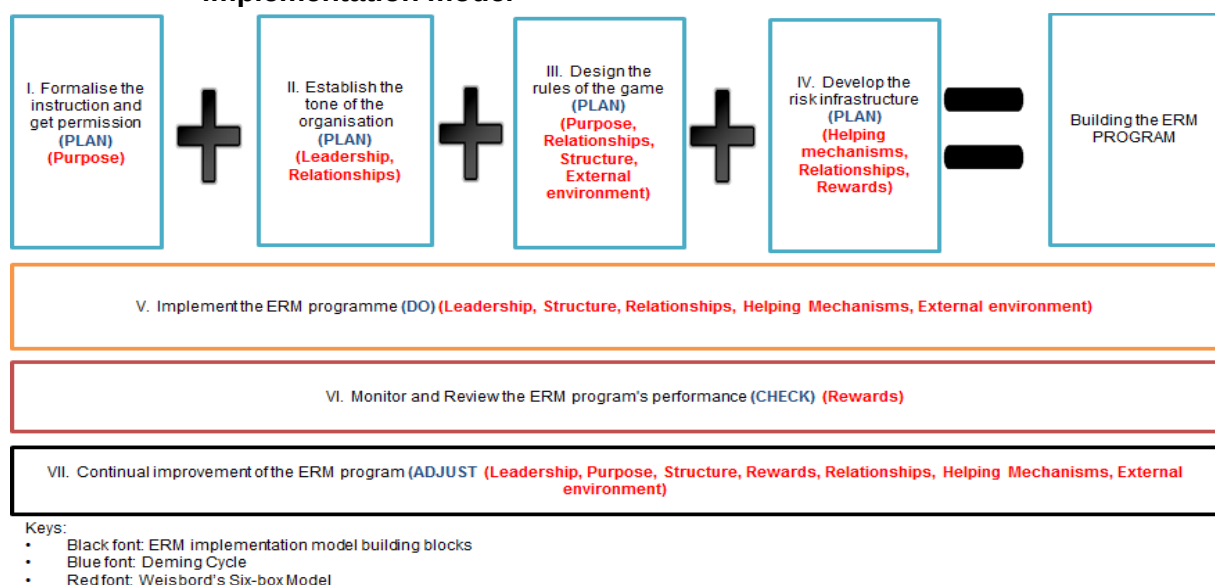
In response to the recommendations from ISO 31000 (ISO, 2009b), the building block is divided into six categories: (1) monitoring activities by the board; (2) review activities by the board; (3) monitoring of the risk management framework, (4) review of the risk management framework; (5) monitoring of the risk management process, and (6) review of the risk management process.

#### 5.2.1.7 Building Block VII: Continual improvement of the enterprise risk management program

The proposed *continual improvement process* is based on the Deming cycle as it was discussed in Section 3.4. The final building block deals with continual improvement of both the risk management framework and the risk management process. It should result in a more agile and fit-for-purpose ERM implementation program (Choi, 1995). As an example, continual improvement with the ERM implementation will be triggered by lessons learnt as discussed in building block VI: the best practice requirements regarding the annual review of the ERM framework, policy and process and improvements suggested by risk stakeholders that are involved in the day-to-day implementation of risk management. It is a repeatable cycle.

Figure 5.2 illustrates an overview of the above-mentioned building blocks of the conceptual ERM implementation model as based on Weisbord's Six-box organisational design model and the Deming Cycle (a continual improvement model). This was intentionally done to bridge the gap between organisational design and ERM implementation program design as alluded to by several stakeholders within the ERM domain (Arena *et al.*, 2010; Bromiley *et al.*, 2014).

**Figure 5.2: An overview of the proposed building blocks of the conceptual ERM implementation model**



**Source:** Researcher's own compilation.

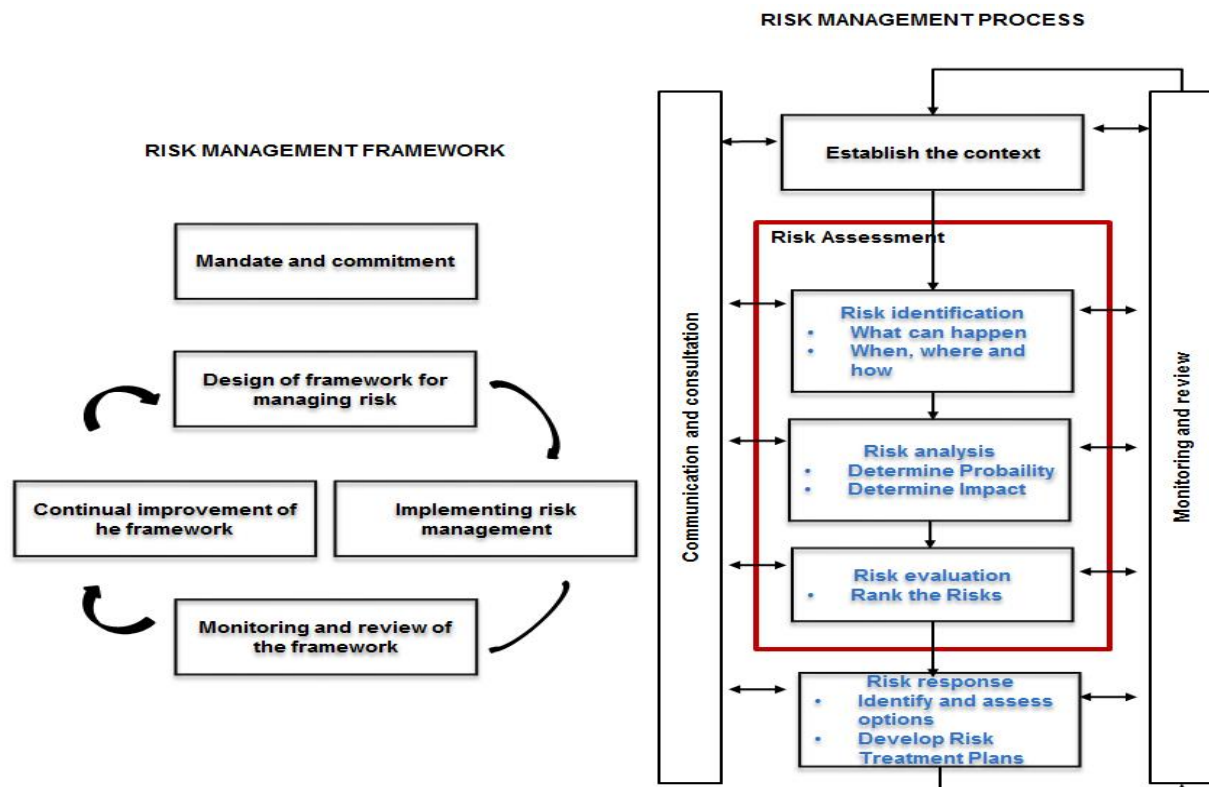
## 5.2.2 Requirements

There are several best practice frameworks for risk management within the ERM landscape that could be utilised as a foundation to identify the requirements to include for each of the seven building blocks. Some examples include:

- Enterprise risk management — integrated framework (COSO, 2004);
- AS/NZS 4360:2004 - Risk management (AUS/NZ, 2004);
- ISO 31000: 2009 - Risk management: principles and guidelines (ISO, 2009b); and
- King III: 2009 Code on Corporate Governance (IODSA, 2009).

The results of the phase 1 questionnaire (refer to Figure 4.16) indicated that the majority of risk practitioners utilise a combination of best practice risk management frameworks as the basis for their organisation's ERM programs. The researcher used ISO 31000 as it is an international standard for risk management (illustrated in Figure 5.3); and King III (refer to Figure 5.4) as the study focuses on South African organisations, as the basis for the ERM implementation model requirements.

**Figure 5.3: ISO 31000 – Risk management principles and guidelines**



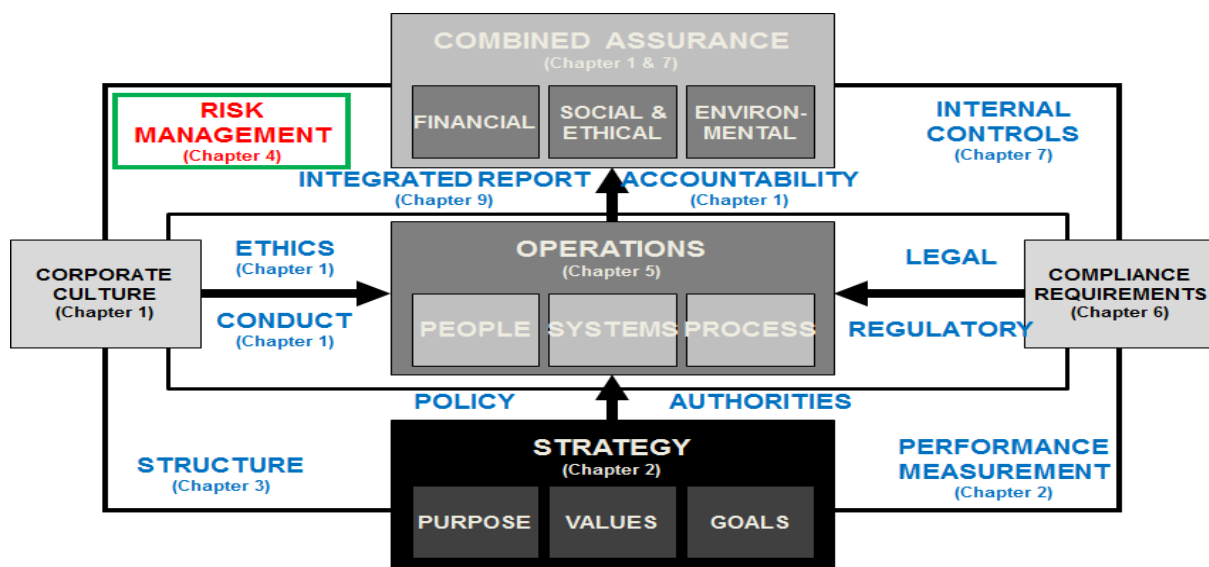
**Source:** ISO (2009b).

ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management as a guideline for risk management principles, frameworks and processes. The guideline can be applied to any organisation of any size in any industry, but in order for risk management to be effective it has to comply with the following principles (ISO, 2009b):

- Risk management creates and protects value;
- Risk management is an integral part of all organisational processes;
- Risk management is part of decision making;
- Risk management explicitly addresses uncertainty;
- Risk management is systematic, structured and timely;
- Risk management is based on the best available information;
- Risk management is tailored;
- Risk management takes human and cultural factors into account;
- Risk management is transparent and inclusive;
- Risk management is dynamic, iterative and responsive to change; and
- Risk management facilitates continual improvement of the organisation.

The success of risk management will depend on the effectiveness of the risk management framework. The guideline suggests the following steps for the risk management framework: (1) mandate and commitment, (2) design the framework, (3) implement risk management, (4) monitor and review the risk management framework, and (5) continual improvement of the framework. The suggested risk management process is: (1) communication and consultation, (2) establish the context, (3) risk assessment, (4) risk treatment and (5) monitor and review (ISO, 2009b).

**Figure 5.4: King III – Code of Corporate Governance for South Africa**



**Source:** King Code on Corporate Governance (IODSA, 2009).

The underlying philosophy of the King III Code of Governance (2009) revolves around leadership, sustainability and corporate citizenship. Chapter 4 of King III provides guidelines with regards to the risk governance responsibilities of Boards of Directors, together with guidelines on management's responsibility for risk management, risk assessment, risk response, risk monitoring, risk assurance and risk disclosure.

ISO 31000 and King III simply provide best practice guidelines with regards to risk management, but it does not provide guidance on how to implement risk management. The purpose of this study therefore is to provide the aforementioned practical guidance to risk practitioners with regards to a conceptual ERM implementation model to employ within their organisations.

Section 5.2.1 detailed the seven building blocks forming the foundation of the conceptual ERM implementation model. That in itself, however, is not enough to guide a risk stakeholder effectively. As a result, the researcher allocated requirements identified from the above-mentioned frameworks to each of these building blocks.

These *requirements* were categorised in two levels. **Level 1** requirements consist of a list of the overarching requirements associated with each building block. In some instances, however, these level 1 requirements needed to be expounded with more detailed requirements that were selected to be included as **level 2**.

Table 5.2 explains, as an example, the process to identify the best practice requirements for Building block 1 – Get permission. The level 1 and level 2 columns contain an extract from the best practice document, the source column specifies the name of the best practice document and the references column refers to the specific reference paragraph in the source document.

**Table 5.2: Best practice requirements for Building block I – Get permission**

| Best practice requirements                                                                                           |           |      |         |        |      |
|----------------------------------------------------------------------------------------------------------------------|-----------|------|---------|--------|------|
| Level 1                                                                                                              | Source    | Ref. | Level 2 | Source | Ref. |
| Ensure legal and regulatory compliance.                                                                              | ISO 31000 | 4.2  |         |        |      |
| The board should delegate to management the responsibility to design, implement and monitor the risk management plan | King III  | 4.4  |         |        |      |

| Best practice requirements                                                                              |           |             |                                                                                                                                                                                                                 |          |         |
|---------------------------------------------------------------------------------------------------------|-----------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|---------|
| Level 1                                                                                                 | Source    | Ref.        | Level 2                                                                                                                                                                                                         | Source   | Ref.    |
| The risk committee or audit committee should assist the board in carrying out its risk responsibilities | King III  | 4.3         | The board should appoint a committee responsible for risk.                                                                                                                                                      | King III | 4.3.1   |
|                                                                                                         |           |             | The risk committee should:                                                                                                                                                                                      |          | 4.3.2   |
|                                                                                                         |           |             | <ul style="list-style-type: none"> <li>consider the risk management policy and plan and monitor the risk management process;</li> </ul>                                                                         |          | 4.3.2.1 |
|                                                                                                         |           |             | <ul style="list-style-type: none"> <li>have as its members' executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;</li> </ul> |          | 4.3.2.2 |
|                                                                                                         |           |             | <ul style="list-style-type: none"> <li>have a minimum of three members; and</li> </ul>                                                                                                                          |          | 4.3.2.3 |
|                                                                                                         |           |             | <ul style="list-style-type: none"> <li>convene at least twice per year.</li> </ul>                                                                                                                              |          | 4.3.2.4 |
|                                                                                                         |           |             | The board's responsibility for risk governance should be expressed in the board charter.                                                                                                                        |          | 4.1.3   |
| Define and endorse the risk management policy                                                           | King III  | 4.1.1       | The board's responsibility for risk governance should manifest in a documented risk management policy and plan.                                                                                                 | King III | 4.1.5   |
|                                                                                                         |           |             | The board should approve the risk management policy and plan.                                                                                                                                                   |          | 4.1.6   |
|                                                                                                         | ISO 31000 | 4.2 & 4.3.2 | The risk management policy should be widely distributed throughout the company.                                                                                                                                 |          | 4.1.7   |

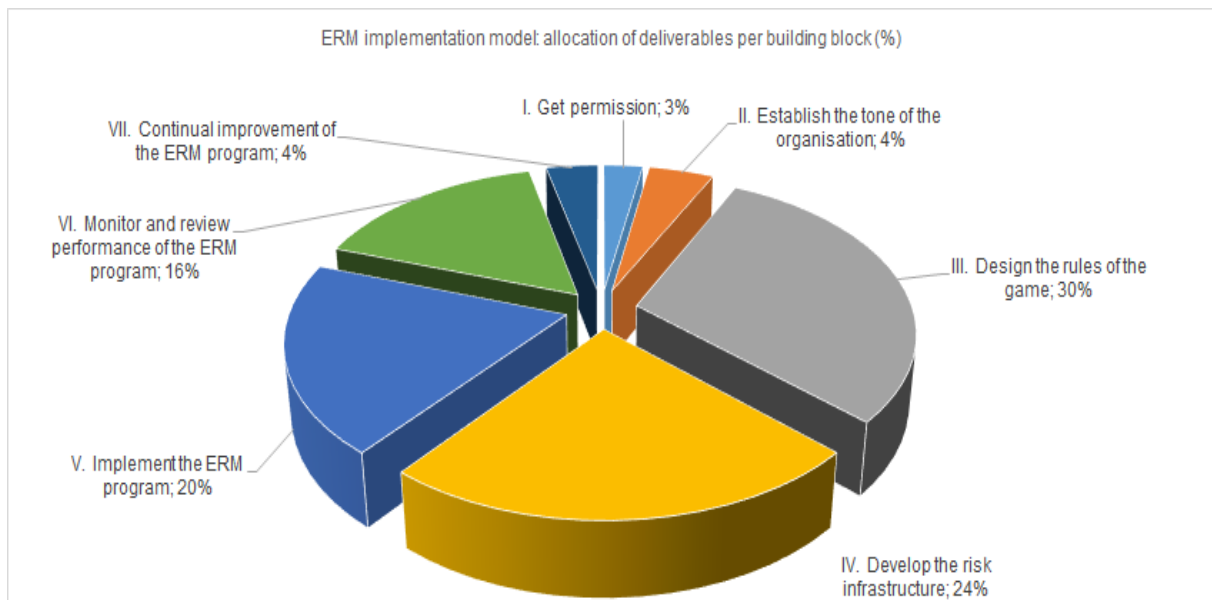
**Source:** ISO 31000 (2009b) and King III (2009).

### 5.2.3 Derived deliverables

The next part of the study is an attempt to provide risk practitioners with tangible deliverables for each requirement per building block. The proposed deliverables were derived from the discussed requirements (Section 5.2.2), based on the researcher's practical experience in

different industries, professional bodies' risk management guidelines (IRM, 2002; IRMSA, 2014), professional bodies' practice notes (CIPS, 2014), standard setting organisations (ISO, 2009b, ISO, 2009c, IODSA, 2009) and suggestions by other authors (Garvey, 2008; Likhang, 2009; Chapman, 2011). Figure 5.5 depicts the percentage of the total number of derived deliverables per ERM implementation model building block.

**Figure 5.5: Allocation of deliverables per ERM implementation model building block**



**Source:** Researcher's own compilation.

The purpose of the building blocks, together with the best practice requirements informed the decision with regards to specific derived deliverables. For example, the last requirement for building block I states: "Define and endorse the risk management policy". The logical *derived deliverable* is an *approved risk management policy* as depicted in Table 5.3.

**Table 5.3: Derived deliverables for building block I – Get permission**

| Best practice requirements                                                                                           |         | Deliverables                                                            |
|----------------------------------------------------------------------------------------------------------------------|---------|-------------------------------------------------------------------------|
| Level 1                                                                                                              | Level 2 |                                                                         |
| Ensure legal and regulatory compliance.                                                                              |         | Compliance requirements (legal + regulatory + best practise frameworks) |
| The board should delegate to management the responsibility to design, implement and monitor the risk management plan |         | Agenda item for board meeting                                           |
|                                                                                                                      |         | Minutes of the board meeting                                            |

| Best practice requirements                                                                              |                                                                                                                                                                                                                 | Deliverables                       |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Level 1                                                                                                 | Level 2                                                                                                                                                                                                         |                                    |
| The risk committee or audit committee should assist the board in carrying out its risk responsibilities | The board should appoint a committee responsible for risk.                                                                                                                                                      | Board risk committee (BRC) charter |
|                                                                                                         | The risk committee should:                                                                                                                                                                                      |                                    |
|                                                                                                         | <ul style="list-style-type: none"> <li>consider the risk management policy and plan and monitor the risk management process;</li> </ul>                                                                         |                                    |
|                                                                                                         | <ul style="list-style-type: none"> <li>have as its members' executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;</li> </ul> |                                    |
|                                                                                                         | <ul style="list-style-type: none"> <li>have a minimum of three members; and</li> </ul>                                                                                                                          | Board risk committee (BRC) charter |
|                                                                                                         | <ul style="list-style-type: none"> <li>convene at least twice per year.</li> </ul>                                                                                                                              |                                    |
|                                                                                                         | <ul style="list-style-type: none"> <li>The board's responsibility for risk governance should be expressed in the board charter.</li> </ul>                                                                      |                                    |
| Define and endorse the risk management policy                                                           | The board's responsibility for risk governance should manifest in a documented risk management policy and plan.                                                                                                 | Risk management policy             |
|                                                                                                         | The board should approve the risk management policy and plan.                                                                                                                                                   |                                    |
|                                                                                                         | The risk management policy should be widely distributed throughout the company.                                                                                                                                 |                                    |

**Source:** Researcher's own compilation.

#### 5.2.4 Purpose of each deliverable

The purpose for each derived deliverable explains the intention of each derived deliverable in the context of the specific building block and the assigned requirements. Successful ERM implementation requires a common understanding of risk related terms and concepts in the organisation. The description relating to the purpose of the derived deliverables is an effort to establish a common risk language amongst all the risk stakeholders. The intention was to remove ambiguity from the model and to embed one concept of ERM in the organisation.

Table 5.4 contains the level 1 and level 2 best practise requirements, as well as the purpose of the proposed deliverables.

**Table 5.4: Purpose of the derived deliverables for building block I – Get permission**

| Best practice requirements                                                                                           |                                                                                                                                                                                                                 | Proposed deliverables                                                               |
|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Level 1                                                                                                              | Level 2                                                                                                                                                                                                         | Purpose                                                                             |
| Ensure legal and regulatory compliance.                                                                              |                                                                                                                                                                                                                 | To motivate the need for an ERM program.                                            |
| The board should delegate to management the responsibility to design, implement and monitor the risk management plan |                                                                                                                                                                                                                 | To ask for permission / mandate to design and implement the ERM program.            |
|                                                                                                                      |                                                                                                                                                                                                                 | To record the permission / mandate received to design and implement an ERM program. |
| The risk committee or audit committee should assist the board in carrying out its risk responsibilities              | The board should appoint a committee responsible for risk.                                                                                                                                                      | To assist the board in carrying out its risk roles and responsibilities.            |
|                                                                                                                      | The risk committee should:                                                                                                                                                                                      |                                                                                     |
|                                                                                                                      | <ul style="list-style-type: none"> <li>consider the risk management policy and plan and monitor the risk management process;</li> </ul>                                                                         |                                                                                     |
|                                                                                                                      | <ul style="list-style-type: none"> <li>have as its members' executive and non-executive directors, members of senior management and independent risk management experts to be invited, if necessary;</li> </ul> |                                                                                     |
|                                                                                                                      | <ul style="list-style-type: none"> <li>have a minimum of three members; and</li> </ul>                                                                                                                          |                                                                                     |
|                                                                                                                      | <ul style="list-style-type: none"> <li>convene at least twice per year.</li> </ul>                                                                                                                              |                                                                                     |
|                                                                                                                      | The board's responsibility for risk governance should be expressed in the board charter.                                                                                                                        |                                                                                     |
| Define and endorse the risk management policy                                                                        | The board's responsibility for risk governance should manifest in a documented risk management policy and plan.                                                                                                 | To document risk management scope, objectives and roles and responsibilities.       |
|                                                                                                                      | The board should approve the risk management policy and plan.                                                                                                                                                   |                                                                                     |
|                                                                                                                      | The risk management policy should be widely distributed throughout the company.                                                                                                                                 |                                                                                     |

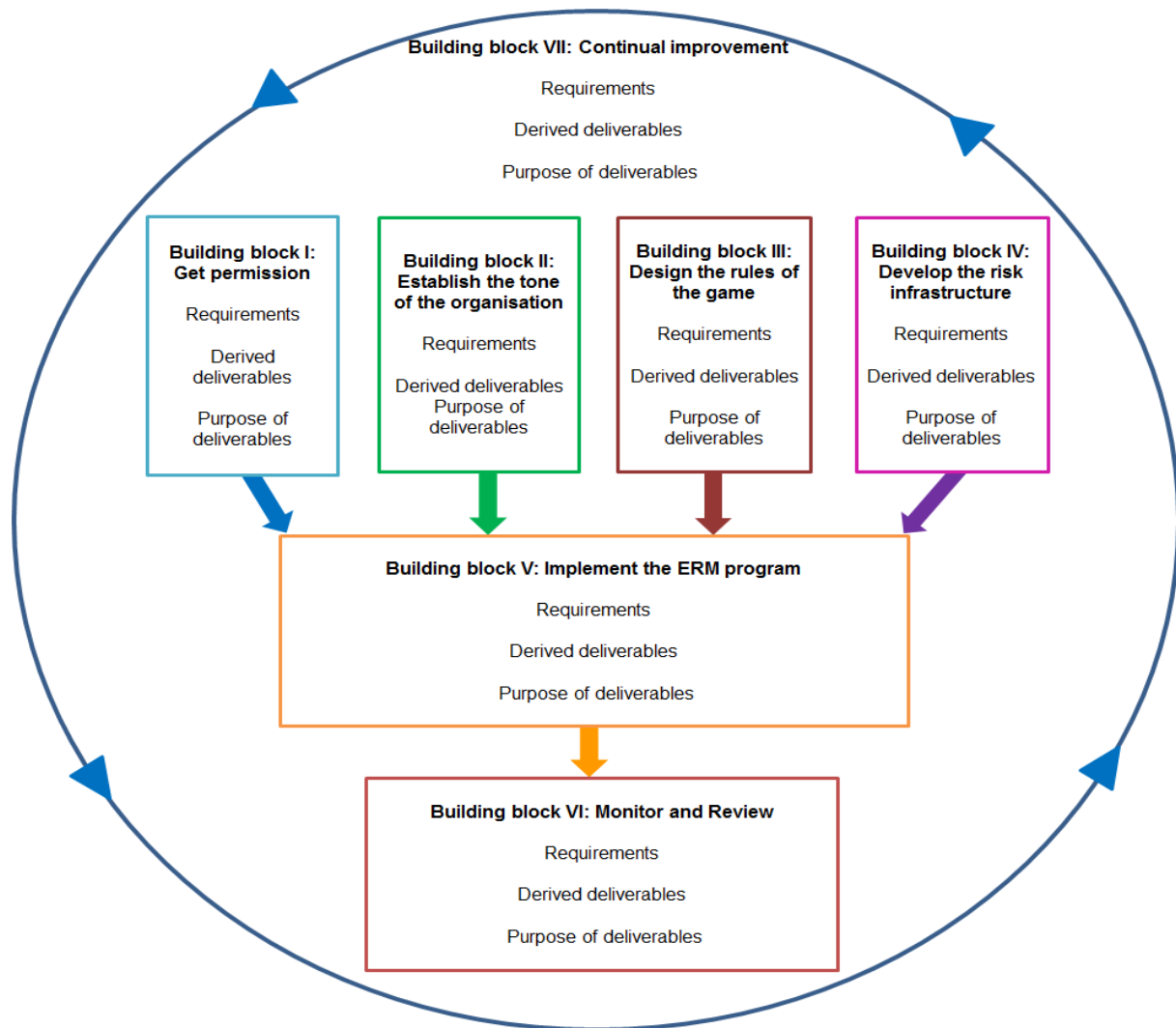
**Source:** Researcher's own compilation.

### 5.2.5 Conceptual enterprise risk management implementation model

Figure 5.6 illustrates the detailed conceptual ERM implementation model (including the discussed seven building blocks, requirements, derived deliverables and the purpose of each of these deliverables) intended for use by risk stakeholders within any organisation and

industry. This conceptual model will be used as the foundation for validating an ERM implementation model empirically, utilising the Delphi technique, and will be discussed in further detail in Chapters 6.

**Figure 5.6: An overview of the conceptual ERM implementation model**



**Source:** Researcher's own compilation.

Table 5.5 reflects the alignment between the Deming cycle and Weisbord's Six-box organisational design model and the elements of the conceptual ERM implementation model (including the discussed seven building blocks, requirements, derived deliverables and the purpose of each of these deliverables). The detail of the theoretical frameworks (Weisbord's six-box organisational design model and the Deming Cycle) were discussed in Sections 3.1.3 and 3.4. Section 5.2 describes the detail of the conceptual ERM implementation model.

**Table 5.5: Conceptual ERM implementation model – theoretical frameworks and best practice requirements**

| Theoretical frameworks |                                                         | Building blocks                             | Level 1 best practice requirements |             | Level 2 best practice requirements |                               |
|------------------------|---------------------------------------------------------|---------------------------------------------|------------------------------------|-------------|------------------------------------|-------------------------------|
| Deming cycle           | Weisbord organisational design model                    |                                             | Source                             | Ref.        | Source                             | Ref.                          |
| Plan                   | Purpose, Leadership                                     | I. Get permission.                          | ISO 31000                          | 4.2         |                                    |                               |
|                        |                                                         |                                             | King III                           | 4.4         |                                    |                               |
|                        |                                                         |                                             | King III                           | 4.3         | King III                           | 4.3.1                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.1                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.2                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.3                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.4                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.3                         |
|                        |                                                         |                                             | King III                           | 4.1.1       | King III                           | 4.1.5                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.6                         |
|                        |                                                         |                                             | ISO 31000                          | 4.2 & 4.3.2 |                                    | 4.1.7                         |
| Plan                   | Leadership, Relationships                               | II. Establish the tone of the organisation. | ISO 31000                          | 4.2         | King III                           | 4.4.3                         |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.2                           |
|                        |                                                         |                                             | King III                           | 4.1.4       |                                    |                               |
| Plan                   | Purpose, Relationships, Structure, External environment | III. Design the rules of the game.          | ISO 31000                          | 4.3         | ISO 31000                          | 4.3.1 & 5.3.2                 |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.3.1 & 5.3.3                 |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.3.1 & 5.3.4                 |
|                        |                                                         |                                             |                                    |             | ISO 31000 / King III               | 4.3.1 & 5.3.5 / 4.2.1 & 4.2.2 |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.3.2                         |
|                        |                                                         |                                             |                                    |             | King III                           | 4.1.1                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.5                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.6                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.7                         |

| Theoretical frameworks |                                                                                | Building blocks                      | Level 1 best practice requirements |                       | Level 2 best practice requirements |               |
|------------------------|--------------------------------------------------------------------------------|--------------------------------------|------------------------------------|-----------------------|------------------------------------|---------------|
| Deming cycle           | Weisbord organisational design model                                           |                                      | Source                             | Ref.                  | Source                             | Ref.          |
| Plan                   | Purpose, Relationships, Structure, External environment                        | III. Design the rules of the game.   | ISO 31000                          | 4.3                   | ISO 31000                          | 4.3.3         |
|                        |                                                                                |                                      |                                    |                       | King III                           | 4.4.2         |
|                        |                                                                                |                                      |                                    |                       | ISO 31000                          | 4.3.4         |
|                        |                                                                                |                                      |                                    |                       | ISO 31000                          | 4.2           |
|                        |                                                                                |                                      |                                    |                       | ISO 31000                          | 4.3.6         |
|                        |                                                                                |                                      |                                    |                       | ISO 31000 / King III               | 4.3.7 / 4.10  |
|                        |                                                                                |                                      | ISO 31000                          | 5                     | ISO 31000                          | 5.2           |
|                        |                                                                                |                                      |                                    |                       |                                    | 4.3.1 & 5.3   |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.4.2         |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.4.3         |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.4.4         |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.5           |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.6           |
|                        |                                                                                |                                      |                                    |                       |                                    | 4.6           |
| Plan                   | Helping mechanisms, Relationships, Rewards                                     | IV. Develop the risk infrastructure. | ISO 31000                          | 4.3.5                 | ISO 31000                          | 4.3.5         |
|                        |                                                                                |                                      | King III                           | 2.23                  | King III                           | 2.23          |
|                        |                                                                                |                                      |                                    |                       |                                    | 2.23.1        |
|                        |                                                                                |                                      |                                    |                       |                                    | 2.23.2        |
|                        |                                                                                |                                      |                                    |                       |                                    | 2.23.3        |
|                        |                                                                                |                                      | King III                           | 2.23                  | King III                           | 4.3.2         |
|                        |                                                                                |                                      |                                    |                       | King III                           | 3.4           |
|                        |                                                                                |                                      |                                    |                       | King III                           | 3.4           |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8           |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8.1         |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8.2         |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8.2.1       |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8.2.2       |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8.2.3       |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.8.2.4       |
|                        |                                                                                |                                      |                                    |                       | King III                           | 3.5           |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.5.1         |
|                        |                                                                                |                                      |                                    |                       |                                    | 3.5.2         |
|                        |                                                                                |                                      | ISO 31000                          | 4.3.5 & 5.7           |                                    |               |
|                        |                                                                                |                                      | ISO 31000 / King III               | 4.3.4 & 4.3.5 / 4.4.1 |                                    |               |
|                        |                                                                                |                                      | ISO 31000 / King III               | 4.3.5 & 5.7 / 4.4.1   |                                    |               |
| Do                     | Leadership, Structure, Relationships, Helping Mechanisms, External environment | V. Implementation.                   | ISO 31000                          | 4.4.1                 | ISO 31000                          | 4.4.1         |
|                        |                                                                                |                                      |                                    |                       | ISO 31000                          | 4.2 & 4.4.1   |
|                        |                                                                                |                                      | ISO 31000                          | 4.4.2                 | ISO 31000                          | 5.2           |
|                        |                                                                                |                                      |                                    |                       | ISO 31000                          | 5.3           |
|                        |                                                                                |                                      | ISO 31000                          | 4.4.2                 | ISO 31000                          | 5.3.2 & 4.3.1 |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.3.3 & 4.3.1 |
|                        |                                                                                |                                      |                                    |                       |                                    | 5.3.4 & 4.3.1 |

| Theoretical frameworks |                                      | Building blocks             | Level 1 best practice requirements |           | Level 2 best practice requirements |               |
|------------------------|--------------------------------------|-----------------------------|------------------------------------|-----------|------------------------------------|---------------|
| Deming cycle           | Weisbord organisational design model |                             | Source                             | Ref.      | Source                             | Ref.          |
|                        |                                      |                             |                                    |           |                                    | 5.3.5 & 4.3.1 |
|                        |                                      |                             |                                    |           | ISO 31000                          | 5.4.2         |
|                        |                                      |                             |                                    |           | King III                           | 4.5           |
|                        |                                      |                             |                                    |           | ISO 31000                          | 5.4.3         |
|                        |                                      |                             |                                    |           | King III                           | 4.5           |
|                        |                                      |                             |                                    |           | ISO 31000                          | 5.4.4         |
|                        |                                      |                             |                                    |           | King III                           | 4.5           |
|                        |                                      |                             |                                    |           | ISO 31000                          | 5.5           |
| Check                  | Rewards                              | VI. Monitor & review.       |                                    |           | King III                           | 4.8           |
|                        |                                      |                             |                                    |           |                                    | 4.8.1         |
|                        |                                      |                             |                                    |           |                                    | 4.8.2         |
|                        |                                      |                             | King III                           | 4.1 & 4.3 | King III                           | 4.1.2         |
|                        |                                      |                             |                                    |           | King III                           | 4.1.8         |
|                        |                                      |                             |                                    |           | King III                           | 4.1.9         |
|                        |                                      |                             |                                    |           | King III                           | 4.3.3         |
|                        |                                      |                             |                                    |           | King III                           | 4.2.3         |
|                        |                                      |                             |                                    |           | ISO 31000                          | 4.5           |
|                        |                                      |                             |                                    |           | ISO 31000                          | 4.5           |
|                        |                                      |                             |                                    |           | ISO 31000                          | 4.2 & 4.4.1   |
|                        |                                      |                             |                                    |           | ISO 31000                          | 4.5           |
| Adjust                 | PDCA                                 | VII. Continual improvement. | King III                           | 4.9       | King III                           | 4.9.1         |
|                        |                                      |                             |                                    |           | ISO 31000                          | 5.6           |

**Source:** Researcher's own compilation.

In summary, the study conducted an extensive evaluation of the systems based models of organisational design by determining the theory base, benefits and limitations of each model. The identified aspects of each model were then measured against the characteristics of effective organisational design (*simplicity, flexibility, reliability, economy and acceptability*) (Johnson *et al.*, 1973) and Weisbord's Six-box model (Weisbord, 1976) was chosen. This model was used as the foundation in conjunction with a focus on continual improvement (the Deming cycle) to develop the postulated conceptual ERM implementation model consisting of building blocks, requirements, deliverables, and the purpose of the deliverable.

The characteristics of effective organisational design - simplicity, flexibility, reliability, economy and acceptability (Johnson *et al.*, 1973) - will now also be employed to evaluate the design of the conceptual ERM implementation model.

The model design outline is **simple** in that it follows a building block approach where the one step builds on the previous to produce a result. For example: building block I to IV represents all the elements that have to be designed and developed for the ERM program. Building block V to VII includes all the activities relevant to the entire ERM program and it represents a continuous cycle of implementation, monitoring, review and continual improvement.

The conceptual model is **flexible** in the sense that derived deliverables can be included or excluded or expanded to reflect the requirements of the specific type of organisation. For example: one of the deliverables from building block I is to get permission for the design and implementation of an ERM program. The derived deliverable is an agenda item for the board meeting. The decision-making body for a listed company will be the board of directors, whereas the decision making body for a government entity will be located in the office of the minister. The deliverable can easily be changed to reflect that.

Even though the conceptual ERM model is flexible and could be changed, the model was intentionally designed to be prescriptive in terms of the building blocks, associated requirements, and proposed deliverables to ensure the **reliability** of the outcomes during the implementation process.

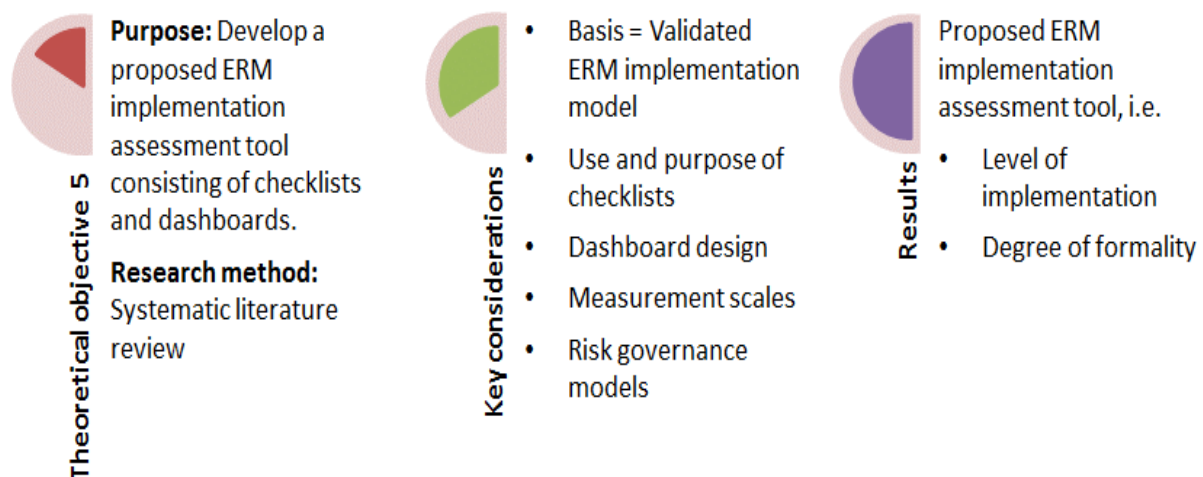
Generally, there are limited resources available for the design and implementation of ERM programs. The prescriptive nature of the conceptual model is such that it should result in improved allocation of scarce risk resources and it consequently adheres to the **economy** characteristic of organisational design. The conceptual model is an attempt to answer the call for a practice-based ERM model that will be easy to understand and that can be implemented by risk stakeholders. This should result in a higher level of **acceptability**.

The complete conceptual ERM implementation model (including all seven building blocks, requirements, derived deliverables and the purpose of each deliverable within the model) is included in Addendum A.

### **5.3 PROPOSED ENTERPRISE RISK MANAGEMENT IMPLEMENTATION ASSESSMENT TOOL**

Section 5.2 concluded the discussion pertaining to the conceptual ERM implementation model and all of its components. Now the focus will shift to the proposed ERM implementation assessment tool that will be used to determine the status of ERM implementation within the organisation and the validated degree of formality achieved. Figure 5.7 describes the purpose, research method, key considerations and results for this part of the study.

**Figure 5.7: Purpose, research method, key considerations and results**



**Source:** Researcher's own compilation.

The ERM implementation assessment activities are executed in accordance with the approved risk governance framework and model for the organisation (refer to Section 5.3.1). The ERM implementation assessment tool consists of:

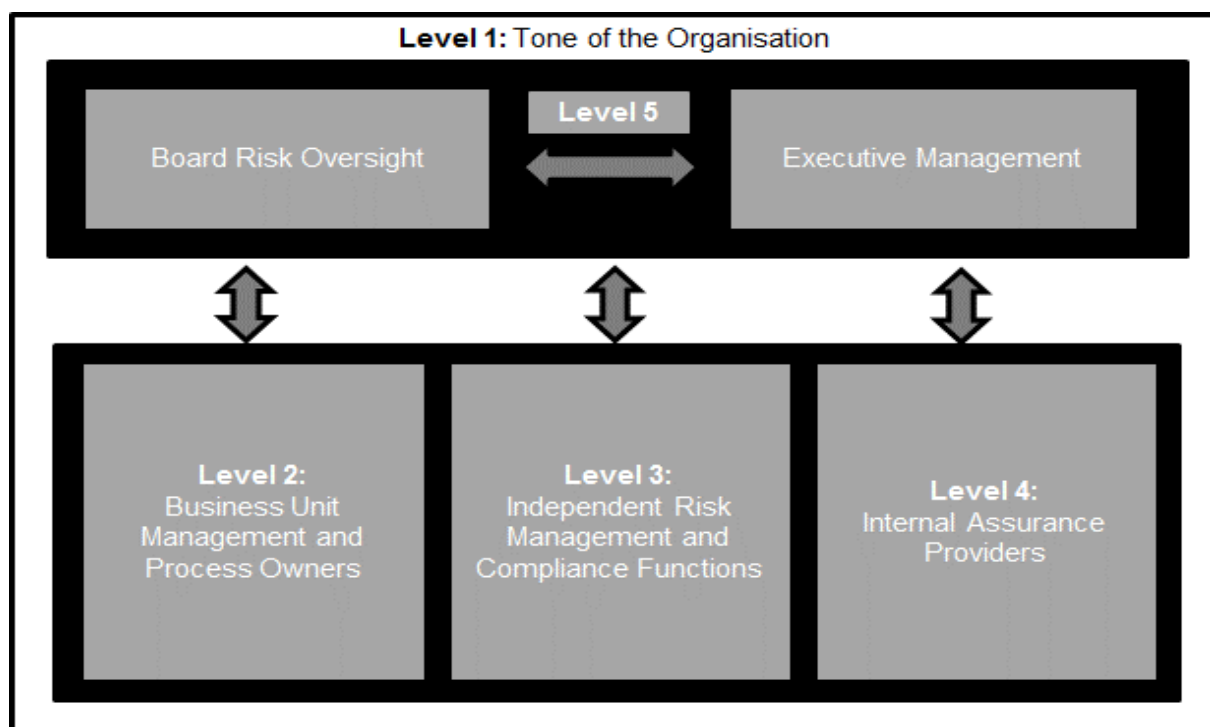
- A *level of ERM implementation checklist* to determine the status of ERM implementation, either per ERM implementation model building block or per risk stakeholder (refer to Section 5.3.2.1);
- A *level of ERM implementation reporting dashboard* (refer to Section 5.3.2.2) that will be communicated to the relevant committees and the ERM project sponsor;
- An *ERM implemented deliverables degree of formality assessment checklist* (refer to Section 5.3.3.1) that will be used by an independent assurer to determine the degree to which an implemented deliverable is actually completed; and
- An *ERM implemented deliverables degree of formality assessment reporting dashboard*, either per ERM implementation model building block or per risk stakeholder (refer to Section 5.3.3.2) that will be communicated to the relevant committees and the ERM project sponsor.

### 5.3.1 Example of a risk governance model

Mark Bevir (2012) defined governance as all of the processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organisation or territory and whether through the laws, norms, power or language. Bevir's definition supports Marc Hufty's (2011) description of governance as the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions.

*Risk governance* provides the structure of the risk management system and specifies responsibilities, authority, and accountability in the risk management system as well as the rules and procedures for making decisions in risk management (Aebi, Sabato, & Schmid, 2012). The King Code on Governance for South Africa clearly states that the organisation's board is responsible for the governance of risk and management is responsible for risk management (IODSA, 2009). Several consulting firms have proposed either *three* (Lvov, 2009; Newsome, 2011; IIA, 2013) or *five* (Protiviti, 2013) *lines-of-defence risk governance models*. The ERM implementation assessment tool will be explained in terms of Protiviti's five-lines-of-defence risk governance model as illustrated in Figure 5.8.

**Figure 5.8: Protiviti's Five-lines-of-defence risk governance model**



Source: Protiviti (2013)

According to Protiviti (2013), the *first line-of-defence* describes an organisation aware of its internal and external risk throughout the culture or tone of the organisation. In other words, “everyone accepts responsibility for risk management”. The *second line-of-defence* discusses the business unit and process owners’ responsibilities regarding risk management. The third line-of-defence pertains to the risk responsibilities of the independent risk and compliance functions. The fourth line-of-defence belongs to the internal and external auditors (hereafter the assurance providers) and the fifth line-of-defence describes the risk oversight responsibilities of the board and executive management. The detail of the model is described in Table 5.6.

**Table 5.6: Protiviti's Five-lines-of-defence risk governance model**

| Line of defence (LoD)          | Role Players                              | Explained                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1st LoD: Risk awareness</b> | Board & executive management              | To establish a risk aware culture where all levels in the organisation accepts responsibility for risk management resulting in responsible risk behaviour.                                                                                                                                                                                            |
|                                |                                           | Dispute resolution by the board: as for a formalised escalation process, even in circumstances where the CEO (or preferably, an executive risk committee or equivalent group) resolves disputes between the second and third lines-of-defence, the board should be informed to the extent such disputes are about significant matters or close calls. |
| <b>2nd LoD: Risk owners</b>    | Business Unit Management & Process Owners | To own and manage the risks their units and processes create, as well as establish the proper tone for managing these risks consistent with the tone at the top.                                                                                                                                                                                      |
|                                |                                           | As the risk owners, these managers:                                                                                                                                                                                                                                                                                                                   |
|                                |                                           | <ul style="list-style-type: none"> <li>• Set objectives;</li> <li>• Establish risk responses;</li> <li>• Train personnel; and</li> <li>• Implement and reinforce risk response strategies.</li> </ul>                                                                                                                                                 |
|                                |                                           | Risk treatment: they implement and maintain effective internal control procedures on a day-to-day basis and are best positioned to integrate risk management capabilities with the activities that create the risks.                                                                                                                                  |
|                                |                                           | Risk monitoring: they must accept and cooperate with the oversight activities of risk management and compliance functions and the assurance activities of internal audit; it is a bright red warning flag if they do not.                                                                                                                             |

| Line of defence (LoD)                       | Role Players                             | Explained                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3<sup>rd</sup> LoD:<br/>Risk Control</b> | Independent Risk Management & Compliance | Effective risk and compliance management requires an independent, authoritative voice to ensure that                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                             |                                          | <ul style="list-style-type: none"> <li>an enterprise-wide framework exists for managing risk,</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                             |                                          | <ul style="list-style-type: none"> <li>risk owners are doing their jobs in accordance with that framework,</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                             |                                          | <ul style="list-style-type: none"> <li>risks are measured appropriately,</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                             |                                          | <ul style="list-style-type: none"> <li>risk limits are respected and adhered to, and</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                             |                                          | <ul style="list-style-type: none"> <li>risk reporting and escalation protocols are working as intended.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                             |                                          | Depending on the industry, these functions may include compliance, environmental, financial control, health and safety, inspection, legal approval, quality assurance, risk management, security and privacy, and supply chain.                                                                                                                                                                                                                                                                                                      |
|                                             |                                          | While these functions collaborate with unit managers and process owners to develop and monitor controls and other processes that mitigate identified risks, they also may conduct independent risk evaluations and alert management and the board to emerging risk and compliance issues.                                                                                                                                                                                                                                            |
|                                             |                                          | To be truly objective and effectively positioned within the organisation, risk management and compliance functions should be insulated from and independent of business unit operations, lines of business, and front-line, customer-facing processes of the business. The expectations of the CEO and the board set the tone in determining whether these functions constitute a robust third line-of-defence.                                                                                                                      |
|                                             |                                          | To be truly objective and effectively positioned within the organisation, risk management and compliance functions should be insulated from and independent of business unit operations, lines of business, and front-line, customer-facing processes of the business. The expectations of the CEO and the board set the tone in determining whether these functions constitute a robust third line-of-defence.                                                                                                                      |
|                                             |                                          | For example, if these functions lack the necessary veto and/or escalation authority to serve as a viable line-of-defence, they may be relegated to serving as mere champions, facilitators or reporters.                                                                                                                                                                                                                                                                                                                             |
| <b>4<sup>th</sup> LoD:<br/>Assurance</b>    | Internal & External Audit                | The fourth line-of-defence provides assurance that the other lines-of-defence are functioning effectively. Accordingly, it should use the lines-of-defence framework as a way of sharpening its value proposition by focusing its assurance activities more broadly on risk management. Internal audit reviews internal controls and risk management procedures; identifies risks, issues and improvement opportunities; makes recommendations; and keeps the board and executive management informed of the status of open matters. |

| Line of defence (LoD)   | Role Players                 | Explained                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5th LoD: Risk oversight | Board & executive Management | The board of directors and executive management play separate and distinct roles in providing the final line-of-defence. The ability to act on escalated risk information is vitally important. “Blind spots” spawned by such dysfunctional behaviour as myopic short-term focus on “making the numbers,” lack of transparency, an unbalanced compensation structure and other tone-at-the-top issues can obstruct action at the crucial moment. A leadership failure to act will almost always undermine even the strongest risk management capabilities, regardless of the various lines-of-defence in place. Under the oversight of the board of directors, executive management must manage the inevitable tension between business unit managers and independent risk management and compliance functions of the organisation by ensuring these activities are balanced appropriately, such that neither one is too disproportionately strong relative to the other. |
|                         |                              | Executive management must align governance processes, risk management capabilities and internal control toward striking the appropriate balance to optimize this natural tension between value creation and value protection. More important, they must act on risk information on a timely basis when it is escalated to them and involve the board in a timely manner when necessary. In this regard, executive management and the board’s risk oversight comprise the last line-of-defence, when significant issues are escalated upward.                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Source:** Protiviti (2013).

### 5.3.2 Level of enterprise risk management implementation

It was established in the discussion contained in Chapter 2, that ERM implementation is an organisation-spanning initiative utilising vast resources to ensure that the organisation renders their core business, mitigate uncertainty, build resilience, and be better poised for opportunities. In order to populate the continual improvement approach to ERM implementation through an action-feedback-correction loop, it is imperative that accurate reporting mechanisms are in place to establish the status of ERM implementation. This will be done by creating a *level of ERM implementation checklist* which will then be reported to the relevant risk committees with the *level of ERM implementation reporting dashboard*.

#### 5.3.2.1 Level of enterprise risk management: checklist

A checklist is a list of items required, things to be done, or points to be considered. It is generally used as a reminder. The level of ERM implementation checklist will be an extension

of the validated ERM implementation model which consists of the discussed building blocks, the associated requirements and the proposed deliverables. Refer to Addendum B for the detailed checklist.

The first item to insert is a column to pinpoint the risk stakeholder(s) responsible to design, develop and implement the respective deliverables. The appointment of these stakeholders will vary according to the organisational structure and design. For example, this could be a chief risk officer (CRO), risk owners or the company secretary.

A **CRO** is a paid executive of the organisation, who may have other duties/responsibilities, but who is primarily responsible for advising on, formulating, overseeing and managing all aspects of the organisation's risk management system; and monitors the organisation's entire risk profile, ensuring that major risks are identified and reported upwards (ISO, 2009a). A **risk owner** is a person or entity with the accountability and authority to manage risk (ISO, 2009a). The **company secretary** is responsible for the efficient administration of a company, particularly with regard to ensuring compliance with statutory and regulatory requirements and for ensuring that decisions of the board of directors are implemented.

The checklist then continues with two columns using a simple Yes/No measurement scale. The measurement scale is used to determine the level of implementation of the ERM program, either per building block as per the conceptual ERM implementation model or per risk stakeholder. The coordination and facilitation of the completion of the checklist is the responsibility of the second line-of-defence (independent risk management and compliance) in the Protiviti risk governance model. The CRO will assign a risk facilitator to the task. A risk facilitator is the person who simplifies the concept and implementation of ERM by engaging the right people at the right time with the right attitude.

The risk facilitator channels the communication of risk objectives and risk deliverables with risk owners in order to establish a common understanding of the people, processes and deliverables involved in the ERM program (Pullan & Webster-Murray, 2011).

This prescriptive checklist is a deliberate attempt to reduce the bias involved when completing the level of ERM implementation report in order to give assurance to the board and senior management regarding the true status of the level of ERM implementation.

#### **5.3.2.2 Level of enterprise risk management implementation: reporting dashboard**

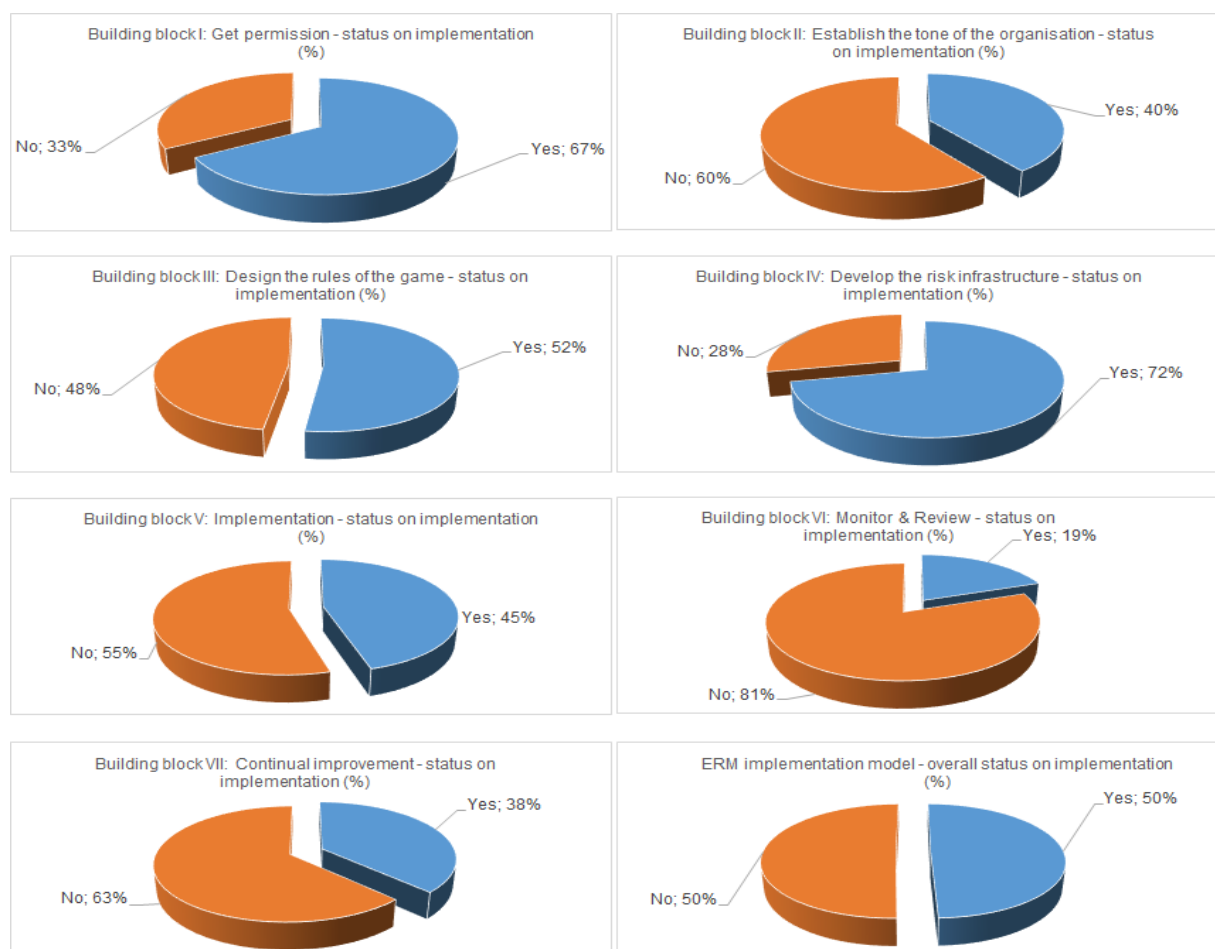
The results of the checklists will be reported with a level of ERM implementation reporting dashboard to the relevant risk committees. A dashboard is a visual interface that provides at-a-glance views into key measures relevant to a particular objective or business process.

Dashboards have three main attributes (Alexander & Walkenbach, 2013):

- Dashboards are typically graphical in nature, providing visualisations that help focus attention on key trends, comparisons, and exceptions;
- Dashboards often display only data that are relevant to the goal of the dashboard; and
- Because dashboards are designed with a specific purpose or goal, they inherently contain predefined conclusions that relieve the end user from performing his own analysis.

The reporting dashboard for the level of ERM implementation can be prepared per building block or per responsible risk stakeholder. It is based on the number of deliverables as per the Yes/No measurement scales used in the ERM implementation status checklist (refer to Section 5.3.2.1). The percentage is calculated as the number of yes or no answers as divided by the total number of deliverables. Figure 5.9 is an example of the aforementioned reporting dashboard per ERM implementation model building block.

**Figure 5.9: Level of ERM implementation reporting dashboard per ERM implementation model building block**



**Source:** Researcher's own compilation.

### **5.3.3 Degree of formality of implemented deliverables**

At this point, the ERM implementation status per ERM implementation building block or per risk stakeholder has been determined with the ERM implemented deliverables degree of formality checklist and the ERM implemented deliverables degree of formality reporting dashboards have been completed.

#### **5.3.3.1 Enterprise risk management implemented deliverables: degree of formality assessment tool**

The next step is to transfer all the implemented deliverables (the Yes answers on the ERM implementation status checklist) to the *degree of formality report*. Degree of formality refers to the extent to which the different ERM implemented deliverables have been formalised within the organisation. An independent assurer from the third line-of-defence of the risk governance model (Protiviti, 2013) will audit the implemented deliverables to confirm that it has been designed, developed and implemented by the relevant risk stakeholder.

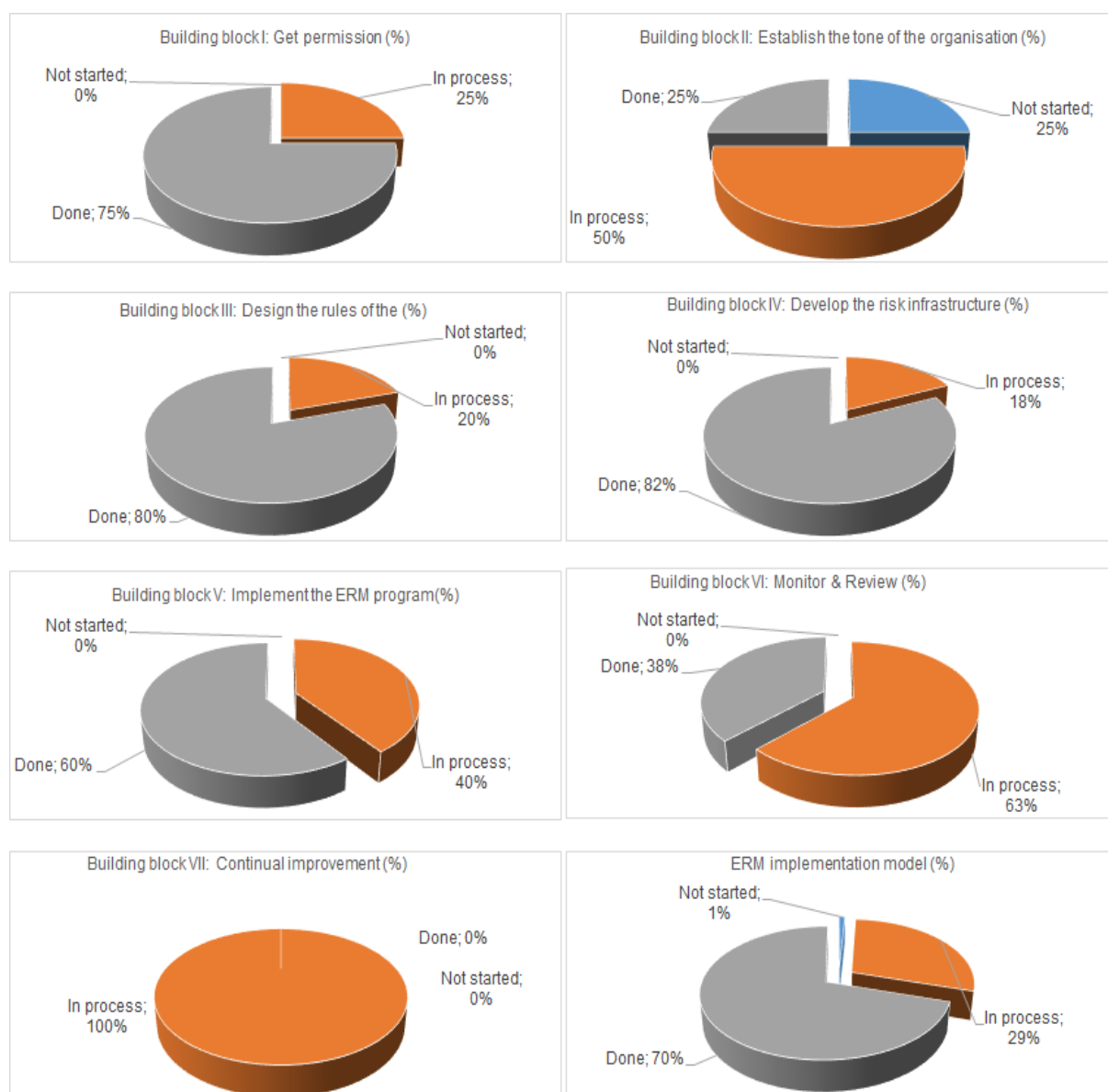
The degree of formality will be assessed with a *Not started/In process/Done* measurement scale. This assessment tool is an attempt to reduce the bias involved when completing the ERM implementation status report in order to give assurance to the board and senior management regarding the true status of the level of ERM implementation. Refer to Addendum C for the detailed ERM degree of formality checklists (after Round 3 of Delphi, it is called the Risk Assurance Checklist as per Addendum M).

The results will be summarised in a reporting dashboard, which will be discussed in the following section.

#### **5.3.3.2 Enterprise risk management implemented deliverables: degree of formality reporting dashboard**

The ERM implemented deliverables degree of formality reporting dashboard can be prepared per building block or per responsible risk stakeholder. It is based on the number of deliverables as per the *Not started/In process/Done* measurement scales used in the degree of formality assessment (refer to Section 5.3.3.1). The percentage is calculated as the number of not started or in process or done answers as divided by the total number of implemented deliverables. Figure 5.10 is an example of the aforementioned ERM implemented deliverables degree of formality reporting dashboard per ERM implementation model building block.

**Figure 5.10: ERM implemented deliverables: degree of formality reporting dashboard**



**Source:** Researcher's own compilation.

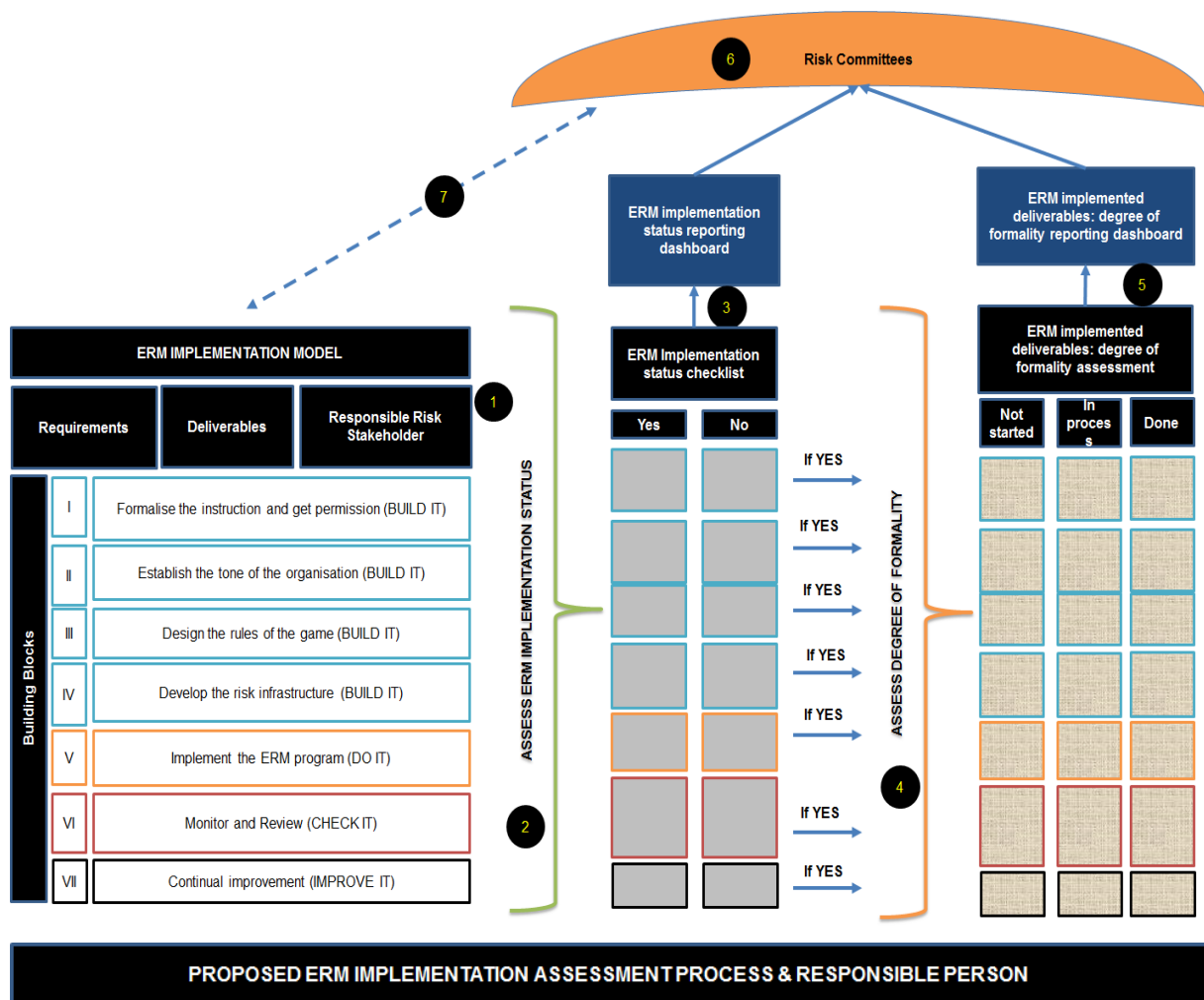
### 5.3.4 Feedback loops

The ERM implementation status checklist and reporting dashboard, together with the ERM implementation degree of formality assessment checklist and reporting dashboard would be included in the relevant risk committee's reporting pack or escalated to the relevant levels of management. The CRO will highlight areas of concern during the committee meetings. The suggested corrective actions and proposed target dates will be communicated to the relevant risk stakeholder and a status report will be expected at the next risk committee meeting.

### 5.3.5 Overview of the proposed enterprise risk management implementation assessment tool

Figure 5.11 illustrates the proposed ERM implementation assessment tools, feedback loops, process flow and the assigned responsibilities as it was discussed in Sections 5.3.1 to 5.3.4.

**Figure 5.11: An overview of the proposed ERM implementation assessment tool**



**Source:** Researcher's own compilation.

## 5.4 SUMMARY

Upon the completion of this review, a conceptual ERM implementation model was designed. This model consists of 7 building blocks, 24 level 1 best practice requirements, 154 level 2 best practice requirements, 67 purposes of deliverables and 165 proposed deliverables as identified in the literature review. The chapter concluded with an emphasis on a proposed ERM implementation assessment tool (consisting of a level of ERM implementation checklist, a level of ERM implementation reporting dashboard, an ERM implemented deliverables degree of formality assessment checklist; and an ERM implemented deliverables degree of formality assessment reporting dashboard) that will be used to determine and report on the status of ERM implementation within the organisation and the validated degree of formality achieved.

Chapter 6 will be dedicated to summarising the results pertaining to empirical objective 3 (Adjust the conceptualised ERM implementation model and the proposed ERM assessment tool based on the expertise of senior risk stakeholders within South African organisations). The chapter will commence with a description of the purpose of phase 2 of the empirical part of the study. Thereafter the data collection process will be described and the chapter will conclude with the results obtained with this phase.

## **CHAPTER 6: VALIDATED ENTERPRISE RISK MANAGEMENT IMPLEMENTATION MODEL AND CONFIRMED ENTERPRISE RISK MANAGEMENT IMPLEMENTATION ASSESSMENT TOOL**

### **6.1 INTRODUCTION**

The detail regarding the development of the conceptual ERM implementation model and the proposed ERM implementation assessment tool was discussed in Chapter 5.

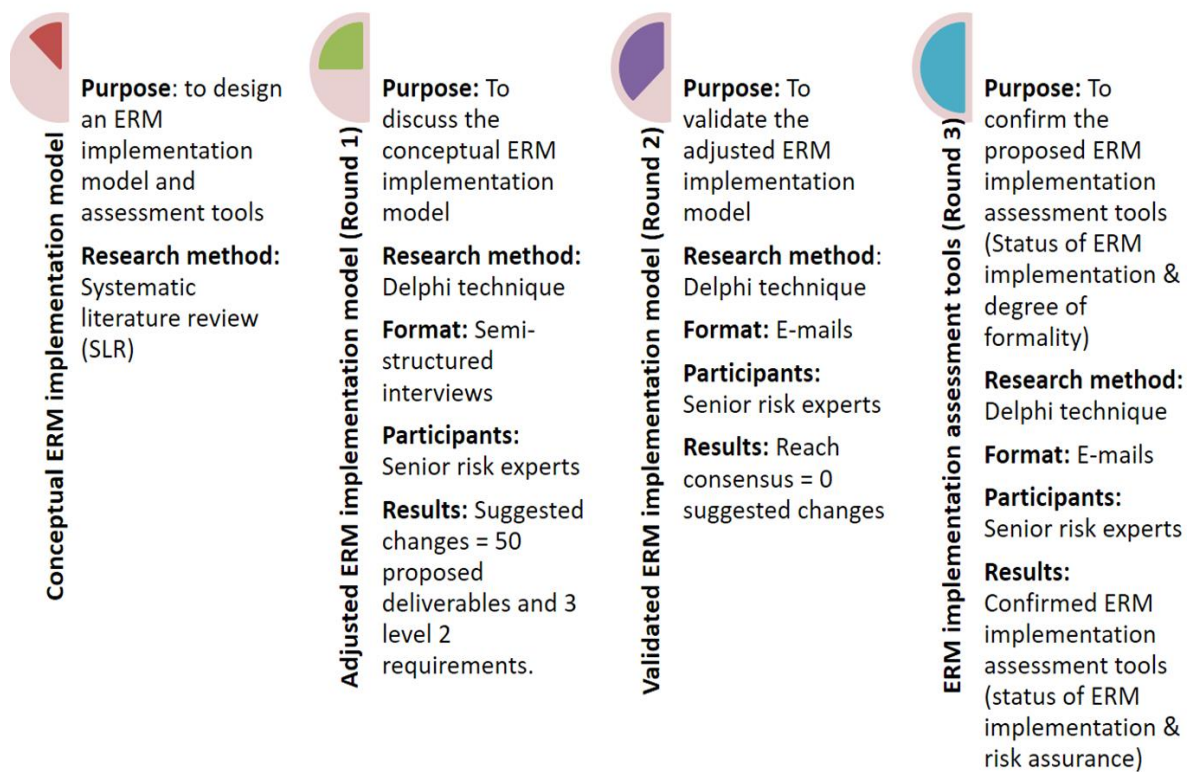
The main purpose of Chapter 6 is to report the findings pertaining to empirical objective 3 (Adjust the conceptualised ERM implementation model and the proposed ERM assessment tool based on the expertise of senior risk stakeholders within South African organisations). This chapter will start with a short description of the purpose of the phase, the data collection process followed and a summary of the results of the data analysis.

### **6.2 PHASE 2: VALIDATION OF THE CONCEPTUAL ERM IMPLEMENTATION MODEL AND PROPOSED ASSESSMENT TOOL**

#### **6.2.1 Purpose of this phase**

The purpose of phase 2 of the empirical study was to validate the conceptual ERM implementation model (refer to Section 6.2.3.2) and to confirm the proposed ERM implementation assessment tool (refer to Section 6.2.3.3) with the selected senior risk experts utilising the Delphi technique. Figure 6.1 gives an overview of the purpose of each round, the research method used, the participants, and a summary of the results obtained.

**Figure 6.1: Phase 2: Overview of round 1 to 3 of the Delphi technique**



**Source:** Researcher's own compilation.

### 6.2.2 Data collection

The senior risk experts, which participated in phase 2 of the empirical part of the study, were selected in accordance with the criteria as explained in Section 4.4.2.4.1 in Chapter 4. The detailed conceptual ERM implementation model (including the seven building blocks, best practise requirements, derived deliverables, and the purpose of each deliverable) and the proposed ERM implementation assessment tool were discussed and validated during:

- A first round of semi-structured interviews with senior risk experts within South African organisations;
- A second round of e-mail communication in which the researcher presented the adjusted ERM implementation model to the same senior risk experts for their affirmation; and
- A final round of e-mail communication to the same senior risk experts where they confirmed the proposed ERM implementation assessment tool.

## 6.2.3 Results

### 6.2.3.1 The participants' profile

Senior risk experts' opinions were sought for their ability to insightfully answer the research questions (Fink, 2016). The sample size for round 1 of the Delphi technique (consisting of face-to-face meetings using semi-structured interviews), round 2 and round 3 (e-mail communication) depended on the target population, which is the number of senior risk experts from different organisations within various industries within the South African risk management context. Most studies use panels of between 15 to 35 people (Gordon, 1994), though Dalkey (2005) suggests that seven as the minimum number would suffice. Nineteen senior risk experts were invited to partake in this research study of which eleven accepted the invitation, given the level of involvement in terms of time and attention. The entire panel of senior risk experts provided input and feedback during round 1 and round 2 of phase 2. Eight senior risk experts provided input for round 3 of the Delphi part of the study.

All of the non-probability purposively selected senior risk experts have been involved in the design, development and implementation of numerous ERM programs across several industries. They are involved at IRMSA (the Institute of Risk Management South Africa), either as executive committee members or subject matter experts, hold Chief Risk Officer or equivalent positions in their organisations (refer to Figure 6.2), are advisors on the King IV Code on Governance and ISO 31000 committees, and they have more than 7 years of risk management experience (refer to Figure 6.3). This is illustrated in Table 6.1.

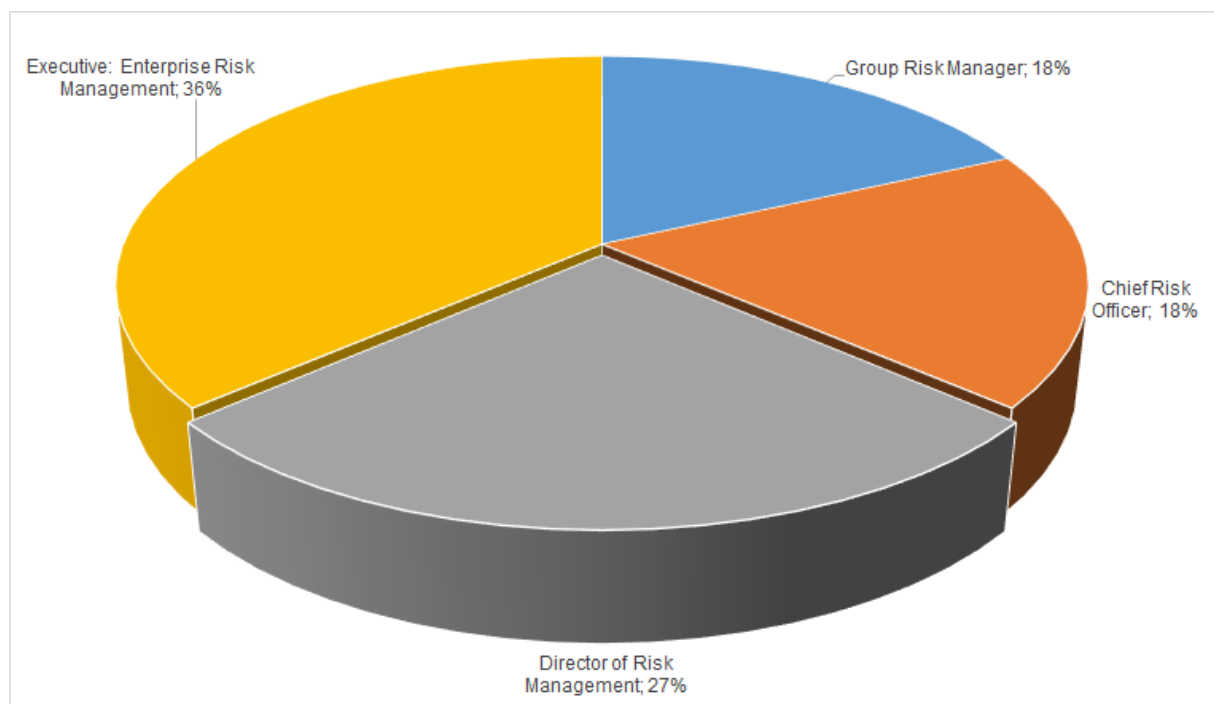
**Table 6.1: Phase 2: Proof of risk expertise**

| Participant code | Job title                 | Primary / secondary risk stakeholder | Risk experience (years) | Design, develop and implement ERM | Standard industrial classification                            |
|------------------|---------------------------|--------------------------------------|-------------------------|-----------------------------------|---------------------------------------------------------------|
| IV1              | Group Risk Manager        | Primary                              | 20 years                | Yes                               | Agriculture, forestry and fishing                             |
| IV2              | Director: Risk Management | Primary                              | 12 years                | Yes                               | Public administration and defence; compulsory social security |

| Participant code | Job title                                         | Primary / secondary risk stakeholder | Risk experience (years) | Design, develop and implement ERM | Standard industrial classification                            |
|------------------|---------------------------------------------------|--------------------------------------|-------------------------|-----------------------------------|---------------------------------------------------------------|
| IV4              | General Manager: Group Enterprise Risk Management | Primary                              | 14 years                | Yes                               | Transportation and storage                                    |
| IV7              | Director of Risk                                  | Primary                              | 30 years                | Yes                               | Accommodation and food service activities                     |
| IV8              | Group Risk Manager                                | Primary                              | 9 years                 | Yes                               | Mining and quarrying                                          |
| IV9              | Chief Risk Officer                                | Primary                              | 10 years                | Yes                               | Agriculture, forestry and fishing                             |
| IV13             | Group Chief Risk Officer                          | Primary                              | 8 years                 | Yes                               | Manufacturing                                                 |
| IV17             | General Manager: Enterprise-wide Risk Management  | Primary                              | 17 years                | Yes                               | Financial and insurance activities                            |
| IV18             | Director: Risk Management                         | Primary                              | 15 years                | Yes                               | Public administration and defence; compulsory social security |
| IV19             | Managing Executive                                | Primary                              | 14 years                | Yes                               | Information and Communication                                 |

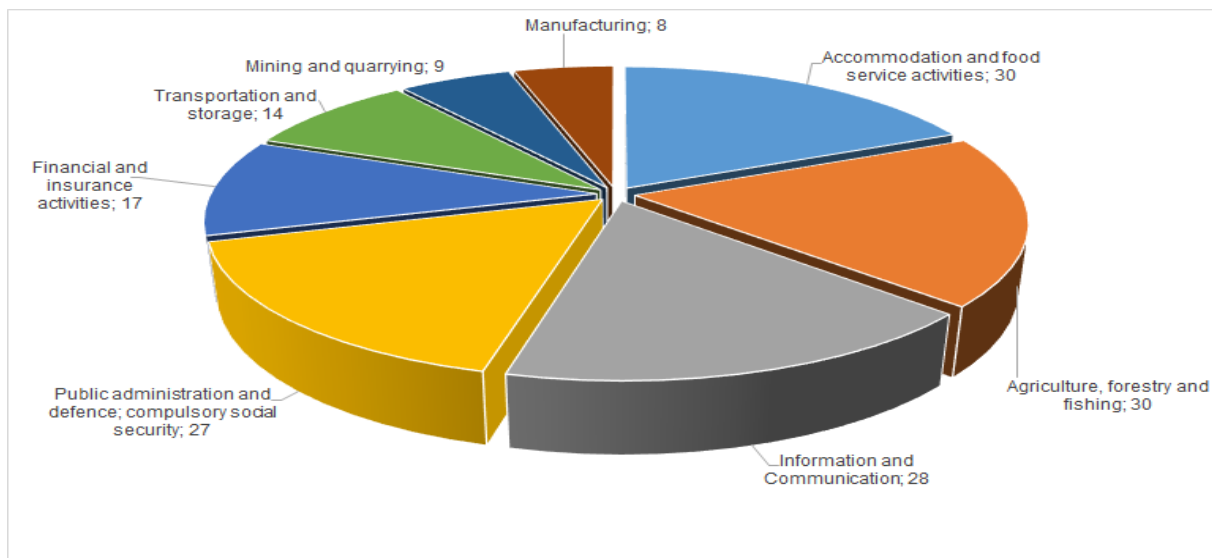
**Source:** Researcher's own compilation.

**Figure 6.2: Job titles**



**Source:** Researcher's own compilation.

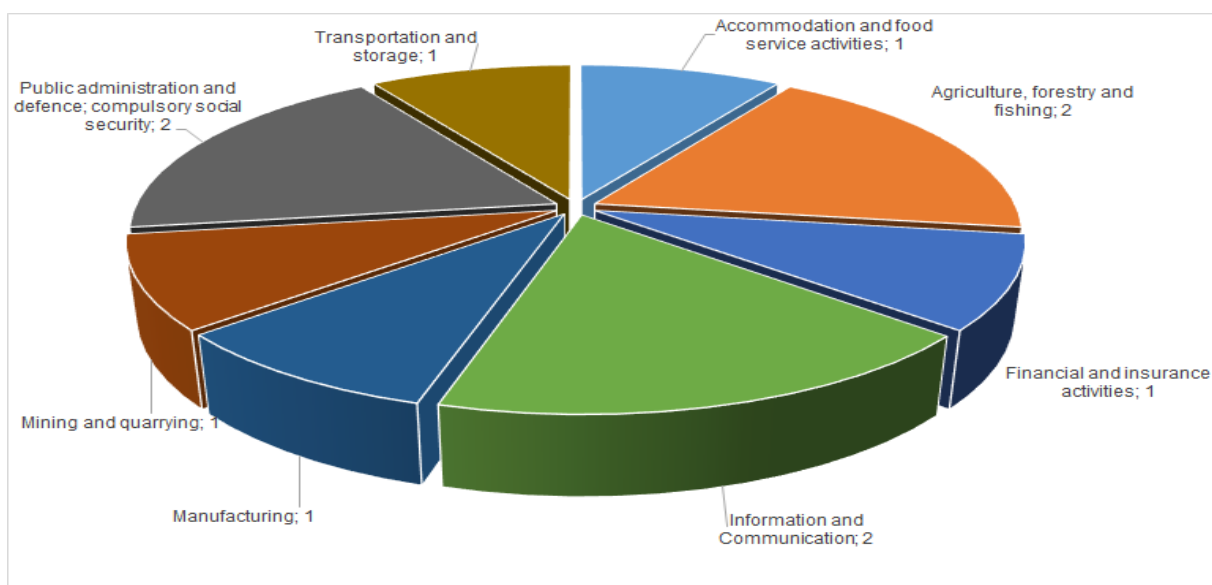
**Figure 6.3: Phase 2 participants: years of risk management experience per industry**



**Source:** Researcher's own compilation.

The senior risk experts represent 8 different industries in South Africa. The following sectors, agriculture, forestry and fishing sector; information and communication sector; public administration and defence; and compulsory social security, each have 2 participants. The manufacturing; mining and quarrying; financial and insurance activities; transportation and transport; and accommodation and food service activities sectors each have 1 participant (refer to Figure 6.4). Reliability of the results was ensured as there is an even spread between industries (Yousuf, 2007).

**Figure 6.4: Phase 2 participants—distribution per industry (number)**



**Source:** Researcher's own compilation.

### **6.2.3.2 Round 1 and round 2: From the conceptual to the validated enterprise risk management implementation model**

To summarise, the conceptual ERM implementation model consists of 7 building blocks, 24 level 1 best practice requirements, 154 level 2 best practice requirements, 67 purposes of deliverables and 165 proposed deliverables. The level 1 requirements consist of a list of the overarching requirements associated with each building block. In some instances, however, these level 1 requirements needed to be expounded with more detailed requirements that were selected to be included as level 2 requirements (Section 3.5.2). The level 1 and level 2 best practice requirements were based on the recommendations of ISO 31000: Risk management principles and guidelines (ISO, 2009b), ISO 31010: Risk management – Risk assessment techniques (ISO, 2009c), Guide 73: Risk management vocabulary (ISO, 2009a), and the King III Code on Governance (IODSA, 2009).

The proposed deliverables were derived from the aforementioned requirements (Section 3.5.2), based on the researcher's practical experience in different industries, professional bodies' risk management guidelines (IRM, 2002; IRMSA, 2014), professional bodies' practice notes (CIPS, 2014), standard setting organisations (ISO, 2009b, ISO, 2009c & IODSA, 2009), and suggestions by other authors (Garvey, 2008; Likhong, 2009; Chapman, 2011).

During the semi-structured interviews (round 1), the primary objectives of this research study, the problem statement, the theoretical frameworks that form the basis of the conceptual ERM implementation model, and the detail of the model were discussed with the senior risk experts. The aforementioned sessions were digitally recorded and these recordings were transcribed and entered into Microsoft Office Word 2016. The researcher received general feedback from the participants together with specific changes and additions to the detail of the conceptual ERM implementation model (level 1 and level 2 best practice requirements, purpose of deliverables and the deliverables). A change represents a variation on the proposed requirements, purpose of deliverables and deliverables in the conceptual ERM implementation model and an addition means additional requirements, purpose of deliverables and deliverables.

Table 6.2 reports the number of changes and additions per ERM implementation model building block.

**Table 6.2: Round 1 result: Number of changes and additions per building block**

| Building blocks    | Level 1 Requirements |           | Level 2 Requirements |           | Purpose |           | Deliverables |           |
|--------------------|----------------------|-----------|----------------------|-----------|---------|-----------|--------------|-----------|
|                    | Changes              | Additions | Changes              | Additions | Changes | Additions | Changes      | Additions |
| Building block I   | 3                    | 0         | 3                    | 3         | 0       | 0         | 4            | 1         |
| Building block II  | 0                    | 0         | 0                    | 0         | 0       | 0         | 7            | 0         |
| Building block III | 0                    | 0         | 0                    | 0         | 0       | -1        | 2            | 13        |
| Building block IV  | 0                    | 0         | 0                    | 0         | 0       | 0         | 8            | 12        |
| Building block V   | 0                    | 0         | 0                    | 0         | 0       | 0         | 3            | 15        |
| Building block VI  | 2                    | 0         | 2                    | 0         | 0       | 0         | 4            | 18        |
| Building block VII | 2                    | 0         | 2                    | 0         | 0       | 0         | 3            | 4         |
| All                | 7                    | 0         | 7                    | 3         | 0       | -1        | 31           | 63        |

**Source:** Researcher's own compilation.

Addendum H reflects the detail of the comments, changes, and additions made categorised per senior risk expert.

The next step was to modify the conceptual ERM implementation model with the comments, suggested changes and additions in order to arrive at the adjusted ERM implementation model. Addendum I shows the detail of the adjusted ERM implementation model for building blocks I to VII.

During round 2 of the Delphi part of the study the researcher presented the adjusted ERM implementation model via e-mail to the same senior risk experts for their final affirmation (refer to Addendum F). This resulted in the validated ERM implementation model with zero changes and additions suggested by the participants, effectively representing consensus. The green 0 block in Table 6.3 illustrates this. Addendum J contains the detailed results of round 2 per senior risk expert.

The detail of the round 1 (semi-structured interviews) and the round 2 (e-mail confirmation) changes and additions per building block will be discussed in the subsequent paragraphs.

### 6.2.3.2.1 Evolution from the conceptual enterprise risk management implementation model to the validated enterprise risk management implementation model

**Table 6.3: Number of changes for round 1 and round 2 of Delphi**

|                                | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|--------------------------------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|                                |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*                           | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1**                      | Adjusted ERM implementation model   | 7                          | 7               | 0                     | 31                   |
| Round 2**                      | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
| * Systematic literature review |                                     | Consensus                  |                 |                       |                      |
| ** Delphi technique            |                                     |                            |                 |                       |                      |

**Source:** Researcher's own compilation.

**Table 6.4: Number of additions for round 1 and round 2 of Delphi**

|                                | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|--------------------------------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|                                |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*                           | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1**                      | Adjusted ERM implementation model   | 0                          | 3                 | 0                     | 63                     |
| Round 2**                      | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
| * Systematic literature review |                                     | Consensus                  |                   |                       |                        |
| ** Delphi technique            |                                     |                            |                   |                       |                        |

**Source:** Researcher's own compilation.

The panel of senior risk experts suggested 31 changes (refer to Table 6.3) and 63 additions (refer to Table 6.4) to the conceptual requirements, purpose to deliverables and deliverables. The detail regarding the changes and new additions *per building block* will be discussed in the following paragraphs.

### 6.2.3.2.2 Building block I: Evolution from the conceptual to the validated

**Table 6.5: Building block I: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 3                          | 3               | 0                     | 4                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

**Table 6.6: Building block I: Number of additions for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|-----------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|           |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*      | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1** | Adjusted ERM implementation model   | 0                          | 3                 | 0                     | 1                      |
| Round 2** | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
|           |                                     | Consensus                  |                   |                       |                        |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

The semi-structured interviews of round 1 resulted in 10 suggested changes (refer to Table 6.5) and 4 additions (refer to Table 6.6) to the level 1 and level 2 best practise requirements and the proposed deliverables of building block I.

Several of the senior risk experts suggested that the purpose of this building block is two-fold: (1) to capture the instruction/trigger that resulted in the design, development and implementation of an ERM program and also to (2) describe the mandate from the board/decision-making body to senior management to create the aforementioned ERM program. This lead to a change in the name of the building block from “get permission” to “formalise the instruction and get permission”.

Another key contribution by the senior risk experts was that the design, development and implementation of an ERM program can be triggered by either legal and regulatory requirements (i.e. compliance mind-set) or by business requirements and conditions (i.e. value-adding mind-set) such as a due diligence associated with a merger and acquisition.

Several changes were made to the level 1 and level 2 requirements and the proposed deliverables in response to the suggestions in this regard: (1) Instruction/Trigger was added as a level 1 requirement with (2) the associated level 2 requirements being a business trigger/event and a legal and regulatory compliance incentive; and (3) a business case document was added to the proposed deliverables.

Thereafter, permission/mandate was added as a second level 1 requirement. The level 1 requirement in the conceptual ERM implementation model was moved to the level 2 requirement for permission/mandate. The next suggestion was to change the committee names in the proposed deliverables for permission/mandate to decision making bodies in order to cater for different types of organisations in different industries.

The last suggestion was to add oversight to the level 1 requirement in the conceptual ERM implementation model and to add the audit committee and different combinations of audit and risk committees to the proposed deliverables.

The adjusted ERM implementation model reflects all the suggested changes from round 1 of the Delphi part of the study and the validated ERM implementation model reflects that consensus was reached.

#### 6.2.3.2.3 Building block II: Evolution from the conceptual to the validated

**Table 6.7: Building block II: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0               | 0                     | 7                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

**Table 6.8: Building block II: Changes for round 1 and round 2 of Delphi**

| Level 2 requirements                                                                            | Deliverables                                                                                                                          |                                                                                                                                                                                                                                         | Changes / additions suggested by: |     |     |     |     |     |     |      |      |      |      |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|-----|-----|-----|-----|-----|-----|------|------|------|------|
|                                                                                                 | Conceptual                                                                                                                            | Adjusted                                                                                                                                                                                                                                | IV1                               | IV2 | IV4 | IV6 | IV7 | IV8 | IV9 | IV13 | IV17 | IV18 | IV19 |
| (a) Ensure that the organisation's culture and risk management policies are aligned.            | Risk management policy                                                                                                                | Risk management policy / Risk requirements evident in business, project and HR requirements and standards / Strategic intent document / Risk communication strategy / Internal audit reports / External audit report / Insurance claims |                                   |     |     | X   | X   |     | X   |      | X    |      |      |
| (c) Align risk management objectives with the objectives and strategies of the organisation.    | Risk appetite & risk tolerance                                                                                                        | Strategic plan / Business plan / Risk plan / Risk management objectives / Risk appetite statement / Risk tolerance levels                                                                                                               |                                   |     | X   |     |     |     | X   |      | X    | X    |      |
| (d) Assign accountabilities and responsibilities at appropriate levels within the organisation. | Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines.) | Risk governance model: (incl. risk owners' matrix, roles & responsibilities, reporting & escalation process & incentives guidelines & individual performance scorecard.)                                                                |                                   |     |     |     |     |     |     |      | X    |      |      |
| (e) Ensure that the necessary resources are allocated to risk management.                       | Risk management plan (People, Processes and Budget)                                                                                   | Risk management plan (People, Processes and Budget) / Annual performance plan / Operational budget                                                                                                                                      |                                   | X   |     |     | X   |     |     |      |      |      |      |
| (f) Communicate the benefits of risk management to all stakeholders.                            | Benefits of risk management                                                                                                           | Risk training material / Business case / Risk management policy / Embedded in risk reports / Board risk report                                                                                                                          |                                   |     |     |     | X   |     |     | X    | X    | X    |      |
|                                                                                                 | Risk maturity model                                                                                                                   | Risk maturity assessment                                                                                                                                                                                                                |                                   |     | X   |     | X   |     |     |      |      |      |      |
|                                                                                                 | Risk awareness plan                                                                                                                   | Risk awareness strategy & plan                                                                                                                                                                                                          | X                                 | X   |     |     |     |     |     |      |      |      |      |

**Source:** Researcher's own compilation.

Building block II addresses the best practice requirements and proposed deliverables in respect of establishing the tone of the organisation. Table 6.7 communicates that 7 changes to the deliverables were suggested by the senior risk experts. The nature of these changes are discussed in Table 6.8 by focussing on the level 2 requirements and the proposed deliverables from the conceptual model, the adjusted deliverables from the round 1 semi-structured interviews, and providing detail as to the origin of the change. The additions to the deliverables create the required flexibility in the model that will suit the needs of different types of organisations.

**Table 6.9: Building block II: Number of additions for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|-----------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|           |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*      | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0                 | 0                     | 0                      |
| Round 2** | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
|           |                                     | Consensus                  |                   |                       |                        |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

Table 6.9 reflects that there were zero additions suggested by the senior risk experts during the round 1 semi-structured interviews.

#### 6.2.3.2.4 Building block III: Evolution from the conceptual to the validated

**Table 6.10: Building block III: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0               | 0                     | 2                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

**Table 6.11: Building block III: Number of additions for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|-----------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|           |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*      | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0                 | -1                    | 13                     |
| Round 2** | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
|           |                                     | Consensus                  |                   |                       |                        |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

Building block III covers the rules of the game as it pertains to the design and development of the risk management framework and the risk management process. The senior risk experts made numerous suggestions regarding additional deliverables for the “establish the internal context of the organisation” level 2 requirement. The additional deliverables are internal audit reports, external audit reports, strategic plan, and business plans.

They also added seven deliverables to the level 2 requirement, stating: “Risk management should be embedded in all the organisation's practices and processes in a way that it is relevant, effective and efficient”. They are: new product development process, operational processes, investment decisions process, combined assurance process, performance management process, change management process, and quality assurance process.

Another key suggestion was made that “to align risk management objectives with the objectives and strategies of the organisation”, does not necessarily culminate into the risk appetite statement and risk tolerance levels, but in some organisations it would be explicit in the strategic plan of the organisation and the business plans of the divisions/departments/business units. The proposed deliverables were adjusted accordingly.

The integrated report: opportunities and risk section deliverable was moved from the external reporting level 2 requirement to building block VI. This accounts for the -1 number of changes in the purposes as it reported in Table 6.11. The changes and additions, reflected in the adjusted ERM implementation model, were accepted by the senior risk experts and consensus was reached for building block 3. This is reported as such in the validated ERM implementation model (refer to Figure 6.5).

#### 6.2.3.2.5 Building block IV: Evolution from the conceptual to the validated

**Table 6.12: Building block IV: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0               | 0                     | 8                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

**Table 6.13: Building block IV: Number of additions for round 1 and round 2 of Delphi**

|                                | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|--------------------------------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|                                |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*                           | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1**                      | Adjusted ERM implementation model   | 0                          | 0                 | 0                     | 12                     |
| Round 2**                      | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
| * Systematic literature review |                                     | Consensus                  |                   |                       |                        |
| ** Delphi technique            |                                     |                            |                   |                       |                        |

**Source:** Researcher's own compilation.

Building block IV deals with designing the risk management infrastructure, i.e. people, committees, models and tools, templates, processes, and systems. The senior risk experts suggested 8 changes (refer to Table 6.12) and 12 additions (refer to Table 6.13) to the conceptual deliverables during round 1 of the Delphi part of the study. One of the key suggestions was to align the model's language to practise-based terminology. This was applied to the people element of the building block insofar as risk competency model was replaced with job profiles as risk practitioners are more familiar with that term.

The 'committees' element was expanded to include an audit and risk committee charter, a combined assurance committee terms of reference, and a risk-specific committee terms of reference. It was highlighted that a charter is developed for a committee that is required by law, e.g. the audit committee and that a terms of reference is developed for other committees, e.g. board risk committee. The appropriated changes were affected in the adjusted ERM implementation model.

A suggestion was made to change models to risk quantification models in order to reduce confusion amongst risk practitioners as to the meaning thereof. The conceptual ERM implementation model was expanded with numerous additions to the templates element. The detail for the processes element was also added to the conceptual model in accordance with the suggestions made by the participants.

### 6.2.3.2.6 Building block V: Evolution from the conceptual to the validated

**Table 6.14: Building block V: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0               | 0                     | 3                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

**Table 6.15: Building block V: Number of additions for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|-----------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|           |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*      | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0                 | 0                     | 15                     |
| Round 2** | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
|           |                                     | Consensus                  |                   |                       |                        |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

The best practice requirements and proposed deliverables for the implementation phase of the ERM program are captured in building block V. The level 1 requirements are split into the risk management framework and the risk management process. The senior risk experts proposed 3 changes (refer to Table 6.14) and 15 additions (refer to Table 6.15) to the proposed deliverables in the conceptual ERM implementation model. The proposed deliverables for the level 2 requirement that states: "Apply the risk management policy and process to the organisational processes", accounts for 10 of the suggested additions as it involved an expansion of the list of processes that should include risk management as a step.

The other 5 additions are included as follows: (1) Level 2 requirement that states “Ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes”. Add strategic plan and ERM framework and policy as proposed deliverables; (2) Level 2 requirement that states “Step 3: Risk identification”. Add risk library as a proposed deliverable; (3) Level 2 requirement that states “Step 4: Risk analysis”. Add root cause analysis as a proposed deliverable.

The suggested changes included, for example, rewording a list of risk controls to controls library and other similar changes.

The adjusted ERM implementation model reflected the changes and additions. It was validated during round 2 of the Delphi part of the study and consensus was reached for this building block.

#### 6.2.3.2.7 Building block VI: Evolution from the conceptual to the validated

**Table 6.16: Building block VI: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0               | 0                     | 4                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher’s own compilation.

**Table 6.17: Building block VI: Number of additions for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|-----------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|           |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*      | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0                 | 0                     | 18                     |
| Round 2** | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
|           |                                     | Consensus                  |                   |                       |                        |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher’s own compilation.

Building block VI prescribes the requirements and proposed deliverables relating to monitoring and review activities pertaining to the risk management framework and the risk management process. The semi-structured interviews produced 4 changes (refer to Table 6.16) and 18 additions (refer to Table 6.17) to the conceptual ERM implementation model. The level 1 requirements consist of 3 sections: (1) Monitoring and review activities by the board; (2) Monitor and review the risk management framework; and (3) Monitor and review the risk management process. Table 6.18 describes the detail regarding the additional deliverables that were suggested by the senior risk experts during round 1.

**Table 6.18: Building block VI: Additions for round 1 of Delphi**

| Level 1 requirements                  | Level 2 requirements                                                                                                                                      | Deliverables                                  | Additions suggested by: |     |     |     |     |     |     |      |      |      |      |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|-------------------------|-----|-----|-----|-----|-----|-----|------|------|------|------|
| Adjusted                              | Adjusted                                                                                                                                                  | Adjusted                                      | IV1                     | IV2 | IV4 | IV6 | IV7 | IV8 | IV9 | IV13 | IV17 | IV18 | IV19 |
| Review activities by the Board        | The board should comment in the integrated report on the effectiveness of the system and process of risk management.                                      | Annual board risk report                      |                         | x   |     |     | x   |     |     |      | x    |      |      |
|                                       | The board should review the implementation of the risk management plan at least once a year.                                                              | Internal audit report                         | x                       |     |     |     |     |     |     |      |      |      | x    |
| Monitor the risk management framework | Report on risk, progress with the risk management plan and how well the risk management policy is being followed;                                         | Deviations from risk management policy report |                         |     |     |     | x   |     |     |      |      |      | x    |
| Review the risk management framework  | Periodically review whether the risk management framework, policy and plan are still appropriate, given the organisations' external and internal context; | Internal audit report                         |                         |     |     |     |     |     |     |      |      | x    |      |
|                                       |                                                                                                                                                           | Risk calendar                                 |                         |     |     |     |     |     |     |      | x    |      |      |
|                                       | Communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.                                               | Subject matter expert gap analysis            |                         |     |     |     | x   |     |     |      |      |      |      |
|                                       |                                                                                                                                                           | Internal audit reports                        |                         |     |     |     | x   |     |     |      |      |      |      |
|                                       |                                                                                                                                                           | Risk calendar                                 |                         |     |     |     |     |     |     |      | x    |      |      |
|                                       |                                                                                                                                                           | ISO 9000 reports                              |                         |     |     |     |     |     |     |      |      |      | x    |

| Level 1 requirements                | Level 2 requirements                                                                                         | Deliverables                       | Additions suggested by: |     |     |     |     |     |     |      |      |      |      |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------|-----|-----|-----|-----|-----|-----|------|------|------|------|
| Adjusted                            | Adjusted                                                                                                     | Adjusted                           | IV1                     | IV2 | IV4 | IV6 | IV7 | IV8 | IV9 | IV13 | IV17 | IV18 | IV19 |
| Monitor the risk management process | Ensuring that controls are effective and efficient in both design and operation.                             | Subject matter expert gap analysis |                         |     |     |     |     | x   |     |      | x    |      |      |
|                                     |                                                                                                              | Combined assurance reports         |                         | x   |     |     |     |     |     |      |      |      |      |
|                                     |                                                                                                              | Risk profile status reports        | x                       |     |     |     |     |     |     |      |      |      |      |
|                                     |                                                                                                              | Internal audit reports             |                         |     |     |     |     |     |     |      | x    | x    | x    |
|                                     |                                                                                                              | External audit reports             |                         |     |     |     |     |     |     |      | x    |      |      |
| Review the risk management process  | Analysing and learning lessons from events (including near-misses), changes, trends, successes and failures; | Post mortem sessions               | x                       |     |     |     |     |     |     |      |      |      |      |
|                                     |                                                                                                              | Environmental scanning             |                         |     | x   |     |     |     |     |      |      |      |      |
|                                     |                                                                                                              | Risk reconciliation reports        |                         |     |     |     | x   |     |     |      |      |      |      |
|                                     |                                                                                                              | Post loss analysis                 |                         |     |     |     | x   |     |     |      |      |      |      |

**Source:** Researcher's own compilation.

#### 6.2.3.2.8 Building block VII: Evolution from the conceptual to the validated

**Table 6.19: Building block VII: Number of changes for round 1 and round 2 of Delphi**

|           | Models                              | Best practice requirements |                 | Proposed deliverables |                      |
|-----------|-------------------------------------|----------------------------|-----------------|-----------------------|----------------------|
|           |                                     | Level 1 changes            | Level 2 changes | Purpose changes       | Deliverables changes |
| SLR*      | Conceptual ERM implementation model |                            |                 |                       |                      |
| Round 1** | Adjusted ERM implementation model   | 0                          | 0               | 0                     | 3                    |
| Round 2** | Validated ERM implementation model  | 0                          | 0               | 0                     | 0                    |
|           |                                     | Consensus                  |                 |                       |                      |

\* Systematic literature review

\*\* Delphi technique

**Source:** Researcher's own compilation.

**Table 6.20: Building block VII: Number of additions for round 1 and round 2 of Delphi**

|                                | Models                              | Best practice requirements |                   | Proposed deliverables |                        |
|--------------------------------|-------------------------------------|----------------------------|-------------------|-----------------------|------------------------|
|                                |                                     | Level 1 additions          | Level 2 additions | Purpose additions     | Deliverables additions |
| SLR*                           | Conceptual ERM implementation model |                            |                   |                       |                        |
| Round 1**                      | Adjusted ERM implementation model   | 0                          | 0                 | 0                     | 4                      |
| Round 2**                      | Validated ERM implementation model  | 0                          | 0                 | 0                     | 0                      |
| * Systematic literature review |                                     | Consensus                  |                   |                       |                        |

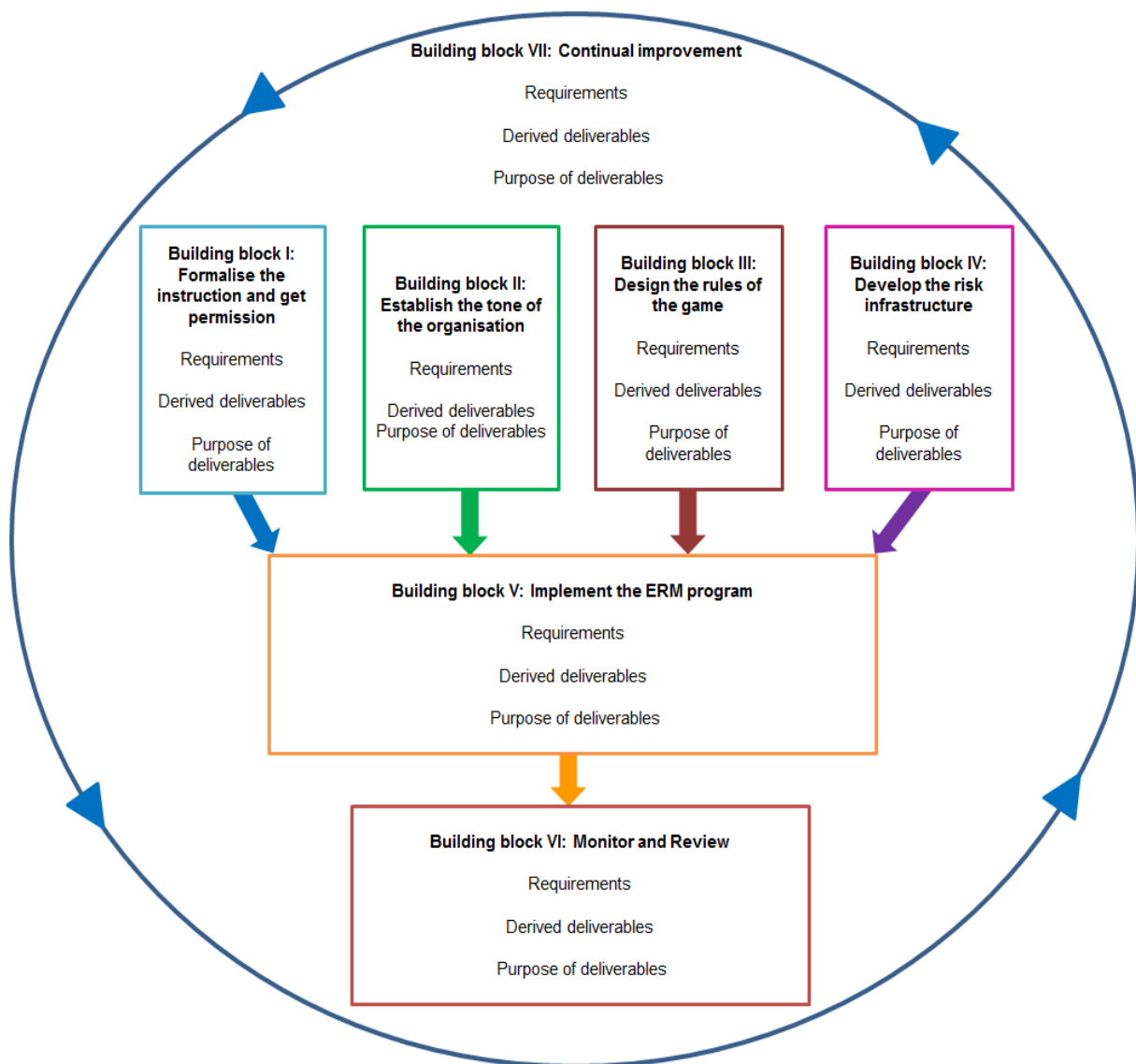
\*\* Delphi technique

**Source:** Researcher's own compilation.

Building block VII describes the requirements and proposed deliverables relating to the continual improvement phase of the ERM program. The senior risk experts suggested 3 changes (refer to Table 6.19) and 4 additions (refer to Table 6.20) to the proposed deliverables. The conceptual ERM implementation model was adjusted accordingly and the adjusted ERM validation model was validated during round 2 of the Delphi part of the study. Consensus was reached after round 2.

In summary, round 1 and 2 of the Delphi part of the study resulted in a validated ERM implementation model (refer to Figure 6.5) where all the senior risk experts reached consensus with regards to the building block names, the best practice requirements (level 1 and level 2), and the proposed deliverables (purpose and deliverables). Refer to Addendum K for the validated ERM implementation model (building blocks, requirements, and proposed deliverables). The validated model was used as the basis for the ERM implementation assessment tool.

**Figure 6.5: Validated ERM implementation model**



**Source:** Researcher's own compilation.

### 6.2.3.3 Round 3: from the proposed to the confirmed enterprise risk management implementation assessment tool and reporting dashboards

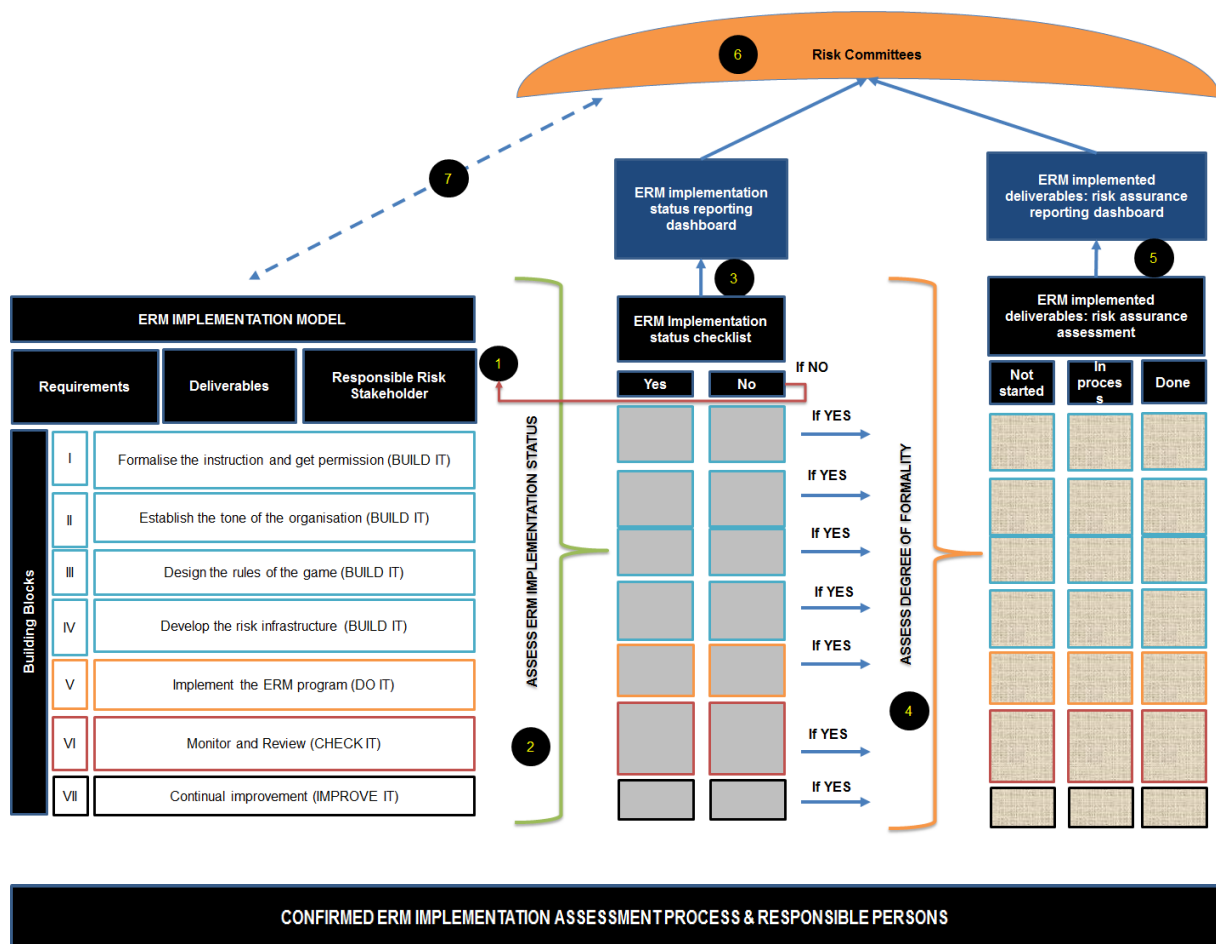
The main objective of round 3 of the Delphi part of the study was to confirm the proposed ERM implementation assessment tools in terms of the process flows and the assigned responsibilities (refer to Figure 5.11). An e-mail communication was sent to the same senior risk experts that were involved in round 1 and 2. The majority of the participants (73%) responded to the request for input.

Addendum L reflects that 88% of the participants that responded, agreed in principle with the proposed process flow and assigned responsibilities.

The feedback received, resulted in the following changes as it is illustrated in Figure 6.6:

- Degree of formality: change the name to risk assurance as the term is an embedded part of the risk governance models (refer to Table 3.6) and it is known to risk practitioners.
- Step 4: add a feedback loop back to the risk stakeholder if the answer is no.

**Figure 6.6: Confirm ERM implementation assessment tool**



**Source:** Researcher's own compilation.

### **6.3 SUMMARY**

Chapter 6 contained the results from phase 2 of the empirical part of this study. The purpose of phase 2 was to validate the conceptual ERM implementation model (refer to Section 6.2.3.2) and to confirm the proposed ERM implementation assessment tool (refer to Section 6.2.3.3) with the selected senior risk experts utilising round 1 to 3 of the Delphi technique.

Chapter 7 will be dedicated to summarising the study, describing the conclusions and limitations of the study and also give recommendations for further research.

## CHAPTER 7: SUMMARY, CONCLUSIONS, LIMITATIONS, CONTRIBUTIONS AND RECOMMENDATIONS

### 7.1 INTRODUCTION

The primary objective of this research study was to assist in the translation of an overarching, strategic ERM approach into a validated practice-based ERM framework with specific tools (an ERM implementation model and assessment tools) to enable risk stakeholders within any organisation and across industries, to sufficiently embed the ERM program, to assess the status of ERM implementation, and to provide independent assurance regarding the status of ERM implementation.

Chapter 7 concludes this study by explaining how this objective was met by summarising the information gathered through the systematic literature review and empirical study; and establishing what inferences can be made from it. The limitations of the study will then be explained; after which recommendations will be made regarding further research opportunities.

### 7.2 SUMMARY AND CONCLUSIONS FROM THE SYSTEMATIC LITERATURE REVIEW

In this section, the systematic literature review (SLR) will be summarised and the conclusions drawn highlighted in accordance with the various theoretical objectives of the research study.

#### 7.2.1 Scope and definition of enterprise risk management

The **first** theoretical objective of the research study was to Describe the ERM domain in terms of the scope and definition of ERM, ERM adoption drivers, and the perceived value proposition of ERM implementation. This was achieved in Chapter 2 of this research study. The following sections contain a summary of the results applied to each element of the ERM domain and, in some instances, the researcher motivates the selection from the researcher's point of view.

- **Scope and definition of ERM:** A one-size-fits-all approach is not applicable to ERM as each organisation will employ such programs and tools in a manner that accommodates differences in mission, vision, corporate governance, strategic direction, and culture. However, core components will be consistent and relevant to any organisation. Recognising this at the outset will encourage the risk management professional to define and modify basic structural elements in the ERM implementation program to fit their specific organisational needs, particularly as they relate to unique delivery settings.

To clearly define the **scope** of the ERM program and obtain agreement from the key stakeholders is imperative to the successful design, development and implementation of the ERM program. After due consideration of the available **ERM definitions** (n = 26) found in current literature (refer to Section 2.2), the researcher supported Mikes and Kaplan's practice-based ERM definition developed in 2013 as the most appropriate definition for this research study. It states: "**Enterprise risk management** consists of a framework of active and intrusive methods and processes that (1) are capable of challenging existing assumptions about the world within and outside the organisation; (2) communicate risk information with the use of distinct tools (such as risk maps, stress tests, and scenarios); (3) collectively address gaps in the control of risks that other control functions (such as internal audit and other boundary controls) leave unaddressed; and, in doing so, (4) complement—but do not displace—existing management control practices". To reiterate, the primary objective of this study was the development of an ERM implementation model and assessment tool. Admittedly, it was never the intention of the study to develop a new ERM definition. As such, the researcher evaluated the 26 ERM definitions that were identified with the SLR in terms of whether it is clear, concise and understandable. The researcher emphasises the principle that without an articulated definition which the organisation can embrace, the activities associated with ERM development, implementation and assessment can become disjointed and without purpose. The researcher deemed the aforementioned ERM definition the most appropriate because it is a logical, practical and an all-encompassing representation of ERM in terms of people, processes and structure.

- The SLR highlighted that the **drivers** for the **adoption of an ERM** program are: (1) the size of the organisation; (2) the regulatory compliance requirements; (3) certain internal organisational motivators such as increasing shareholder wealth and ownership structure of the organisation; (4) a broader scope of risks resulting from the changing business environment; (5) the presence of a chief risk officer (CRO); and (6) the increase in operational benefits from a formalised ERM program (refer to Section 2.3). The researcher's extensive practical experience in 7 industries supports the aforementioned drivers for the adoption of an ERM program. It can be deduced from the literature and the researcher's practical experience that highly regulated industries such as the financial industry are more prone to design, develop and implement formalised ERM programs and also to appoint a CRO as the ERM program champion. In less regulated industries, the tendency is to implement parts of ERM programs and the main objective is to improve the bottom line in terms of cost savings, profit enhancing and resource allocation.

- According to the results of surveys done by the North Carolina University in 2010 on the state of ERM oversight; as well as the Risk & Insurance Management Society (RIMS) in 2013 on ERM, the **perceived value added** (refer to Section 2.4) by an ERM program could be to: (1) increase risk awareness; (2) align risk appetite and strategy; (3) avoid and/or mitigate risks; (4) enhance risk based decisions; (5) reduce operational surprises and losses; (6) eliminate silos, such as identifying and managing risks across the enterprise; and (7) improve resource allocation. The researcher is of the opinion that a formalised and straightforward ERM program will result in (1) improved risk awareness due to an improved level of understanding; (2) ERM program adoption across all the levels of management, departments and subsidiaries due to the simplicity of the ERM program; (3) enhanced risk based decisions due to clear value added by ERM and, (4) an improvement in the allocation of scarce risk resources due to clear deliverables, timelines and value added.

### 7.2.2 Barriers to enterprise risk management implementation

The **second** theoretical objective – to identify and document the barriers to ERM implementation – was achieved in Section 2.5 of this study. The relevant section contained an account of the barriers from academic literature and risk practitioner reports. The summary is:

- Lack of board or C-level or senior executive leadership;
- Difficult to identify risk owners for particular risks and responses;
- Role confusion: lack of clarity with regards to risk roles and responsibilities in the organisation;
- Insufficient resources (i.e. people, technology, budget) to manage risks;
- Lack of perceived value added by the enterprise risk management program;
- Badly designed ERM program, namely:
  - Misalignment between the ERM program design and the design of the organisation.
  - A common view from management is that risk is intuitively managed, and therefore there is no need to deploy a formal approach.
  - Ignoring existing risk management activities.
  - Inadequate information to make risk-based decisions.
- Incentives do not reward making risk-based decisions;
- Risk management criteria is not standardised throughout the organisation;
- Competing priorities between the risk owner's operational (day-to-day) and risk responsibilities; and
- Little or no monitoring regarding risk management plan execution.

This discussion can be concluded by referring to the outline depicted in Figure 2.1 (Thematic representation of the barriers to ERM implementation). The barriers were organised according to the following themes: 1) risk culture; 2) risk assessment; 3) risk governance; 4) risk integration; 5) ERM program design; 6) risk criteria; 7) risk infrastructure (People, Process, System, Time, Budget); 8) risk measurement; 9) ERM program value added; 10) monitoring and review; 11) performance management system; 12) risk management framework; 13) risk reporting; 14) risk treatment; and 15) risk communication.

### **7.2.3 Conclusions for theoretical objectives 1 and 2**

It is clear from the contents of the SLR within chapter 2 that, in order for organisations to realise the proposed value added through the successful deployment of ERM implementation and assessment within any organisation, operating within any industry, that there are certain homogenous requirements that have to be met:

- Clarifying and agreeing on the scope of an ERM program is imperative to the successful design, development and implementation of the ERM program;
- Agreeing on a clear, concise and understandable ERM definition should be the starting block for developing an ERM implementation program and assessment tool prior to embedding such a program within any organisation in any industry to ensure that all aspects associated with ERM development, implementation and assessment does not become disjointed and without purpose;
- Clarifying organisation specific adoption drivers influencing the degree of formality with which the ERM implementation program and assessment tool needs to be adopted within any organisation (such as the size of the organisation, the type of industry, changes in the regulatory environment, internal organisational factors, ownership structure, the training of the risk managers, the appointment of a chief risk officer (CRO), and a broader scope of risks and operational benefits;
- A carefully designed ERM implementation model should then be planned, based on the design of the organisation, identifying risks and exploiting opportunities based on adequate information to make risk-based decisions;
- With incentives in place to reward the stakeholders making risk-based decisions weighing up competing priorities between the risk owner's operational and risk responsibilities;
- Monitoring and assessing the ERM implementation program through an appropriately designed assessment tool;
- Top management support, including the appointment of specific risk owners with a clearly defined outline of their roles and responsibilities within the organisation;

- The potential for value being added to the organisation by implementing an ERM program should be clearly outlined and understood; and
- Sufficient resources (such as people, technology and budget) should be allocated to the risk initiative.

#### **7.2.4 The conceptual enterprise risk management implementation model and proposed assessment tool**

The **third** theoretical objective was to explore the use of different organisational design models and continual improvement models (such as the Deming cycle) as the theoretical framework for the conceptual ERM implementation model. This objective was an intentional effort by the researcher to address the misalignment between the principles of organisational design and ERM program design that were identified as an area of concern (refer to Chapter 3) by several other researchers in the fields of accounting, management and risk management.

In response, the researcher evaluated 14 organisational design models in order to identify the model best suited to determine and support the specific building blocks on which the conceptual ERM implementation model was built. The Weisbord Six-box organisational design model was chosen as it contained all of the components necessary to form the basis for the conceptual ERM implementation model. The underlying premise was that it should reduce the misalignment between organisational design principles and ERM program design. The role of continual improvement in the successful implementation of an ERM program was recognised and the Deming cycle (plan-do-check-adjust) was applied to the ERM implementation model.

The **fourth** theoretical objective was to develop the conceptual ERM implementation model. The researcher based the conceptual ERM implementation model on Weisbord's Six-box organisational design model (box 1: purpose; box 2: structure; box 3: relationships; box 4: rewards; box 5: leadership, and box 6: helpful mechanisms), the Deming cycle (plan-do-check-adjust), the ISO 31000 risk management principles and guidelines (the international best practice standard), and the South African King III Code on Corporate Governance. Table 7.1 reflects the alignment between the theoretical frameworks and the conceptual ERM implementation model (the building blocks and the level 1 and 2 best practice requirements). It contains the Deming cycle phases and the Weisbord organisational design model boxes that are aligned with the conceptual ERM implementation model building blocks in the first three columns. The level 1 and level 2 best practice requirements refer to the source document and the specific paragraph in the source document.

**Table 7.1: Conceptual ERM implementation model—theoretical frameworks and best practice requirements**

| Theoretical frameworks |                                                         | Building blocks                             | Level 1 best practice requirements |             | Level 2 best practice requirements |                               |
|------------------------|---------------------------------------------------------|---------------------------------------------|------------------------------------|-------------|------------------------------------|-------------------------------|
| Deming cycle           | Weisbord organisational design model                    |                                             | Source                             | Ref.        | Source                             | Ref.                          |
| Plan                   | Purpose, Leadership                                     | I. Get permission.                          | ISO 31000                          | 4.2         |                                    |                               |
|                        |                                                         |                                             | King III                           | 4.4         |                                    |                               |
|                        |                                                         |                                             | King III                           | 4.3         | King III                           | 4.3.1                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.1                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.2                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.3                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.3.2.4                       |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.3                         |
|                        |                                                         |                                             | King III                           | 4.1.1       | King III                           | 4.1.5                         |
| Plan                   | Leadership, Relationships                               | II. Establish the tone of the organisation. |                                    |             |                                    | 4.1.6                         |
|                        |                                                         |                                             | ISO 31000                          | 4.2 & 4.3.2 |                                    | 4.1.7                         |
|                        |                                                         |                                             | ISO 31000                          | 4.2         | King III                           | 4.4.3                         |
| Plan                   | Purpose, Relationships, Structure, External environment | III. Design the rules of the game.          |                                    |             | ISO 31000                          | 4.2                           |
|                        |                                                         |                                             | King III                           | 4.1.4       |                                    |                               |
|                        |                                                         |                                             | ISO 31000                          | 4.3         | ISO 31000                          | 4.3.1 & 5.3.2                 |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.3.1 & 5.3.3                 |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.3.1 & 5.3.4                 |
|                        |                                                         |                                             |                                    |             | ISO 31000 / King III               | 4.3.1 & 5.3.5 / 4.2.1 & 4.2.2 |
|                        |                                                         |                                             |                                    |             | ISO 31000                          | 4.3.2                         |
|                        |                                                         |                                             |                                    |             | King III                           | 4.1.1                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.5                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.6                         |
|                        |                                                         |                                             |                                    |             |                                    | 4.1.7                         |

| Theoretical frameworks |                                                         | Building blocks                      | Level 1 best practice requirements |                       | Level 2 best practice requirements |              |
|------------------------|---------------------------------------------------------|--------------------------------------|------------------------------------|-----------------------|------------------------------------|--------------|
| Deming cycle           | Weisbord organisational design model                    |                                      | Source                             | Ref.                  | Source                             | Ref.         |
| Plan                   | Purpose, Relationships, Structure, External environment | III. Design the rules of the game.   | ISO 31000                          | 4.3                   | ISO 31000                          | 4.3.3        |
|                        |                                                         |                                      |                                    |                       | King III                           | 4.4.2        |
|                        |                                                         |                                      |                                    |                       | ISO 31000                          | 4.3.4        |
|                        |                                                         |                                      |                                    |                       | ISO 31000                          | 4.2          |
|                        |                                                         |                                      |                                    |                       | ISO 31000                          | 4.3.6        |
|                        |                                                         |                                      |                                    |                       | ISO 31000 / King III               | 4.3.7 / 4.10 |
|                        |                                                         |                                      | ISO 31000                          | 5                     | ISO 31000                          | 5.2          |
|                        |                                                         |                                      |                                    |                       |                                    | 4.3.1 & 5.3  |
|                        |                                                         |                                      |                                    |                       |                                    | 5.4.2        |
|                        |                                                         |                                      |                                    |                       |                                    | 5.4.3        |
|                        |                                                         |                                      |                                    |                       |                                    | 5.4.4        |
|                        |                                                         |                                      |                                    |                       |                                    | 5.5          |
|                        |                                                         |                                      |                                    |                       |                                    | 5.6          |
|                        |                                                         |                                      |                                    |                       |                                    | 4.6          |
| Plan                   | Helping mechanisms, Relationships, Rewards              | IV. Develop the risk infrastructure. | ISO 31000                          | 4.3.5                 | ISO 31000                          | 4.3.5        |
|                        |                                                         |                                      | King III                           | 2.23                  | King III                           | 2.23         |
|                        |                                                         |                                      |                                    |                       |                                    | 2.23.1       |
|                        |                                                         |                                      |                                    |                       |                                    | 2.23.2       |
|                        |                                                         |                                      |                                    |                       |                                    | 2.23.3       |
|                        |                                                         |                                      |                                    |                       | King III                           | 4.3.2        |
|                        |                                                         |                                      |                                    |                       | King III                           | 3.4          |
|                        |                                                         |                                      | King III                           | 2.23                  | King III                           | 3.4          |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8          |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8.1        |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8.2        |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8.2.1      |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8.2.2      |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8.2.3      |
|                        |                                                         |                                      |                                    |                       |                                    | 3.8.2.4      |
|                        |                                                         |                                      |                                    |                       | King III                           | 3.5          |
|                        |                                                         |                                      |                                    |                       |                                    | 3.5.1        |
|                        |                                                         |                                      |                                    |                       |                                    | 3.5.2        |
|                        |                                                         |                                      | ISO 31000                          | 4.3.5 & 5.7           |                                    |              |
|                        |                                                         |                                      | ISO 31000 / King III               | 4.3.4 & 4.3.5 / 4.4.1 |                                    |              |
|                        |                                                         |                                      | ISO 31000 / King III               | 4.3.5 & 5.7 / 4.4.1   |                                    |              |

| Theoretical frameworks |                                                                                | Building blocks             | Level 1 best practice requirements |           | Level 2 best practice requirements |               |
|------------------------|--------------------------------------------------------------------------------|-----------------------------|------------------------------------|-----------|------------------------------------|---------------|
| Deming cycle           | Weisbord organisational design model                                           |                             | Source                             | Ref.      | Source                             | Ref.          |
| Do                     | Leadership, Structure, Relationships, Helping Mechanisms, External environment | V. Implementation.          | ISO 31000                          | 4.4.1     | ISO 31000                          | 4.4.1         |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 4.2 & 4.4.1   |
|                        |                                                                                |                             | ISO 31000                          | 4.4.2     | ISO 31000                          | 5.2           |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 5.3           |
|                        |                                                                                |                             | ISO 31000                          | 4.4.2     | ISO 31000                          | 5.3.2 & 4.3.1 |
|                        |                                                                                |                             |                                    |           |                                    | 5.3.3 & 4.3.1 |
|                        |                                                                                |                             |                                    |           |                                    | 5.3.4 & 4.3.1 |
|                        |                                                                                |                             |                                    |           |                                    | 5.3.5 & 4.3.1 |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 5.4.2         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.5           |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 5.4.3         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.5           |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 5.4.4         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.5           |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 5.5           |
|                        |                                                                                |                             |                                    |           | King III                           | 4.7           |
| Check                  | Rewards                                                                        | VI. Monitor & review.       |                                    |           | King III                           | 4.8           |
|                        |                                                                                |                             |                                    |           |                                    | 4.8.1         |
|                        |                                                                                |                             |                                    |           |                                    | 4.8.2         |
|                        |                                                                                |                             | King III                           | 4.1 & 4.3 | King III                           | 4.1.2         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.1.8         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.1.9         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.3.3         |
|                        |                                                                                |                             |                                    |           | King III                           | 4.2.3         |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 4.5           |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 4.5           |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 4.2 & 4.4.1   |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 4.5           |
|                        |                                                                                |                             | ISO 31000                          | 5.6       | ISO 31000                          | 5.6           |
| Adjust                 | PDCA                                                                           | VII. Continual improvement. | King III                           | 4.9       | King III                           | 4.9.1         |
|                        |                                                                                |                             |                                    |           | ISO 31000                          | 5.6           |

Source: Researcher's own compilation.

This was done deliberately by the researcher in an attempt to: (1) the reduce the misalignment between organisational design principles and ERM program design; (2) improve compliance to international best practice risk management standards and South African corporate governance guidelines; and (3) reduce the ambiguity surrounding the concept of practice-based ERM by providing a straightforward ERM implementation model with clear building blocks, best practice requirements and specific deliverables.

The result was a conceptual ERM implementation model (refer to Figure 5.6) that consists of 7 building blocks, 26 level 1 best practice requirements, 154 level 2 best practice requirements, 69 purposes of deliverables, and 145 proposed deliverables that were derived from the requirements as identified by the researcher.

The **fifth** theoretical objective was to develop a proposed ERM implementation assessment tool consisting of checklists and dashboards (refer to Figure 5.11). The proposed ERM implementation assessment tool is based on the validated ERM implementation model. The assigned responsibilities were aligned with Protiviti's five lines of defence risk governance model. It consists of: (1) an ERM implementation status checklist to determine the status of ERM implementation, either per ERM implementation model building block or per risk stakeholder (refer to Section 5.3.2.1); (2) an ERM implementation status reporting dashboard (refer to Section 5.3.2.2) that will be communicated to the relevant committees and the ERM project sponsor; (3) an ERM implemented deliverables risk assurance assessment checklist (refer to Section 5.3.3.1 and Section 6.2.3.3) that will be used by an independent assurer to determine the degree to which an implemented deliverable is actually completed; and (4) an ERM implemented deliverables risk assurance reporting dashboard, either per ERM implementation model building block or per risk stakeholder, (refer to Section 5.3.3.2 and Section 6.2.3.3) that will be communicated to the relevant committees and the ERM project sponsor.

### 7.2.5 Conclusions for theoretical objectives 3 to 5

The characteristics of effective organisational design (simplicity, flexibility, reliability, economy and acceptability (Johnson *et al.*, 1973) will now also be employed to evaluate the design of the conceptual ERM implementation model.

The model design outline is **simple** in that it follows a building block approach where the one step builds on the previous to produce a result. For example: building blocks I to IV represent all the elements that have to be designed and developed for the ERM program. Building blocks V to VII include all the activities relevant to the entire ERM program and it represents a continuous cycle of implementation, monitoring, review and continual improvement.

The conceptual model is **flexible** in the sense that the derived deliverables can be included or excluded or expanded to reflect the requirements of the specific type of organisation. For example: one of the deliverables from building block I is to get permission for the design and implementation of an ERM program. The derived deliverable is an agenda item for the board meeting. The decision-making body for a listed company will be the board of directors, whereas the decision-making body for a government entity will be located in the office of the minister. The deliverable can easily be changed to reflect that.

Even though the conceptual ERM model is flexible and could be changed, the model was intentionally designed to be prescriptive in terms of the building blocks, associated requirements, and the proposed deliverables to ensure the **reliability** of the outcomes during the implementation process.

Generally, there are limited resources available for the design and implementation of ERM programs. The prescriptive nature of the conceptual model is such that it should result in improved allocation of scarce risk resources and it consequently adheres to the **economy** characteristic of organisational design. The conceptual model is an attempt to answer the call for a practice-based ERM model that will be easy to understand and that can be implemented by risk stakeholders. This should result in a higher level of **acceptability**.

### **7.3 SUMMARY AND CONCLUSIONS FROM THE EMPIRICAL STUDY**

The empirical part of the primary objective—to describe the ERM domain for South African organisations, to confirm the problem statement (phase 1), to validate the ERM implementation model and to confirm the assessment tool (phase 2)—was achieved in the empirical study undertaken.

Chapter 4 explained the research paradigm, research design and method followed, together with the results of phase 1 of the empirical portion of the study. Chapter 6 contained the detail results and discussions relating to phase 2 of the empirical part of the research. In this section the empirical portion of the study will be summarised and the conclusions drawn highlighted in accordance with the various empirical objectives of the research study.

#### **7.3.1 Summary of process and findings**

The empirical portion of the study was divided into **phase 1** to satisfy the requirements of the first (the ERM domain in South Africa) and second (ERM programs in South African organisations) empirical objectives and **phase 2** to satisfy the requirements of the third (validation of the ERM implementation model and confirmation of the ERM implementation assessment tool) empirical objective.

The **first** empirical objective was to obtain information about the South African ERM domain with specific reference to the industry, the type of organisation, and the position of the risk practitioner within the organisation (refer to Section 4.7). A questionnaire was developed to gather information to satisfy the requirements for phase 1. The primary and secondary risk stakeholders that responded to the questionnaire were employed within 11 different industries in South Africa. The financial and insurance activities industry accounts for 46% of the participants; the transportation and storage industry, the manufacturing industry, and the mining and quarrying industry for 9% each; and the public administration and defence, compulsory social security industry, and the information and communication industry for 6% each. Agriculture, forestry and fishing; electricity, gas, steam and air conditioning supply; professional, scientific and technical activities; public order and safety activities; and water supply, sewerage water management and remediation industries only contributed 3% each. This translated to 46% participation from the financial sector and 54% participation from the non-financial sector.

Most of the participants (43%) were employed by private companies, 39% by public companies, 9% by government and 9% by other types of organisations. 73% formed part of middle management (heads of departments, directors of risk or on a manager level); 15% were at top management (executives, C-levels, executive directors and presidents); 9% were involved in first-line management and 3% were at board level.

The **second** empirical objective was to identify and document information about the current ERM programs for South African organisations and to rank the barriers to ERM implementation. The main indication by the participants (94%) was that their organisations have implemented a formalised ERM program. This affirms the notion that the participants have been involved with some or all elements of the design, development, and implementation of their organisations' ERM program. In South African organisations, the most important adoption driver is corporate governance requirements from the board of directors (27%), with legal and regulatory compliance requirements as the second highest adoption driver (25%). This is followed by requirements from shareholders/investors/owners (11%), financial crisis of 2008 (9%), influence by risk practitioners (9%), rating agency requirements (9%), catastrophic events (5%), and pressure from the market (4%).

The majority of the participants indicated that their organisations' ERM programs are based on a combination of best practice risk management frameworks (25%), whereas an equal percentage of 23% is based on ISO 31000 and the COSO risk management best practice frameworks. 24% is based on the King III code of corporate governance as is reflected in Figure 4.16. The majority of the ERM programs (55%) have been implemented for more than 7 years and 45% for 3–7 years. The chief risk officer (CRO) is the ERM program sponsor for 54% of the participants' organisations and the chief executive officer for 26%.

The majority of the participants indicated according to a 'yes-no-don't know' measurement scale that risk management is integrated into their operational processes. The key risks are reported to either the board (26%), the board risk management committee (22%), the executive risk committee (21%), or the departmental risk committee (21%). The participants indicated that the most important perceived benefits from their ERM programs are (1) to enhance risk based decisions (18%) and (2) to align risk appetite and strategy (18%).

The most important barrier to ERM implementation is a lack of board or C-level senior executive leadership. This is followed by role confusion and little or no risk monitoring. Insufficient resources, lack of perceived value added by the ERM program and competing priorities between the risk owner's operational- (day-to-day) and risk responsibilities were ranked at number three. The fourth barrier was that risk management criteria are not standardised. Difficult to identify risk owners, badly designed ERM programs, and incentives do not reward making risk-based decisions were ranked at number 5.

The **third** empirical objective was to adjust the conceptualised ERM implementation model and assessment tool based on the expertise of senior risk stakeholders within South African organisations (refer to Chapter 5). This was done during phase 2, utilising the Delphi technique, where the detailed conceptual ERM implementation model (including the seven building blocks, allocated best practices, derived deliverables and the purpose of each deliverable) and assessment tool were discussed and validated during:

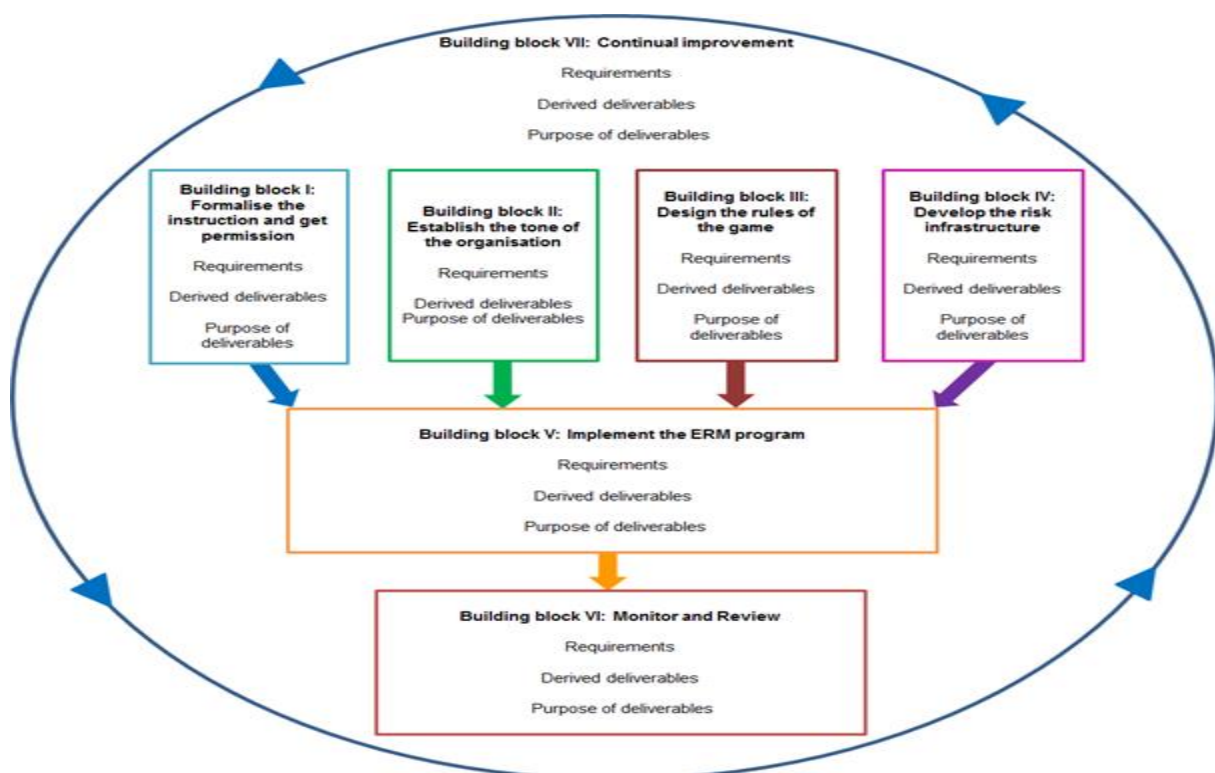
- A first round of semi-structured interviews with the senior risk stakeholders within South African organisations;
- A second round of e-mail communication in which the researcher presented the adjusted ERM implementation model to the same senior risk stakeholders for their final affirmation; and
- A final round of e-mail communication to the same senior risk stakeholders to identify the degree of formality of the ERM implementation model according to the validated deliverables.

The senior risk experts complied with the requirements for expertise in that they:

- Have knowledge and experience regarding the design, development and/or implementation of an ERM program;
- Hold senior level risk management positions within their organisations; and
- Gave written informed consent stating their capacity and willingness to participate in the study.

Round 1 (the semi-structured interviews) resulted in a total of 7 suggested changes and 0 additions to the level 1 best practise requirements; 7 suggested changes and 3 additions to the level 2 best practice requirements; 0 suggested changes and 0 additions to the purpose of the deliverables; and 31 suggested changes and 63 additions to the deliverables of the conceptual ERM implementation model. The conceptual ERM implementation model was adjusted with the suggested changes and additions. The results of round 1 is reflected in Addendum H. This resulted in the adjusted ERM implementation model (refer to Addendum I) which was presented to the same senior risk experts during round 2 of the Delphi technique. They accepted the adjusted ERM implementation model which means that consensus was reached. Addendum J contains the results of round 2 and Addendum K holds the detail of the validated ERM implementation model.

**Figure 7.1: The validated ERM implementation model**



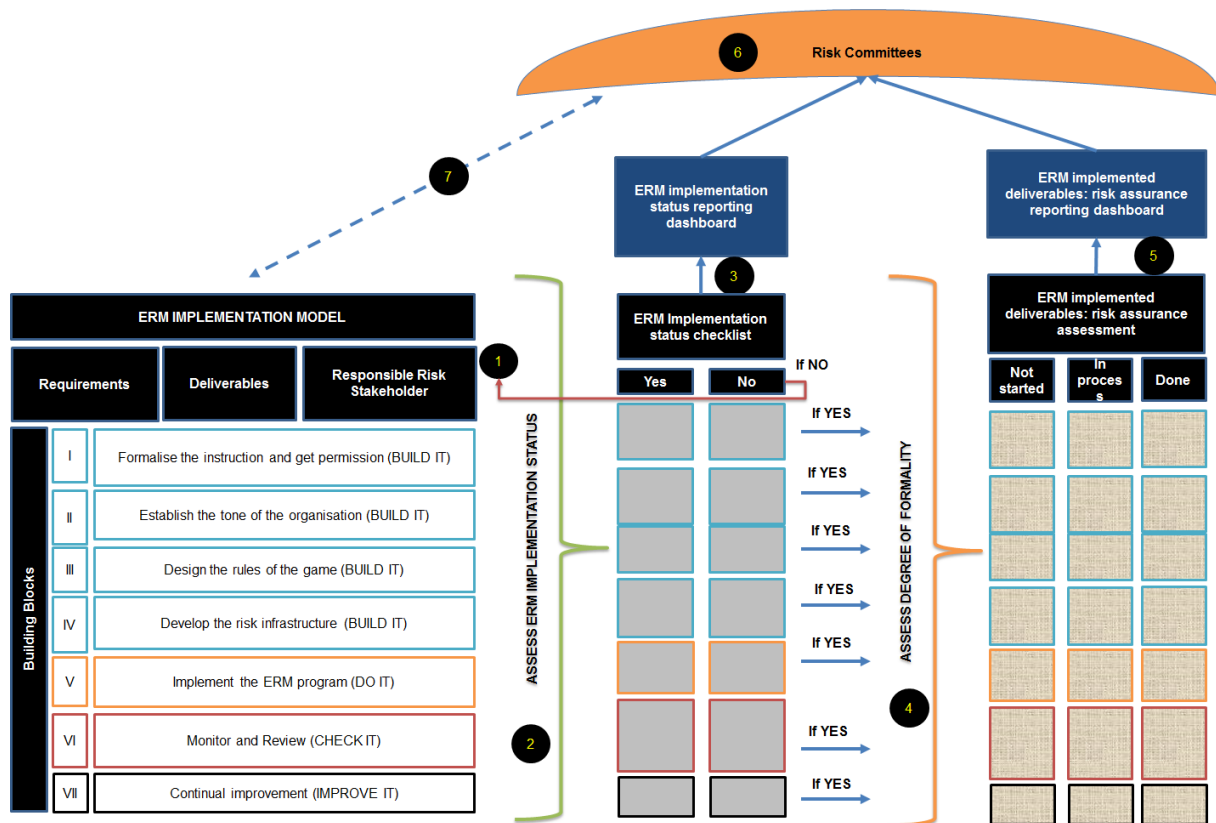
**Source:** Researcher's own compilation.

During round 3 the panel of senior risk experts were asked to comment on the proposed ERM implementation assessment tool's process flow and the assigned responsibilities (refer to Addendum L). The proposed ERM implementation assessment tool is based on the validated ERM implementation model (building blocks, best practice requirements and the derived deliverables) and it consists of formalised checklists, reporting dashboards and feedback loops. The ERM implementation activities (implementation and assessment of implementation) will be executed in accordance with the approved risk governance framework and model for the organisation (refer to Section 5.3.1).

Round 3 concluded with the ERM implementation assessment tool consisting of:

- An ERM implementation status checklist to determine the status of ERM implementation, either per ERM implementation model building block or per risk stakeholder (refer to Section 5.3.2.1 and Addendum B);
- An ERM implementation status reporting dashboard (refer to Section 5.3.2.2 and Figure 5.9) that will be communicated to the relevant committees and the ERM project sponsor;
- An ERM implemented deliverables risk assurance checklist (refer to Section 5.3.3.1 and Addendum M) that will be used by an independent assurer to determine the degree to which an implemented deliverable is actually completed;
- An ERM implemented deliverables risk assurance reporting dashboard, either per ERM implementation model building block or per risk stakeholder (refer to Section 5.3.3.2 and Figure 5.10), that will be communicated to the relevant committees and the ERM project sponsor; and
- Feedback loops from risk committees to the risk facilitators and/or the independent assurance providers.

**Figure 7.2: The overview of the confirmed ERM implementation assessment tool**



#### CONFIRMED ERM IMPLEMENTATION ASSESSMENT PROCESS & RESPONSIBLE PERSONS

- 1 Assign the responsible risk stakeholder per deliverable.
- 2 Get implementation status (Who? Risk facilitator)
- 3 Prepare the ERM implementation status reporting dashboard (Who? Risk facilitator)
- 4 For YES deliverables, assess the degree of formality (Who? Independent assurance provider). For NO deliverables, refer back to the responsible risk stakeholder.
- 5 Prepare the ERM implemented deliverables: risk assurance reporting dashboard (Who? Independent assurance provider)
- 6 Report to relevant risk committees.
- 7 Feedback loops from risk committees to risk facilitators and independent assurance providers.

**Source:** Researcher's own compilation.

### 7.3.2 Conclusions for empirical objectives 1 to 3 (phase 1 and 2)

The purpose of the research study was to develop a practice based ERM implementation model and assessment tool that can be used in any organisation across industries in South Africa. This notion that a need for the model and assessment tool exist in any type of organisation and across industries is supported by the findings of phase 1 (the ERM domain

in South African organisation) where the participants represented 11 industries (refer to Figure 4.9) in all types of organisations (refer to Figure 4.11) and at all levels of management (refer to Figure 4.10) and phase 2 where the senior risk experts represented 8 industries.

The decision by the researcher to use ISO 31000 and King III as the basis for the best practice requirements in the conceptual ERM implementation model is supported by the results of Section 4.7.3.2.1 (refer to Figure 4.16).

The prescriptive nature of the validated ERM implementation model (building blocks with specific requirements and deliverables) means that it can be used as an implementation blueprint by each of the risk stakeholders: The board of directors, the ERM project sponsor, members of the ERM department, the risk owners, and the risk champions. This should also eradicate the barriers to ERM implementation as follows: (1) improve the level of board/C-level/senior executive leadership; (2) reduce role confusion; (3) improve risk monitoring; (4) secure more risk resources due to the ERM project sponsor's improved ability to demonstrate and explain the potential value added by the ERM program; (5) improve buy-in from secondary risk stakeholders that have competing priorities with their operational responsibilities; and (6) improve the ability to identify risk owners due to clarity with regards to ERM program process flow, requirements and deliverables.

The conceptual ERM implementation model and the proposed assessment tool were well received by the senior risk experts during round 1, 2 and 3 of the Delphi technique.

The general comments during the semi-structured interviews were that the ERM implementation model:

- Is unique, comprehensive, practical and logical;
- Easy to follow and understand;
- It can be used as a blueprint for the development of a new ERM program and as a checklist to identify developmental areas for a mature ERM program; and
- It can be used as a guideline by every risk stakeholder to determine the requirements for implementation and their responsibilities in terms of implementation.

The main objective of the ERM implementation assessment tool was two-fold: (1) to determine the level of implementation and (2) to provide assurance that the deliverables were implemented. The researcher and the panel of senior risk experts are of the opinion that the aforementioned objective has been reached by the confirmed ERM implementation assessment tool, process flows and assigned responsibilities (refer to Section 6.2.3.3 and Addenda B and M). The fact that the ERM implementation assessment tool is anchored in the

validated ERM implementation model means that the assessment tool also complies with the characteristics of effective organisational design: simplicity, flexibility, reliability, economy and acceptability. The study exceeded the expectation that was set, in that it resulted in two assessment tools. One that can be used by the ERM department/risk facilitators as a tool to determine the level of ERM implementation and another that can be used by the independent assurance department to provide assurance to the board/senior management/stakeholders regarding the level of ERM implementation in the organisation. This prescriptive nature of the checklist is a deliberate attempt to reduce the bias involved when completing the ERM implementation status report in order to give assurance to the board and senior management regarding the *true* status of the level of ERM implementation. It should also mean that the assessment tools could be used at any level of management within the organisation and within any industry.

#### **7.4 LIMITATIONS OF THE STUDY**

The most obvious limitation of the study is the sample size for phase 1. The sample size was 300 of which 15% responded to the questionnaire (e-survey). It can be argued that the quality of the participants in terms of the level of management (refer to Figure 4.10), years of risk-related experience (refer to Figure 4.13) and the maturity of their ERM programs (refer to Figure 4.17) mean that the results are valid and reliable and that it can be generalised to a larger population of risk practitioners.

The second limitation was that data collection was confined to organisations registered in South Africa. The results of the study could, however, be used in a wider geographical context due to the fact that the best practice requirements were extracted from ISO 31000—an international best practice standard for risk management.

Despite these limitations, the study resulted in a well-constructed ERM implementation model and assessment tools that could be used at any level of management for any type of organisation across all industries.

#### **7.5 CONTRIBUTION OF THE STUDY**

Chapter 3 explains that this study centres on the design of an ERM implementation solution (model and assessment tools) that will address certain areas of concern as identified by various researchers. The first area of concern is the misalignment between the principles of organisational design and ERM program design. The researcher evaluated 14 different organisational design models and different continual improvement models to identify the best

-suited model with which to align the conceptual ERM implementation model. Weisbord's six-box organisational design model and the Deming continual improvement cycle were selected due to its simplicity of design and the ease with which it could be applied to the ERM program.

The second area of concern that the researcher focussed on was the availability of limited literature on *how to* implement ERM. The way in which this research study attempts to address this area of concern is by proposing an ERM implementation model with a specific structure (7 building blocks that are based on Weisbord's six-box organisational design model and the continual improvement Deming cycle); with specific level 1 and level 2 best practice requirements (based on ISO 31000, ISO 31010 and King III); with specific deliverables per requirement (derived from the best practice requirements and based on the researchers practical experience as a risk practitioner); and also by proposing ERM implementation assessment tools that are based on the validated ERM implementation model. The confirmed ERM implementation assessment tools comply with Protiviti's 5 lines of defence risk governance model in terms of structure, assigned responsibility and process flow.

The third area of concern that this study attempts to address is the ambiguity surrounding the concept practice-based ERM. The conceptual ERM implementation model and the proposed ERM implementation assessment tools were validated by senior risk stakeholders from 8 different industries in an attempt to close the gap between ERM theory and ERM application. This resulted in the validated ERM implementation model and confirmed ERM implementation assessment tools.

## **7.6 RECOMMENDATIONS FOR FURTHER RESEARCH**

### **7.6.1 Scope and definition of ERM**

As part of the literature review, the researcher identified several suggestions made by other researchers and practitioners for future research pertaining to the different elements of the ERM domain. These suggestions will be discussed in the next section by categorising the suggested research opportunities according to three themes: (1) Theme 1: ERM definition, fundamentals and importance; (2) Theme 2: Drivers of ERM adoption, implementation and effectiveness; and (3) Theme 3: Value add/usefulness/impact of ERM.

#### **7.6.1.1 Theme 1: Enterprise risk management definition, fundamentals and importance**

The researcher supports the notion of future research in the areas of practice-based ERM in terms of the definition of risk management and to further explore the fundamentals of ERM (definition, underlying principles, comparison between ERM standards and the nature of ERM); as well as the other aspects (such as quantification of reputation and strategic risks, risk management maturity, occurrence of public announcements and disclosures regarding ERM). This should be done in consultation with risk practitioners to ensure an ERM program/discipline that can be applied across industries and for all types of organisations.

#### **7.6.1.2 Theme 2: Drivers of enterprise risk management adoption, implementation and effectiveness**

Several researchers have highlighted that more attention needs to be paid to the *drivers of ERM adoption* (including the size of the organisation, the type of industry, changes in the regulatory environment, internal organisational factors, ownership structure, the training of risk managers, the appointment of a chief risk officer (CRO), a broader scope of risks and operational benefits); and *ERM implementation* (including the process, mechanisms and barriers to implementation).

Other researchers advised that, in addition to all of the above, the impact of interconnectedness on ERM adoption, implementation and effectiveness is also important to explore. A number of researchers have also highlighted the role of different risk stakeholders as a driver of ERM adoption, implementation and effectiveness. It was also recommended that researchers ascertain the role of stakeholders, such as audit committees, when applying ERM for regulated industries. Another area for further research focuses on the importance of the Chief Risk Officer's (CRO's) role in ERM adoption, implementation and effectiveness, but also other risk stakeholders such as members of the board, managers and so forth.

Other areas for future research that can add value to the ERM implementation efforts can be research focused on the generation of risk knowledge, risk reporting and risk communication. A number of experts also suggest that the connection between risk reporting/risk aggregation process/risk reporting and ERM, as well as managerial characteristics (CEO, CRO, managers and so forth) and ERM, can be researched as an indication of the value added/usefulness or impact of ERM. Several researchers proposed that further research is required concerning the

study of ERM adoption in public corporations and the governmental sphere and ERM's role in corporate governance in terms of (1) the nature of ERM (quantification of reputation risk and strategic risk, risk management maturity, occurrence of public announcements and disclosures regarding ERM); and (2) fundamentals of ERM (definition and underlying principles, as well as the comparison between ERM standards).

#### **7.6.1.3 Theme 3: Value added/usefulness/impact of enterprise risk management**

ERM needs to be examined in a pragmatic and practical manner; specifically, focussing on the links between organisational structure and ERM design. Researchers must also focus on ERM's impact on organisational value (including but not limited to strategic planning, organisational performance, and so forth) and ERM impact on shareholder wealth. The following aspects are worth further investigation as part of this theme of future research: risk quality; risk contingency theory; risk knowledge generation; risk reporting and risk communication; risk aggregation; and risk maturity.

#### **7.6.2 Enterprise risk management implementation model and assessment tools**

As the study postulated a validated ERM implementation model and confirmed assessment tools, the logical next step is to utilise this model to ascertain the approach to ERM of various organisations within different industries, and to provide assurance of the actual level of implementation of the ERM programs within these organisations. This information can then be used to develop project plans; as well as risk stakeholder roles and responsibilities matrices per deliverable with the objective to transform the ERM implementation model into a unique ERM implementation and assessment plan with organisation specific deliverables, project plans and assigned responsibilities, thereby increasing transparency and also improving the effective allocation of scarce risk resources.

The King IV Code on Corporate Governance was approved and it will be adopted by organisations in the second half of 2016. The impact of the risk management requirements as described in the King IV Code on Corporate Governance therefore presents an area for further research in terms of its bearing on the validated level 1 and level 2 best practice requirements and the derived deliverables captured in the validated ERM implementation model and confirmed ERM implementation assessment tools.

ISO standards come up for revision every five years, and ISO 31000 and its accompanying Guide 73 on risk management terminology are no exception. The ISO/TC 262/WG 2, the working group responsible for developing core risk management standards, started the process in 2015. Further research is recommended on the potential impact of the revised international best practice risk management principles, guidelines and risk vocabulary on the validated ERM implementation model, and as a result the confirmed ERM implementation assessment tools.

## LIST OF REFERENCES

- Aabo, T., Fraser, J.R.S. & Simkins, B.J. 2005. The rise and evolution of the chief risk officer: enterprise risk management at hydro one. *Journal of Applied Corporate Finance*, 17(3):62-75. <https://erm.ncsu.edu/az/erm/i/chan/m-articles/documents/TheRiseandEvolutionoftheChiefRiskOfficer.pdf> Date of access: 02 March 2015.
- Accenture. 2015. 2015 Global risk management study. [https://www.accenture.com/t20150806T154453\\_\\_w\\_\\_us\\_en/\\_acnmedia/Accenture/Conversion\\_Assets/DotCom/Documents/Global/PDF/Dualpub\\_13/Accenture-2015-Global-Risk-Management-Study-Capital-Markets-Report.pdf](https://www.accenture.com/t20150806T154453__w__us_en/_acnmedia/Accenture/Conversion_Assets/DotCom/Documents/Global/PDF/Dualpub_13/Accenture-2015-Global-Risk-Management-Study-Capital-Markets-Report.pdf) Date of access: 10 April 2016.
- Acharyya, M. & Mutenga, S. 2013. Investigating the development of enterprise risk management in the insurance industry: an empirical study of four major European insurers. Paper presented at the Enterprise Risk Management Symposium, Chicago, IL, 22-24 April 22-2013. <http://www.ermsymposium.org/2013/pdf/erm-2013-paper-acharyya.pdf> Date of access: 1 November 2014.
- Adler, M. & Ziglio, E. 1996. Gazing into the oracle: the Delphi method and its application to social policy and public health. London and Philadelphia: Jessica Kingsley Publishers.
- Aebi, V., Sabato, G. & Schmid, M. 2012. Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, 36(12):3213-3226.
- Alexander, M. & Walkenbach, J. 2013. Excel Dashboards and Reports. 2nd ed. Hoboken, N.J.: John Wiley & Sons.
- Arena, M., Arnaboldi, M. & Azzone, G. 2010. The organisational dynamics of enterprise risk management. *Accounting, Organisations and Society*, 35:659-675. <http://nwulib.nwu.ac.za/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edselp&AN=S0361368210000565&site=eds-live>. Date of access: 18 February 2015.
- Arena, M., Arnaboldi, M. & Azzone, G. 2011. Is enterprise risk management real? *Journal of Risk Research*, 14(7):779-797. <http://www.tandfonline.com/doi/abs/10.1080/13669877.2011.571775> Date of acces: 18 February 2015.

AUS/NZ (Council of Standards Australia and Council of Standards New Zealand. 2004. AS/NZS 4360:2004 - Risk Management. [www.standards.com.au](http://www.standards.com.au) Date of access: 27 September 2015.

Banham, R. 1999. Kit and Caboodle: understanding the scepticism about enterprise risk management. CFO Magazine. <http://www.cfo.com/printable/article.cfm/2987618#> Date of access: 3 April 2015.

Barton, T.L., Shenkir, W.G. & Walker, P.L. 2002. Making enterprise risk management pay off. Upper Saddle River, NJ: FT/Prentice Hall.

Bates, L. 2010. Avoiding the pitfalls of enterprise risk management. Journal of Risk Management in Financial Institutions, 4(1):23-28.

Baxter, R., Bedard, J.C., Hoitash, R. & Yezegel, A. 2013. Enterprise risk management program quality: determinants, value relevance, and the financial crisis. Contemporary Accounting Research, 30(4):1264-1295. [http://onlinelibrary.wiley.com/doi/10.1111/j.1911-3846.2012.01194.x/abstract;jsessionid=379A36D8F0BD8D1790A4C91E6DB4A205.f02t04?syst](http://onlinelibrary.wiley.com/doi/10.1111/j.1911-3846.2012.01194.x/abstract;jsessionid=379A36D8F0BD8D1790A4C91E6DB4A205.f02t04?systemMessage=Wiley+Online+Library+will+be+unavailable+on+Saturday+14th+May+11%3A00-14%3A00+BST+%2F+06%3A00-09%3A00+EDT+%2F+18%3A00-21%3A00+SGT+for+essential+maintenance.Apologies+for+the+inconvenience.&userIsAuthenticated=false&deniedAccessCustomisedMessage=)  
[emMessage=Wiley+Online+Library+will+be+unavailable+on+Saturday+14th+May+11%3A00-14%3A00+BST+%2F+06%3A00-09%3A00+EDT+%2F+18%3A00-21%3A00+SGT+for+essential+maintenance.Apologies+for+the+inconvenience.&userIsAuthenticated=false&deniedAccessCustomisedMessage=](http://onlinelibrary.wiley.com/doi/10.1111/j.1911-3846.2012.01194.x/abstract;jsessionid=379A36D8F0BD8D1790A4C91E6DB4A205.f02t04?systemMessage=Wiley+Online+Library+will+be+unavailable+on+Saturday+14th+May+11%3A00-14%3A00+BST+%2F+06%3A00-09%3A00+EDT+%2F+18%3A00-21%3A00+SGT+for+essential+maintenance.Apologies+for+the+inconvenience.&userIsAuthenticated=false&deniedAccessCustomisedMessage=) Date of access: 19 February 2015

Beasley, M., Branson, B. & Pagach, D. 2015. An analysis of the maturity and strategic impact of investments in ERM. Journal of Accounting and Public Policy. 34(3):219-243. <http://eds.b.ebscohost.com/nwulib.nwu.ac.za/eds/detail/detail?sid=ff486b33-eaec-4790-88d1-48e56e47430b%40sessionmgr104&vid=0&hid=113&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=S0278425415000101&db=edselp> Date of access: 09 March 2015.

Beasley, M., Pagach, D. & Warr, R. 2008. Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. Journal of Accounting, Auditing & Finance, 23(3):311-332. <https://erm.ncsu.edu/az/erm/i/chan/m-articles/documents/MS1192FullPaperforWebPostingJune1907.pdf> Date of access: 18 February 2015.

Beasley, M.S., Branson, B.C. & Hancock, B.V. 2008. Rising Expectations. Journal of Accountancy, 205(4):44-51.

Beasley, M.S., Branson, B.C. & Hancock, B.V. 2009. ERM: Opportunities for improvement. *Journal of Accountancy*, 208(3):28-32.

Beasley, M.S., Branson, B.C. & Hancock, B.V. 2015a. 2015 Report on the current state of enterprise risk oversight: update on trends and opportunities. [http://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa\\_erm\\_research\\_study\\_2015.pdf](http://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa_erm_research_study_2015.pdf) Date of access: 20 July 2015.

Beasley, M.S., Branson, B.C. & Hancock, B.V. 2015b. 2015 Report on the current state of enterprise risk oversight. The ERM Initiative at North Carolina State University, Raleigh, NC. <https://erm.ncsu.edu/library/article/current-state-erm-2015> Date of access: 10 April 2015.

Beasley, M.S., Clune, R. & Hermanson, D.R. 2005. Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24(6): 521-531. <https://erm.ncsu.edu/az/erm/i/chan/library/EmpiricalAnalysis.pdf> Date of access: 18 February 2015.

Beaumier, C. & DeLoach, J. 2011. Ten common risk management failures and how to avoid them. *Business Credit*, 113(8):46.

Beckhard, R. 1972. Optimising team building efforts. *Journal of Contemporary Business*. p. 23-27.

Bevir, M. 2012. Governance: a very short introduction. Vol. 333. Oxford, UK: Oxford University Press.

Blaskovich, J. & Taylor, E.Z. 2011. By the numbers: individual bias and enterprise risk management. *Journal of Behavioral & Applied Management*, 13(1):5-23. [http://www.ibam.com/pubs/jbam/articles/vol13/Article\\_1\\_Blaskovich.pdf](http://www.ibam.com/pubs/jbam/articles/vol13/Article_1_Blaskovich.pdf) Date of access: 18 February 2015.

Bolman, L.G. & Deal, T.E. 1991. Leadership and management effectiveness: a multi-frame, multi-sector analysis. *Human Resource management*, 30(4):509-534.

Boulding, K. E. 1965. The image. Ann Arbor: University of Michigan Press.

Boulton, B. & Dominus, M. 2014. Developing an effective risk culture. *Electric Perspectives*, 39(3):57.

Bowen, J.K., Cassel, R., Collins, C., Dickson, K., Fleet, M., Ingram, D., Meyers, S., Mueller, H., Samaniego, Z., Siberón, J., Wille, S. & Yu, M. 2006. Society of actuaries: enterprise risk management specialty guide. Discussion paper, May 2006.

Bromiley, P., McShane, M., Nair, A. & Rustambekov, E. 2014. Enterprise Risk Management: review, critique, and research directions. Long Range Planning, 48(2015):265-276 <http://dx.doi.org/10.1016/j.lrp.2014.07.005> Date of access: 18 February 2015.

Bullen, P. 2015. Thriving organisations. <http://www.mapl.com.au/organisations/organisations4.htm> Date of access: 18 May 2016.

Burke W.W. & Litwin G.H. 1992. A causal model of organisation performance and change. Journal of Management, 18(3):523-545.

Burnaby, P. & Hass, S. 2009. Ten steps to enterprise-wide risk management. Corporate Governance, 9(5): 539-550. <http://eds.b.ebscohost.com.nwulib.nwu.ac.za/eds/detail/detail?sid=593c5957-5a8f-4be9-af62-4edbfaddba3a%40sessionmgr106&vid=0&hid=113&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=45205574&db=buh> Date of access: 05 March 2015.

Carroll, R.L., Hoppes, M., Hagg-Rickert, S., Youngberg, B.J., McCarthy, B.A., Shope, D., Kielhorn, T., & Driver, J. 2014. Enterprise risk management: a framework for success. American Society for Healthcare Management. [http://www.ashrm.org/pubs/files/white\\_papers/ERM-White-Paper-8-29-14-FINAL.pdf](http://www.ashrm.org/pubs/files/white_papers/ERM-White-Paper-8-29-14-FINAL.pdf) Date of access: 17 May 2016.

CAS (Casualty Actuarial Society). 2003. Overview of enterprise risk management. The 2002 enterprise risk management Committee. <https://www.casact.org/area/erm/overview.pdf> Date of access: 3 April 2015.

Chapman, R.J. 2011. Simple tools and techniques for enterprise risk management. Hoboken, N.J.: John Wiley & Sons.

Choi, T. 1995. Conceptualizing continuous improvement: implications for organisational change. Omega, 23(6):607-624.

CIPS (Chartered Institute of Purchasing and Supply Chain). 2014. Internal, connected and external stakeholders. Chartered Institute of Purchasing and Supply Chain.

Colquitt, L.L., Hoyt, R.E. & Lee, R.B. 1999. Integrated risk management and the role of the risk manager. *Risk Management and Insurance Review*, 2(3):43-61.

Companies Act. 2008. No 71 of 2008: Companies Act, 2008.

COSO (Committee of Sponsoring Organisations). 2004. Enterprise risk management — integrated framework. <http://www.coso.org/erm-integratedframework.htm> Date of access: 3 April 2015.

CQI (Chartered Quality Institute). 2016. Continual improvement. Available from: <http://www.thecqi.org/Knowledge-Hub/Knowledge-portal/Concepts-of-quality/Continual-improvement> Date accessed: 30 May 2016.

Dalkey, N.C. 2005. The Delphi Methodology. <Http://www.fernuni-hagen.de/ZIFF/v2-ch45a.Htm>. Date of access: 12 July 2016.

D'Arcy, S.P. & Brogan, J.C. 2001. Enterprise risk management. *Journal of Risk Management of Korea*, 12(1):207-228. <http://www.business.illinois.edu/~s-darcy/Fin321/2007/Readings/erm.pdf> Date of access: 31 March 2015.

Daft, R. L. 1992. Organisation theory and design. 4th ed. St. Paul, MN: West Publishing.

DeLoach, J.W. 2000. Enterprise-wide risk management: strategies for linking risk and opportunity. 1st ed. Harlow, UK: FT Prentice Hall.

Deloitte. 2015. Operating in the new normal: increased regulation and heightened expectations. University Press <https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/>

Deming, W.E. 1982. Out of the crisis. 1st ed. Cambridge, UK: MIT Press.

Deragon, J. 2000. Old knowledge with a new name. Online publishing. <http://www.Erisk.com> Date of access: 27 September 2015.

Desender, K.A. 2011. On the determinants of enterprise risk management implementation. (In Si Shi, N. & Silvius, G. eds. 2011. Enterprise IT governance, business value and performance measurement, Hershey, PA: IGI Global.)

- Dickinson, G. 2001. Enterprise risk management: its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance*, 26(3):360-366. <https://www.actuaries.org.uk/documents/enterprise-risk-management-its-origins-and-conceptual-foundation-gerry-dickinson> Date of access: 02 March 2015.
- Dornberger, K., Oberlehner, S. & Zadrazil, N. 2014. Challenges in implementing enterprise risk management. *ACRN Journal of Finance and Risk Perspectives*, 3(3):1-14. <http://www.acrn-journals.eu/resources/jfrp201403a.pdf> Date of access: 28 February 2015.
- Fink, A. 2016. *How to conduct surveys: a step-by-step guide*. 6th ed. Los Angeles, CA: Sage Publications, Inc.
- Fox, C. 2012. 10 Easy steps to implement enterprise risk management. *Risk Management Journal*, November:34-36. <http://connection.ebscohost.com/c/articles/86666806/10-easy-steps-implement-enterprise-risk-management> Date of access: 18 February 2015.
- Fraser, J.R.S. & Simkins, B.J. 2007. Ten common misconceptions about enterprise risk management. *Journal of Applied Corporate Finance*, 19(4):75-81.
- Freedman, A.M. 1987. *The swamp model: a sociotechnical systems approach to understanding organisations and enhancing organisational effectiveness. Facilitating and Managing Complex System Change*. Alexandria, VA: NTL Institute.
- Frigo, M.L. & Anderson, R.J. 2011. *Embracing enterprise risk management. Thought Leadership in ERM. Working paper. Committee of Sponsoring Organisation of the Treadway Commission*. <http://www.cosa.org> Date of access: 11 April 2015.
- Galbraith, J.R. 1970. Organisation design. (In Phillips, V., ed. 1970. *Organisation behaviour: prospectives and perceptions*. AFOSR 70-2310TR, Air Force Systems Command: USAF).
- Galbraith, J. R. 1987. Organisation design. (In Lorsch, J.W. ed. *Handbook of organisational behaviour*. Englewood Cliffs, NJ: Prentice Hall. p. 343-357).
- Garvey, P.R. 2008. *Analytical methods for risk management: A systems engineering perspective*. Boca Raton, FL: CRC Press.

Gates, S., Nicolas, J.L. & Walker, P.L. 2012. Enterprise risk management: a process for enhanced management and improved performance. *Management Accounting Quarterly*, 13(30):28-38.

Gordon, L.A., Loeb, M.P. & Tseng, C.-Y. 2009. Enterprise risk management and firm performance: a contingency perspective. *Journal of Accounting and Public Policy*, 28:301-327.

Gordon, T.J. 1994. The Delphi Method. *Futures Research Methodology*, AC/UNU Project. <http://fpf.ueh.edu.vn/imgnews/04-Delphi.pdf> Date of access: 12 July 2016.

Greenberg, J. 2011. *Behaviour in organisations*. 10th ed. Boston, London: Pearson.

Guba, E.G. & Lincoln, Y.S. 2005. *Paradigmatic controversies, contradictions, and emerging influences*. 3rd ed. London: Sage Publications.

Hallebone, E. & Priest, J. 2009. *Business and management research: paradigms and practices*. New York: Palgrave Macmillan.

Hamill, M. 2007. The practical challenges of ERM. <http://eds.a.ebscohost.com.nwulib.nwu.ac.za/eds/detail/detail?vid=2&sid=e708dc95-5f22-4787-89ca-593f875888f8%40sessionmgr4005&hid=4102&bdata=JnNpdGU9ZWRzLWxpdm>

Handfield, R.B., Monczka, R.M., Giunipero, L.C. & Patterson, J.L. 2009. *Sourcing and supply chain management*. 4th ed. Mason, OH: South-Western Cengage Learning.

Hanna, D.P. 1988. *Designing organisations for high performance*. Boston, MA: Addison-Wesley.

Harner, M.M. 2010. Barriers to effective risk management. *Section Hall Law Review*, 40(4): 1323-1364. <http://nwulib.nwu.ac.za/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=hein.journals.shlr40.43&site=eds-live> Date of access: 02 March 2015.

Harrington, S. E., Niehaus, G., & Risko, K.J. 2002. Enterprise risk management: the case of United Grain Growers. *Journal of Applied Corporate Finance*, 14(4):71-81.

Harrison, M.I. 1987. *Diagnosing organisations: Methods, models, and processes*. 1st ed. London: Sage Publications.

Hasson, F., Keeney, S. & McKenna, H. 2000. Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4):1008-1015.

Hellings, S. 2014. The trials and tribulations of ERM. *Credit Control*, 35(6/7):51. <http://eds.b.ebscohost.com.nwulib.nwu.ac.za/eds/detail/detail?sid=b788ed1b-077b-4380-98f0-6e5f8d14716c%40sessionmgr106&vid=0&hid=113&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=100414933&db=f5h> Date of access: 18 February 2015.

Holton, G.A. 1996. Closed form value at risk. *Contingency Analysis*. <http://www.contingencyanalysis.com/frame/framevar.htm> Date of access: 27 September 2015.

Holton, G.A. 2004. Defining risk. *Financial Analysts Journal*, 60(6):19-25. <http://2fljy5491hlzc8ww3j1ntejkw.wpengine.netdna-cdn.com/wpcontent/uploads/2006/10/risk.pdf> Date of access: 31 March 2015.

Hoyt, R.E. & Liebenberg, A.P. 2011. The value of enterprise risk management. *Journal of Risk & Insurance*, 78(4):795-822. <http://www.irmsymposium.org/pdf/papers/hoyt.pdf> Date of access: 18 February 2015.

Hubbard, D.W. 2009. *The failure of risk management: why it's broken and how to fix it*. 1st ed. New Jersey, NJ: John Wiley & Sons.

Hufty, M. 2011. Investigating policy processes: the governance analytical framework (GAF). *Research for sustainable development: foundations, experiences, and perspectives*: 403-424.

IIA (Institute of Internal Auditors). 2013. The three lines of defense in effective risk management and control: Institute of Internal Auditors. <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf> Date of access: 15 May 2016.

IODSA (Institute of Directors Southern Africa). 2009. *The King Code of Corporate Governance for South Africa 2009*. Institute of directors in Southern Africa, Parklands, Johannesburg, South Africa. <http://www.iodsa.co.za/?kingIII> Date of access: 11 October 2015.

IRM (The Institute of Risk Management). 2002. *A risk management standard*. The Institute of Risk Management, London, UK.

IRMSA (The Institute of Risk Management South Africa). 2014. *The IRMSA Guideline to Risk Management*. The Institute of Risk Management South Africa, Johannesburg, South Africa.

ISO (International Organisation for Standardisation). 2009a. Guide 73: 2009 - Risk management vocabulary. International Organisation for Standardisation, Geneva, Switzerland.

ISO (International Organisation for Standardisation). 2009b. ISO 31000: 2009 Risk management – principles and guidelines. International Organisation for Standardisation, Geneva, Switzerland.

ISO (International Organisation for Standardisation). 2009c. ISO 31010: Risk assessment techniques. International Organisation for Standardisation, Geneva, Switzerland.

Janićijević, N. 2010. Business processes in organisational diagnosis. *Management: Journal of Contemporary Management Issues*, 15(2):85-106.

Jonker, J. & Pennink, B. 2010. The essence of research methodology: a concise guide for master and PhD students in management science. Heidelberg: Springer.

Johnson, R.A., Kast, F.E. & Rosenzweig, J.E. 1973. Systems theory and management. *Management Science Journal*, 10(2):367-384.

Kerstin, D, Simone, O & Nicole, Z. 2014. Challenges in implementing enterprise risk management. *ACRN Journal of Finance and Risk Perspectives*, 3(3):1-15.

Kilmann, R.H. 1984. Beyond the quick fix, managing five tracks to organisational success. San Francisco, CA: Jossey-Bass.

Kleffner, A.E., Lee, R.B. & McGannon, B. 2003. The effect of corporate governance on the use of enterprise risk management: evidence from Canada. *Risk Management & Insurance Review*, 6(1):53-73. <http://eds.b.ebscohost.com.nwulib.nwu.ac.za/eds/detail/detail?sid=e17e6198-c8d0-4d01-ba04-bd2f12fe4e68%40sessionmgr103&vid=0&hid=113&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=10143841&db=buh> Date of access: 16 March 2015.

Lam, J. 2010. Enterprise risk management: back to the future: several challenges still need addressing before enterprise risk management can truly be called a success. *The RMA Journal*, (9):16.

Lam, J.C. & Kawamoto, B.M. 1997. Emergence of the chief risk officer. *RIMS Magazine*, 44(9):30.

Leavitt, H.J. 1965. Applied organisational change in industry, (In March. J.G. ed. *Handbook of organisations*. Chicago, IL: Rand McNally. p. 1144-1170.)

Lewin, K. 1943. Defining the "Field at a given time." *Psychological Review*, (50):292-310.

Liebenberg, A.P. & Hoyt, R.E. 2003. The determinants of enterprise risk management: evidence from the appointment of chief risk officers. *Risk Management & Insurance Review*, 6(1):37-52. <https://erm.ncsu.edu/az/erm/i/chan/m-articles/documents/TheDeterminantsofEnterpriseRiskManagement.pdf> Date of access: 02 March 2015.

Likert, R. 1967. *The human organisation: its management and values*. New York, NY: McGraw-Hill.

Likhang, R. 2009. Embedding risk management in organisational processes. Paper for CIS Corporate Governance Conference in Johannesburg, South Africa, on 10 to 11 September 2009. <http://www.chartsec.co.za/documents/speakerPres/RobertLikhang/LikhangEmbeddingRiskManagementInOrgansationICSA.pdf> Date of access: 25 March 2014.

Lvov, B. 2009. The three lines of defense. Audit Committee Institute. <https://www.kpmg.com/RU/en/IssuesAndInsights/ArticlesPublications/Audit-Committee-Journal/Documents/The-three-lines-of-defence-en.pdf> Date of access: 15 May 2016.

Martin, D. & Power, M. 2007. The end of enterprise risk management. Aei-Brookings Joint Center for Regulatory Studies. August. <http://www.centerforfinancialstability.org/research/ERM.pdf> Date of access: 23 February 2015.

McMillan, E. 2004. *Complexity, organisations and change*. London, UK: Routledge.

McShane, M.K., Nair, A. & Rustambekov, E. 2011. Does enterprise risk management increase firm value? *Journal of Accounting, Auditing and Finance*, 26(4):641-658.

Merchant, K.A. 2012. ERM: where to go from here: why new tools are needed to help companies properly assess risks and opportunities. *Journal of Accountancy*, (3):32.

Meulbroek, L.K. 2002. Integrated risk management for the firm: a senior manager's guide. *Journal of Applied Corporate Finance*, 14(4):56-70. <http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6622.2002.tb00449.x> Date of access: 29 September 2015.

Miccolis, J. 2000. Enterprise risk management in the financial services industry: still a long way to go. <https://www.irmi.com/articles/expert-commentary/enterprise-risk-management-in-the-financial-services-industry-still-a-long-way-to-go> Date of access: 15 March 2015.

- Miccolis, J. & Shah, S. 2001. Creating value through enterprise risk management - a practical approach for the insurance industry. New York, NY: Tillinghast-Towers Perrin. <http://ermworkingparty.pbworks.com/f/Value+through+ERM+TP+2002051306.pdf> Date of access: 27 September 2015.
- Mikes, A. & Kaplan, R. 2013. Managing risks: towards a contingency theory of enterprise risk management. Working Paper. Harvard Business School Division of Research. p.1-41. [http://www.hbs.edu/faculty/Publication%20Files/13-063\\_5e67dffe-aa5e-4fac-a746-7b3c07902520.pdf](http://www.hbs.edu/faculty/Publication%20Files/13-063_5e67dffe-aa5e-4fac-a746-7b3c07902520.pdf) Date of access: 9 March 2015.
- Miller, K.D. & Waller, H.G. 2003. Scenarios, real options and integrated risk management. Long Range Planning, 36:93-107.
- Nadler, D.A. & Tushman, M.L. 1980. A model for diagnosing organisational behaviour. Organisational Dynamics, 9(2):35-51.
- Nadler, D.A. & Tushman, M.L. 1999. The organisation of the future: strategic imperatives and core competencies for the 21st century. Organisational Dynamics, 28(1):45-60.
- Nelson, L. & Burns, F.L. 1984. High performance programming: a framework for transforming organisations. Transforming work: a collection of organisational transformation readings. p. 226-242.
- Newsome, R. 2011. Governance of Risk. Johannesburg, SA: Price Waterhouse Cooper. <https://www.pwc.co.za/en/assets/pdf/governance-of-risk.pdf> Date of access: 15 May 2016.
- Nocco, B.W. & Stulz, R.M. 2006. Enterprise risk management: theory and practice. Journal of Applied Corporate Finance, 18(4):8-20.
- Paape, L. & Speklé, R.F. 2012. The adoption and design of enterprise risk management practices: an empirical study. European Accounting Review, 21(3):533-564.
- Pagach, D.P. & Warr, R.S. 2010. The effects of enterprise risk management on firm performance. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1155218](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155218) Date of access: 18 March 2015.
- Pagach, D.P. & Warr, R.S. 2011. The characteristics of firms that hire chief risk officers. Journal of Risk & Insurance, 78(1):185-211.

Palinkas, L. A., Aarons, G. A., Horwitz, S. M., Chamberlain, P., Hurlburt, M., & Landsverk, J. 2011. Mixed method designs in implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 38:44-53.

Palinkas, LA, Horwitz, SM, Carla A. Green, CA, Wisdom, JP, Duan, N & Hoagwood, K. 2015. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, September 2015, 42(5):533-544.

Pfeffer, J. 1997. *New directions for organisation theory: problems and prospects*. Oxford, UK: Oxford University Press.

Prodyot, S., Wolfe, S. & McCabe, K. 2013. Translating ERM from a theoretical perspective into practical and effective actions that impact performance. *University Risk Management and Insurance Association (URMIA) Journal*, 59-66. [www.urmia.org](http://www.urmia.org) Date of access: 02 March 2015.

Protiviti. 2013. Applying the five lines-of-defense in managing risk. *The Bulletin*, 5(4). <https://www.protiviti.com/en-US/Documents/Newsletters/Bulletin/The-Bulletin-Vol-5-Issue-4-Applying-5-Lines-Defense-Managing-Risk-Protiviti.pdf> Date of access: 25 September 2015.

Pugh, D.S., Hickson, D.J., Hinings, C.R. & Turner, C. 1968. Dimensions of organisation structure. *Administrative Science Quarterly*, 13(1):65-105.

Pullan, P. & Murray-Webster, R. 2011. *A short guide to Facilitating Risk management*. Farnham, UK: Gower Publishing Limited.

RIMS (Risk & Insurance Management Society). 2011. *RIMS Enterprise risk management (ERM) Survey*: RIMS/Advisen Ltd.

RIMS (Risk & Insurance Management Society). 2013. *RIMS Enterprise risk management (ERM) Survey*: RIMS/Advisen Ltd.

Robbins, S.P. and Barnwell, N. 2006. *Organisation theory: concepts and cases*. 5th ed. Frenchs Forest, AUS: Pearson Education.

Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research methods for business students*. London: Pearson Education.

Schanfield, A. & Helming, D. 2008. 12 top ERM implementation challenges. *Internal Auditor*, 65(6):41-44.

Scott, W.R. & Meyer, J.W. 1994. *Institutional environments and organisations: structural complexity and individualism*. Thousand Oaks, CA: Sage Publications.

Selznick, P. 1957. *Leadership in administration: a sociological interpretation*. Evanston, IL.: Row, Peterson.

Senior Supervisors Group. 2009. Risk management lessons from the global banking crisis of 2008. <https://www.sec.gov/news/press/2009/report102109.pdf> Date of access: 28 February 2015.

Smith, C., Niehaus, G., Briscoe, C., Coleman, W., Lawder, K., Ramamurtie, S., Verbrugge, J. & Chew, D. 2003. University of Georgia roundtable on enterprise-wide risk management. *Journal of Applied Corporate Finance*, 15:8-26.

Sobel, P.J. & Reding, K.F. 2004. Aligning corporate governance with enterprise risk management. *Management Accounting Quarterly*, 5(2):29.

Spencer-Pickett, K.H. 2003. *The internal auditing handbook*. 2nd ed. NJ: John Wiley & Sons.

Standard & Poor. 2008. Enterprise risk management: Standard & Poors to apply enterprise risk analysis to corporate ratings. <https://erm.ncsu.edu/library/article/ERM-Credit-ratings> Date of access: 3 April 2015.

Stanford, N. 2007. *Guide to organisation design: creating high-performing and adaptable enterprises*. 10th ed. London, UK: Profile Books.

Statistics South Africa. 2012. *Standard industrial classification of all economic activities (SIC)*. Pretoria: Government printer.

Stulz, R.M. 1996. Rethinking risk management. *Journal of Applied Corporate Finance*, 9(3):8-25.

TBCS (Treasury Board of Canada Secreteriat). 2001. *Integrated risk management framework*. <http://www.tbs-sct.gc.ca> Date of access: 03 April 2015.

Teach, E. 2013. The upside of ERM. *CFO Magazine*, 29(9):42.

Tersine, R.J. 2004. The primary drivers for continuous improvement: the reduction of the triad of waste. *Journal of Managerial*, (1):15.

Thompson Reuters Accelus. 2014. Driving enterprise risk management best practices for energy firms. <https://risk.thomsonreuters.com/sites/default/files/GRC01119.pdf> Date of access: 17 May 2016.

Tichy, N.M. 1983. Managing strategic change: technical, political, and cultural dynamics. New York, NY: John Wiley & Sons.

Toplis, M.J. & Randell, G. 2014. Towards organisational fitness: a guide to diagnosis and treatment. Farnham, UK: Gower Publishing, Ltd.

Tufano, P. 1996. Who manages risk? An empirical examination of risk management practices in the gold mining industry. *Journal of Finance*, 51(4):1097-1137.

Ulieru, M. & Unland, R. 2004. Enabling technologies for the creation and restructuring process of emergent enterprise alliances. *International Journal of Information Technology & Decision Making*, 3(01):33-60.

Vaill, P. 1975. Reflections on technology. *Social Change*, 5(4):3-7.

Van Zyl, S. 2014. Risk data to risk intelligence. *Canadian Underwriter*, 81(10):46-49.

Viscelli, T.R., Hermanson, D.R. & Beasley, M.S. 2014. ERM: the implementation process and strategic effectiveness. Unpublished.

Von Bertalanffy, L. 1950. An outline of general system theory. *British Journal for the Philosophy of science*, 1(2):134-165.

Waterman, R.H. & Peters, T.J. 1982. In search of excellence: lessons from Americas best run companies. New York, NY: Harper Collins.

WEF (World Economic Forum). 2016. The global risks report 2016. <http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf> Date of access: 27 April 2016.

Weisbord, M.R. 1976. Organisational diagnosis: six places to look for trouble with or without a theory. *Group & Organisation Studies*, 1(4): 430-447.

Wilber, K. 2003. Introduction to integral theory and practice. Integral Naked. <http://www.humanemergence.nl/uploads/2011/03/IOS-Basic-Intro-to-Integral.pdf> Date of access: 18 May 2015.

Yousuf, M.I. 2007. Using Experts' Opinions Through Delphi Technique. Practical Assessment, Research & Evaluation Journal, 12(4)