A FRAMEWORK FOR INFORMATION SECURITY RISK MANAGEMENT COMMUNICATION

[1]Werner G. Bornman **[2]Les Labuschagne**

Academy for Information Technology, University of Johannesburg, South Africa

[1]werner.bornman@kpmg.co.za [2]ll@na.rau.ac.za

PO Box 524, Auckland Park, Johannesburg, South Africa, 2006

+27 (11) 489-2847

ABSTRACT

Organisations have over the last couple of years become more aware of the importance of information security risk management and its corresponding due diligence requirements. A cornucopia of information security risk management approaches exist that can assist organisations in determining and controlling risks. However, with these choices organisations are finding it increasingly difficult to communicate the information security risks to the strategic level or for strategic management to communicate information security goals to the organisation. An approach is necessary that will enable organisations to communicate information security risk information to strategic level management quickly and unambiguously. This approach will have to provide information in accordance with corporate governance requirements and be based on best practice. This article suggests a framework that was developed from best practice and industry standards, and takes into consideration various information security risk management approaches.

KEYWORDS

Information security; information security risk management; risk management, risk communication, corporate governance, IT governance

A FRAMEWORK FOR INFORMATION SECURITY RISK MANAGEMENT COMMUNICATION

1 INTRODUCTION

Information security risk management is a business area that has over the last decade become a prominent risk management field within organisations. This increased importance is mainly through the due diligence expected by governmental regulations or recommendations such as King II [KING 02], Sarbanes-Oxley Act [TUDO 01] and the Turnbull Report [INCA 99].

These recommendations require that management take responsibility and accountability for risks within their organisations, including the information technology (IT) related risks that radiate from within and around modern organisations. However, organisations regard IT as a supporting function that should be managed as such. This "supporting" function can have a far greater impact on organisations that what is sometimes expected.

Management cannot manage what they are not aware of; therefore it is necessary that management obtain risk management information (including the controls to mitigate those risks) in a timely manner. Currently various information security risk management (ISRM) methodologies can be implemented, but these methodologies, approaches or frameworks are targeted at different levels in the organisation, which makes it difficult to consolidate the risk information.

A solution would have to be developed that can assist organisations in communicating ISRM information across all levels of the organisation. The framework should fulfil three basic requirements: it should be easy to implement in any organisation irrespective of size and industry type, it should be based on corporate governance requirements and industry best practice and finally it should communicate ISRM information effectively.

The goal of this article is to present a framework that solves the ISRM communication dilemma that exists between the various managerial levels of the organisation. This goal will be reached through several objectives. The first is to provide background on why ISRM communication is a problem in modern organisations. The second objective is to discuss the processes that were followed in developing the solution, and the third objective is to discuss the structure and processes involved in implementing the framework. The fourth objective is to provide an objective evaluation of the framework.

The next section provides a high level overview of the ISRM environment and why communication within this environment is difficult for modern organisations.

2 INFORMATION SECURITY RISK MANAGEMENT CACOPHONY

Organisations have always been aware of the importance of good corporate governance, none so much as in the last couple of years. Governments and stock trading institutions require organisations to demonstrate due diligence [TUDO 01]. With these requirements imposed, organisations have to institute methodologies, frameworks and approaches in ensuring compliance. Coupling due diligence with the proliferation of information technology in organisations, there is a need for organisations to extend their financial and organisational controls to the IT environment to ensure that the information is kept confidential, accurate and available when required. These three components form the basis of information security [CRAM 03] [TUDO 01] [SABS 00].

There are numerous information security risk management related methodologies, approaches and frameworks [CRAM 03] [COBI 00] [IST 03] [ALBE 03]. However, none consider the context of information security communication within the organisational structure. These approaches, methodologies and frameworks have a horizontal plane view of risks of either the operational,

tactical or strategic levels. Several methodologies such as CRAMM [CRAM 03] and CORAS [IST 03] are operational level ISRM methodologies that rely on software applications. These applications produce lengthy reports based on technical evaluation of the information security risks in an organisation.

Several documents can be produced for different divisions or business units. These documents are not communicated in a business sense for top management to understand the impact the risks can have on the organisation. Furthermore, the different documents might not provide sufficient business case or regulatory required information for top management to action the risk controls [BORN 04]. Organisations' strategic decisions are not made on technical reports; therefore organisations require a framework that will enable the communication of ISRM information to top management.

3 BUILDING THE FRAMEWORK

Different approaches were considered in solving the communication problem. However, a framework is a flexible approach that can be applied to all organisations. It is a structure that enables organisations to "fit" their requirements, methods and approaches in an organised formation to achieve a specific goal [OXFO 80]. The goal of the framework is to communicate ISRM information throughout the organisation in order to ensure due diligence and management of information security risks accordingly.

A top-down approach was followed in order to determine the components of the framework. The framework was developed from three different ISRM levels. The levels were corporate governance, tactical management and operational actions.

At corporate governance level a control set was developed from the King II report on corporate governance [KING 02] to determine what requirements are set at strategic level for information security in organisations. From these requirements several strategic/tactical level methodologies, approaches and guidelines were evaluated to determine which would meet the requirements. The single PO9 (Planning and Organisation 9) control objective of the CobiT Framework [COBI 00] was identified to directly address information security at strategic/tactical level. From this control, throughout the various CobiT products, numerous individual indicators were identified. An indicator is the set of related data that provides values for the specific framework component such as assets. The asset indicator will for instance provide data on the number and types of assets. These indicators were logically grouped to form the Bornman Framework for ISRM Methodology Evaluation (BFME) [BORN1 04] [BORN 04]. Corresponding scales were developed that could be applied to the BFME to evaluate which ISRM methodologies at operational and tactical level meet those requirements. It became evident that these lower level methodologies do not provide information that complies with the strategic level requirements [BORN 04].

The BFME is the precursor to the Bornman Framework for ISRM Information Communication (BFIC) [BORN1 04]. Where the BFME determines whether or not a framework can deliver on strategic requirements, the BFIC communicates the ISRM status to strategic management.

4 BORNMAN FRAMEWORK FOR ISRM INFORMATION COMMUNICATION (BFIC) TAXONOMY

Several indicators were identified from the Planning and Organisation Control number 9 (Assess Risks) of the Control Objective of Information and Related Technologies set of products [COBI 00]. From the different indicators it became clear that some of the recommended controls are in line with the generic risk management processes, actions and considerations that support specific processes, and actions that support the whole risk management programme. Subsequently the BFIC

was developed to provide information for the three different groupings of ISRM information. The identified indicators were grouped according to their function as indicated in Figure 1.

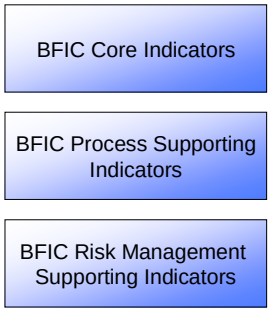

Figure 1: Indicator groupings

Each of the indicator groupings is discussed below.

4.1 BFIC Core Indicators

The Core Risk Management Indicators provide information about the risk management programme employed by the organisation. In total there are six functions, four of which consist of subindicators. In total there are 15 individual indicators that have been defined. Each of these indicators provides information of the risk management programme as required by corporate governance. In general these 15 Core Risk Management Indicators correspond to the processes of ISRM methodologies and approaches. An example of the information that is communicated is type and number of assets that have been considered during the risk determination phases.

4.2 BFIC Process Supporting Indicators

BFIC Process Supporting Indicators provide information specific to two groupings of the Core Risk Management Indicators. The two groupings that have Core Risk Management Supporting Indicators are Identification and Control. The purpose of these supporting indicators is to provide additional information about the generic risk management steps that is not required by corporate governance nor forms part of the generic risk management processes. An example would be the various considerations such as type and value of assets identified as part of the risk identification phase.

4.3 BFIC Risk Management Supporting Indicators

The BFIC Risk Management Supporting Indicators provide information about the supporting factors to the ISRM function. In particular, they provide information about the soft issues related to BFIC Core Risk Management Indicator functions and the BFIC Process Supporting Indicators. More importantly, this indicator grouping provides information specific to corporate governance's due diligence requirements. This grouping supports all the other indicators of the BFIC. An example is time frames associated with each of the risk management processes, since corporate governance recommendations specify annual reviews.

Each of the above groupings' indicators is discussed in more detail in the next section.

5 FRAMEWORK INDICATORS

The indicators that make up the Framework provide values that are specific to a function of the ISRM programme. Each of these indicators is discussed as part of their respective BFIC categories.

Figure 2 provides a graphical representation of the BFIC and clearly illustrates the three different indicator groupings and their related indicators. To the left of the numerous indicators are the labels indicating the three indicator groupings. At the top of the figure the BFIC core indicators are

displayed within their six subgroupings of indicators. In the middle of the diagram the indicators that support the BFIC Core Indicators are displayed, followed below them by the BFIC Risk Management Supporting Indicators.

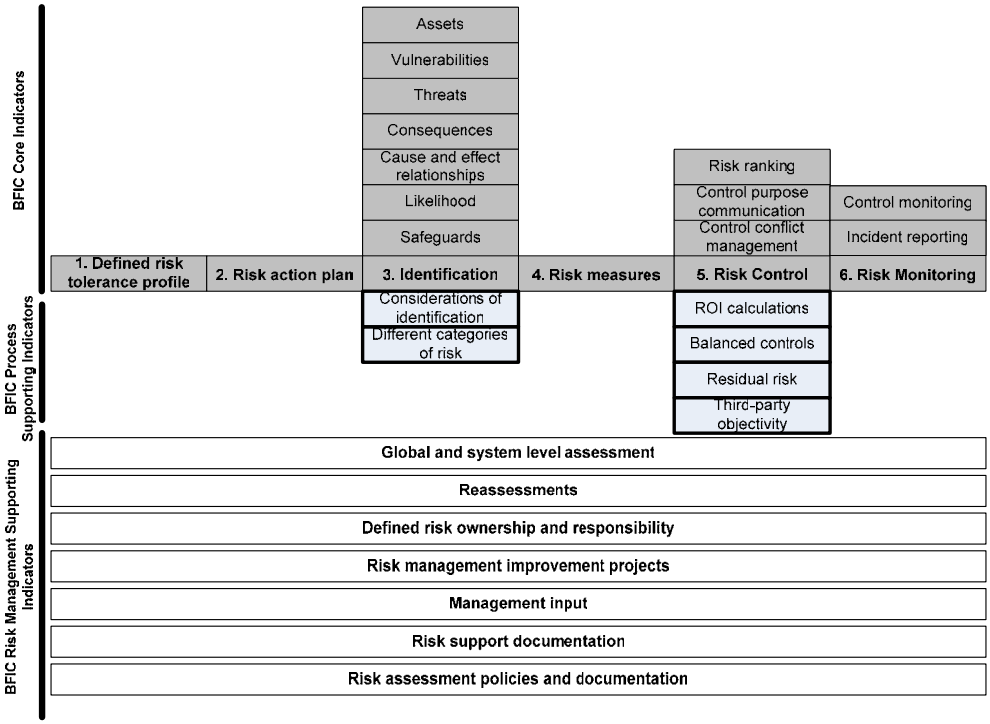

Figure 2: Bornman Framework for ISRM Information Communication

5.1 BFIC Core Risk Management Indicators

The first of the two initial indicators is the *Defined risk tolerance profile*. This profile provides an indication of the organisation's willingness to accept risk. Tolerance has to be defined by strategic management as it guides the overall risk management programme's direction. The second indicator is the *Risk action plan*; this plan outlines how risk will be addressed. The high level risks, priority, impact and related controls are displayed in this high level plan.

The remaining four indicators refer to subgroupings of processes and are in line with a generic risk management methodology [PELT 01] which is supported by several ISRM methodologies such as CRAMM [ALBE 03] [CRAM 96] , CORAS [IST 03][IST 03] and OCTAVE [ALBE 03]. The four generic risk management processes are *Identification*, *Risk measure*s, *Risk control* and *Risk monitoring* (see Figure 2).

The *Identification* grouping refers to the process of identifying the various components necessary to determine risk. The generic risk management process which most closely relates to the identification of risk is the *measurement* of the risk. The importance of assigning a comparative value to risk can never be overstated. The goal of this measurement indicator is to provide management with an indication of how risks are measured and the risk value per asset-threat relationship. This provides the user/reader with an indication of how the risks have been measured and how to interpret the findings.

The remaining two BFIC Core Risk Management Indicators are also closely related. They are the *Risk control* and *Risk monitoring* indicators. Once the risks have been identified, the most appropriate controls have to be selected for the risks that affect the organisation the most. There are numerous steps that pre-empt the final selection of the controls, for instance ensuring that controls do not counteract each other. The *Risk control* indicator is important as it conveys what controls have been put in place to address risks as well as what control selection processes were used to determine the most effective and efficient controls. Considering the investments organisations make

in the controlling of risks, monitoring the risk management programme as well as monitoring the effectiveness and efficiency of the implemented controls is paramount. *Monitoring* ensures a feedback loop where the effectiveness of controls is ensured. The indicator can also supply information of the progress of the selected control action, for instance how many controls should have been put in place offset by the number currently in place.

The goal of the BFIC Core Risk Management Indicators is to indicate the progress and findings of the generic risk management processes. However, it has been determined that two indicator groupings are supported by other actions/considerations. These considerations should also be communicated as part of the Framework.

5.2 BFIC Process Supporting Indicators

The BFIC Process Supporting Indicators as discussed in 4.2 provide information about the supporting components to the BFIC Core Risk Management Indicators. There are two groupings of Process Supporting Indicators; they support the Identification and Risk control process groupings.

5.2.1 Identification Supporting Indicators

There are two indicators that support the Identification Core Risk Management Indicators. Considerations of *Identification* are components that are soft issues regarding the identification of risks. These considerations usually form part of the methodology. Examples of considerations are business, technology and legal considerations.

Various categories can be taken into consideration when determining the actual risk on information. For instance, an organisation could store sensitive information that is required to be handled as confidential due to regulatory requirements. This requires that regulatory and legal risks be taken into account when determining and communicating the information security risks.

Considerations should not be confused with risk categories. Considerations take into account different environments and impacts, whereas risk categories use inputs from other risk management programmes, for instance financial or tax risks.

5.2.2 Control Supporting Indicators

The Control Supporting Indicator grouping consists of four separate indicators. These indicators provide additional information on how the controls were selected and how they are currently managed. These supporting indicators provide assurance to top management that the appropriate processes and actions were taken in the selection and implementation of the controls.

Control assurance is provided through the four Control Supporting Indicators, which provides information on the control efficiency, for instance return on investment (or similar) calculations. These types of calculations provide assurance that the most efficient controls were selected. The Balanced Controls Indicator provides a breakdown of the different types of controls. CobiT recommends that four different types of control be implemented. These different types of control should be preventative, detective, corrective and recovery. The indicator provides assurance that if any of the controls fail; the other controls will ensure that the risk is not as severe as an unbalanced control.

The purpose of risk management is not to eliminate risk but to minimise it to an acceptable level [CONR 03]. Management wants to know what risk remains after controls have been put in place. The *Residual Risk* Indicator provides management with an idea of the actions that should be taken to reduce risks even further or over the control of risk. A clear and important indicator should be the third-party objectivity of risk management actions. The risk action plan dictates what actions should be taken and the organisation has to implement this. However, CobiT recommends that management have complete assurance of the actions, processes, controls and implementations that should be in place. Third-party objectivity, their roles and responsibilities will provide the final confirmation that risks are controlled as they are intended to be.

These two indicator groupings provide information for two BFIC Core Risk Management Indicator groupings, but some factors have been identified that even support the BFIC Process Supporting Indicators. These are discussed in the next section.

5.3 BFIC Risk Management Supporting Indicators

The BFIC Risk Management Supporting Indicators are very involved indicators. They support each indicator of the BFIC Core Risk Management and BFIC Process Supporting Indicators. They provide supporting information not only to the other two groupings of indicators, but also to each other. Each BFIC Risk Management Supporting Indicator provides supporting information to the other BFIC Risk Management Supporting Indicators. Overall the BFIC Risk Management Supporting Indicators are predominantly targeted at due diligence information. The cross-supporting nature of the BFIC Risk Management Supporting Indicators has not been investigated as this would involve superfluous information that would not support the nature of the Framework for effective and efficient communication.

There are seven BFIC Risk Management Supporting Indicators. These indicators address issues that show responsibility and ownership, as well as general high level information about each of the indicators. Each of the seven indicators is briefly discussed:

- Global and System Level Assessment – This indicator provides information about the scope of the risk management programme. Global refers to the macro environment that can have an impact on the information security, while system level refers only to the isolated system.
- Reassessments – Considering the fact that information technology is constantly changing and that new risks are introduced on a daily basis, the reassessments provide status indicators of the latest risk management information. If the reassessments have not been conducted in a decent time frame, the reliance on the indicators is brought into doubt.
- Defined Risk Ownership and Responsibility – The board and management of organisations are being held more accountable for their actions. This indicator provides information on the business owner and the ultimate responsibility for ensuring that the risk management action is executed.
- Risk Management Improvement Projects – As the IT environment evolves, so to should the processes to manage the risks. This indicator provides information on current and future projects to better identify, measure, control or monitor risks.
- Management Input – Management usually has a holistic view of processes and actions within the organisation, be it at strategic, tactical or operational level. This indicator provides information on the participation of management in the management of risks.
- Risk Support Documentation – Risk should be based on realistic evidence. This evidence can be based on system logs, security studies or vulnerability alerts. This indicator provides information on what supporting documentation was used in the various steps of the ISRM programme.
- Risk Assessment Policies and Procedures Documentation – Risk management has to be conducted according to a set structure or plan; something that has been proven by a magnitude of methodologies and approaches. This indicator provides information on the policies and procedures related to the approach that was followed.

In this section the various indicators of the BFIC were discussed. These indicators on their own do not clearly provide a framework on how to communicate risks. Figure 3 provides a graphical representation of how the Framework can be used to communicate ISRM action from operational level to strategic level. The figure also indicates how the Framework can be used to

communicate the strategic actions through the Framework to the tactical and operational levels of the organisation. Tactical and operational levels provide input for the Framework. While the Framework is being populated, strategic management can communicate requirements based on the indicators to the lower managerial levels.

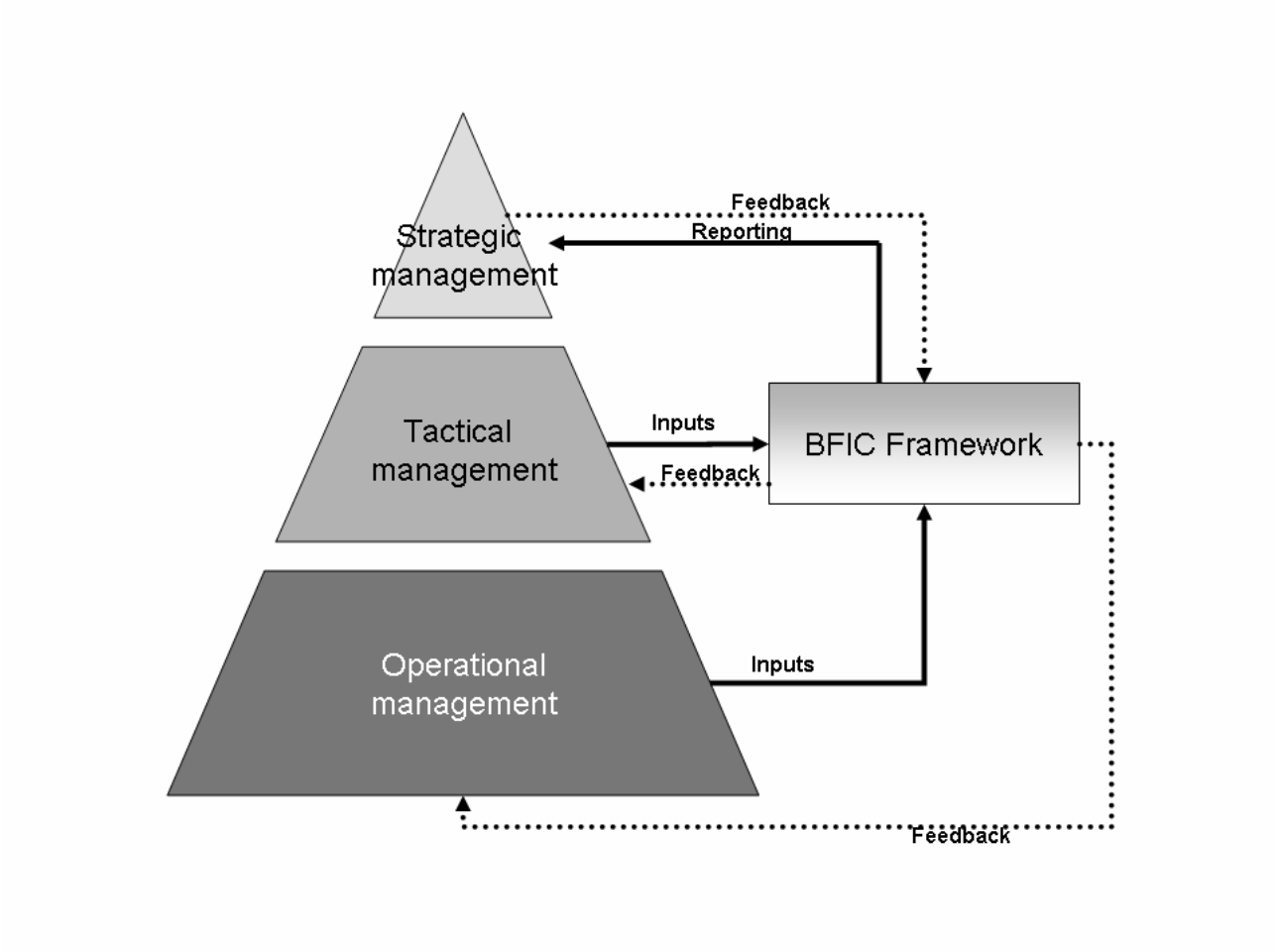

Figure 3: Framework use in relation to generic managerial levels

The next section discusses how the Framework should be used in combination with processes to communicate ISRM information.

6 FRAMEWORK PROCESSES

Although the Framework has logical indicators that facilitate quick and easy ISRM information communication, there are processes that should be followed in order to make the Framework function. There are three steps that should be completed in a specific order as indicated in Figure 4.

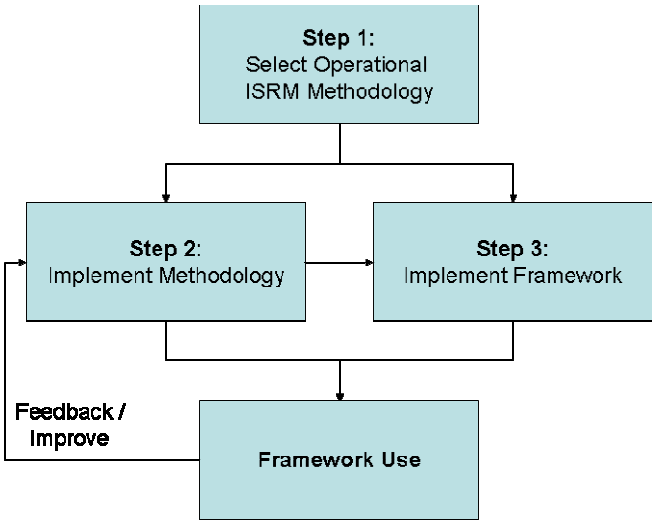

Figure 4: BFIC Implementation Process

The first step is to select an appropriate ISRM methodology or approach that can be implemented at operational level. This methodology will have to be able to provide sufficient ISRM information required by strategic management. The Bornman Framework for ISRM Methodology Evaluation can be used [BORN 04] for this purpose.

Steps 2 and 3 should be considered as linked. While the selected methodology is implemented, processes should be put in place to enable the risk management information produced by the methodology to be transferred to the Framework indicators. The rationale behind splitting the two processes is that organisations that have already implemented an ISRM methodology can link their outputs to the Framework's indicators.

Once the ISRM methodology has been implemented along with the linkages to the Framework, the Framework indicates the status of the ISRM programme. The indicators can provide information on how to better implement the ISRM methodology or improve the linkages to the Framework.

The Framework has numerous advantages and some shortcomings. The next section highlights these advantages and shortcomings.

7 FRAMEWORK EVALUATION

The Framework was constructed with multiple ISRM methodologies and approaches in mind. It does not prescribe a specific ISRM methodology to be followed in order to obtain valuable information security information. This methodology independence is not only at operational level but at all managerial levels.

Due to the relatively independent nature of the indicators, organisations can implement the Framework at any business level, for instance division, subsidiary or business unit, or provide a holistic view of information security risks in the organisation.

The Framework has three groupings of indicators that provide specific information to strategic management. It provides information about the processes that are used and the components that are taken into consideration. The most valuable information, though, is the BFIC Risk Management Supporting Indicators that provide due diligence information.

One of the biggest advantages of using this Framework is the fact that the Framework is entirely based on best practice methodologies, frameworks, approaches, standards and guidelines. The indicators have been proven to address all of the King II requirements of risk management controls [BORN1 04].

Although there are numerous advantages to the Framework, there are also some shortcomings. The Framework has not yet been proven in a real-world environment. However, a software prototype was developed that allows for the viewing of ISRM information in the structure and indicators of the BFIC. This Framework was based on the CORAS methodology [IST 03] which enabled the use of an open-source XML based database [EXIS 04]. Through the use of Microsoft .Net framework [MICR 04] the information was communicated in terms of the Framework.

The Framework requires the ISRM methodology that is implemented in an organisation to provide sufficient risk management information to populate the Framework. If the methodology is not software-based or the stored information is unobtainable, the processes involved in populating the Framework will be counterproductive. Therefore, it is necessary for organisations wanting to implement the Framework to evaluate their methodology utilising the BFME [BORN 04].

8 CONCLUSION

Organisations have been made aware by corporate governance recommendations that the IT risks have to be managed within any organisation. This has led organisations to select methodologies without taking into consideration the communication of technical risks to strategic management. The Bornman Framework for ISRM Information Communication discussed in this article provides management with a structured approach to communicate the information security risk management information. The structure provides management with a communication framework of risk information not only to strategic management, but to the tactical and operational levels of the organisation as well. The BFIC is a bilateral communication framework.

BFIC provides a holistic view of all the ISRM components that are recommended by corporate governance best practice. The Framework provides indicators for the qualitative and quantitative, hard and soft issues related to ISRM. It allows for the integration of the strategic, tactical and operational ISRM principles to merge with a common goal in mind, namely to manage the risks of information security more effectively and efficiently and most importantly holistically within the organisation.

The Framework is a set of grouped components that allow for communicating all information security risk related information. Metrics can be applied to these components that can facilitate bilateral communication within any organisation. The Framework is structured so that it can be implemented in any size organisation by applying it in divisions or business units and consolidating results for an overall risk view. The practical implementation of the Framework has been proven in a software prototype which enables more effective consolidation of ISRM information.

The goal of the Framework was met by achieving four objectives. The objectives were to assist in communicating ISRM information, provide an overview of the organisation's ISRM status, provide an overview of roles, responsibilities and accountability, and indicate what actions are taken in the organisation to meet ISRM requirements.

9 REFERENCES

[ALBE 03] Alberts C., Dorofee A.; 2003; *Managing Information Security Risks – The OCTAVE℠ Approach.* Pearson Education. ISBN: 0- 321-11886-3.

[BORN 04] Bornman W.G., Labuschagne L.; 2004; *A Comparative Framework for Evaluating Information Security Risk Management Methodologies.* Conference proceedings of the 4th annual Information Security South Africa held in Midrand, South Africa.

[BORN1 04] Bornman W.G., Labuschagne L; 2004; *Information Security Risk Management: A Comparative Framework;* University of Johannesburg. MCom Dissertation.

[COBI 00] IT Governance Institute; 2000; *CobiT 3rd Edition – Framework;* Information Systems Audit and Control Foundation; ISBN: 1-893209-14-8.

[COSO] The Committee of Sponsoring Organizations of the Treadway Commission; d.u.; *Enterprise Risk Management Framework – Executive Summary (Draft);* Available from http://www.erm.coso.org.

[CONR 03] Conrow E.H.; 2003; *Effective Risk Management: Some Keys to Success.* American Institute of Aeronautics and Astronautics. ISBN: 1-56347-581-2.

[CRAM 96] CCTA – The Central Computer and Telecommunication Agency; 1996; *CRAMM Management Guide*. Crown Copyright.

[CRAM 03] Insight Consulting - CRAMM Methodology; Available from http://www.cramm.com; Accessed 31 March 2003.

[EXIS 04] Exist-db.org; 2004; *eXist Open Source XML Database;* Available from http://exist.sourceforge.net/; Accessed 29 July 2004.

[INCA 99] The Institute of Chartered Accountants in England and Wales; 1999; Internal Control – Guidance for Directors on the Combined Code; ISBN: 1-84152-010-1.

[IST 03] Information Society Technologies (IST) Programme; 2003; *The CORAS methodology for Model-Based Risk Assessment – Platform Documentation;* Platform available from http://coras.sourceforge.net.

[KING 02] King Committee on Corporate Governance; 2002; *King Report on Corporate Governance for South Africa;* Institute of Directors. ISBN: 0-620-28851-5.

[MICR 04] Microsoft; 2004; *Microsoft .Net;* Available from: http://www.microsoft.com/net/; Accessed 29 July 2004.

[OXFO 80] Oxford University Press; 1980; *The Oxford Illustrated Dictionary;* Book Club Associates London.

[PELT 01] Peltier, T.R.; 2001; *Information Security Risk Analysis;* Auerbach; ISBN: 0-8493-0880.

[SABS 00] South African Bureau of Standards (SABS); 2000; *Information Technology – Code of Practice for Information Technology Risk Management, SABS ISO/IEC 17799*. ISBN: 0-626-12835-8.

[SOX 02] Senate and House of Representatives of the United States of America; 2002; *Sarbanes-Oxley Act of 2002;* H.R. 3763.

[TUDO 01] Tudor J.K.; 2001; *Information Security Architecture – An Integrated Approach to Security in the Organisation.* CRC Press. ISBN: 0-8493-9988-2.