A FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODOLOGIES FOR SMMEs

[1]L van Niekerk **[2]L Labuschagne**

Academy for Information Technology, University of Johannesburg, South Africa

[1]lieslv@netsurit.com [2]ll@na.rau.ac.za

+27 11 489-2847

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

ABSTRACT

The South African economy has grown considerably in the last 10 years, with black empowerment being supported by the state and investors to develop previously disadvantaged communities. Government has also targeted small, medium and micro enterprises (SMMEs) for development.

SMMEs are not directly affected by corporate or IT governance, and as a result 80% of SMME failures are attributed to lack of management knowledge. This lack of knowledge extends to the management of information security risk.

This article evaluates information security risk management methodologies available to international small businesses for fit to the South African SMME to discover whether they may be used to reduce the failure rate. The evaluation framework provides a tool that may forewarn the lack of fit of a methodology.

KEYWORDS

Information security risk management; SMME; small business; OCTAVE-S; CRAMM V Express

A FRAMEWORK FOR EVALUATING INFORMATION SECURITY RISK MANAGEMENT METHODOLOGIES FOR SMMEs

1 INTRODUCTION

Small, medium and micro enterprises (SMMEs) form a sizable portion of the gross domestic product (GDP) in South Africa. The SMME market portion contributes 42% to the GDP [South Africa, Business Guidebook], but comprises an estimated 99% of the total number of enterprises in the economy [National Treasury].

The information security risk management (ISRM) methodologies commercially available to SMMEs were created in developed countries, and for different types of small businesses to that of the South African SMME. These methodologies require evaluation for a South African SMME before they can be recommended as an organisational improvement tool.

This article presents the creation of a framework for this evaluation, and the subsequent evaluation of two internationally available methodologies for small businesses.

The framework was created considering the requirements of corporate governance and IT governance, as well as the constraints experienced by SMMEs, time and resources.

The article first presents the framework, followed by a summary of the methodologies of OCTAVE-S and CRAMM V Express. Each are evaluated using the framework before a conclusion is drawn.

2 FRAMEWORK FOR THE EVALUATION OF ISRM METHODOLOGIES

The framework has been created out of the characteristics of an SMME, as well the benchmark of procedural order required by corporate and IT governance. The characteristics were devised from the most pertinent constraints faced by the SMME, being cost, resources and business knowledge.

Corporate and IT governance both require a process including planning, execution and control or monitoring of risk management as a cyclical process [King Commission on Corporate Governance; IT Governance Institute]. This creates continual awareness of risk, and the management thereof.

A further requirement is the fit of the methodology to the definition of the South African SMME, as it is unique compared to that of other countries. These requirements, coupled with the constraints mentioned above, create the major elements of the framework.

2.1 The Framework Explained

The framework in figure 1 that has been created for evaluation of SMME methodologies is three-dimensional, comprising the following:

Dimension 1. Elements. There are 4 elements in the framework: availability, cost, regulatory fit and SMME fit.

Dimension 2. Factors. The elements consist of factors, and in some cases, sub-factors. The constraints and requirements mentioned above are multi-faceted and cannot be represented fairly in one dimension.

Dimension 3. Weights. All of the elements and factors have associated quantifiable weights assigned. The weights create a quantitative measure for the framework, allowing comparisons of methodologies after evaluation.

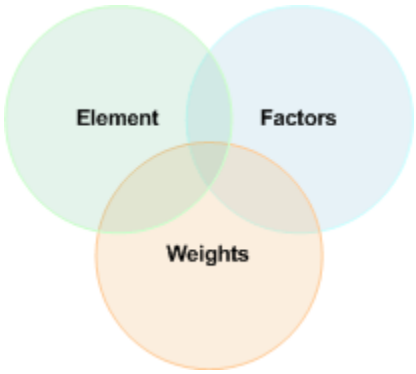

Figure 1: The three-dimensional framework

The elements based on the constraints faced by an SMME and the requirements of corporate and IT governance are:

2.1.1 Visibility

Visibility pertains to the ease with which the ISRM approach may be obtained, specifically by an SMME. This includes whether the full methodology is obtainable with ease, or whether only promotional material is available. The objective of visibility is to measure whether the interested party within the SMME can reasonably obtain an understanding of the methodology and thus make an informed decision of whether to proceed with the ISRM methodology.

2.1.2 Cost

The cost of implementing the methodology is an estimated measure, as the true cost of any exercise can only be determined after the fact. Cost is, however, a relative term, as there are many facets to a methodology that may be added as a cost, even though no direct spending was involved. Cost is therefore split into these factors:

- Purchase cost is the requirement of cash spend on the methodology, whether it is an upfront cost, or expenditure throughout the methodology for obtaining the methodology.
- Organisational involvement is attributable to the human resources involved in the methodology, through various channels. These channels, known as sub-factors, are:

- Knowledge requirement. All training required by the organisation, or elected individuals.
- Senior management buy-in. The involvement of senior management in a methodology is an expensive factor, as senior management time is at a higher premium than an operational employee's.
- Self-directed or consulted. The nature of the methodology also impacts the cost of the implementation. A self-directed approach may be higher in organisational involvement cost, but lower in purchase cost. The inverse applies to a consulted approach. The purchase cost may be higher, but organisational involvement is less. The duration of the methodology, as prescribed by the nature of the methodology, must also be considered.

  The duration of a consulted approach may be shorter, as the schedule is managed by a third party. The duration of a self-directed approach is self-led, and thus may be prone to operational delays.

2.1.3 Regulatory Fit

The regulatory fit refers to the process being of a cyclical nature and including both planning and monitoring phases. This would create fit to the corporate and IT governance standards of King II and CobiT, respectively [King Commission on Corporate Governance; IT Governance Institute].

2.1.4 Fit to the South African SMME

The South African SMME has been determined to be unique when compared to 5 other nations' definitions, and this should be considered before implementing a methodology created for the SMME of a different nation.

The fit to the South African SMME is evaluated contrariwise against the following factors:

- Horizontal or vertical industry. The methodology should not promote or be aligned with a horizontal or vertical industry. There should be no restriction on the industry of the SMME.
- The size of organisation. The South African SMME is defined as ranging from 1 staff member to 200 [South Africa]. The methodology should not be focused on a number excluding parameters of this range.
- The type of organisation. Any structure of small businesses should be allowed, especially when considering the existing lack of business skills. There should be no restriction on structure.

To summarise, the only restriction that is endorsed is the maximum allowance of 200 employees.

The framework is summarised in figure 2.

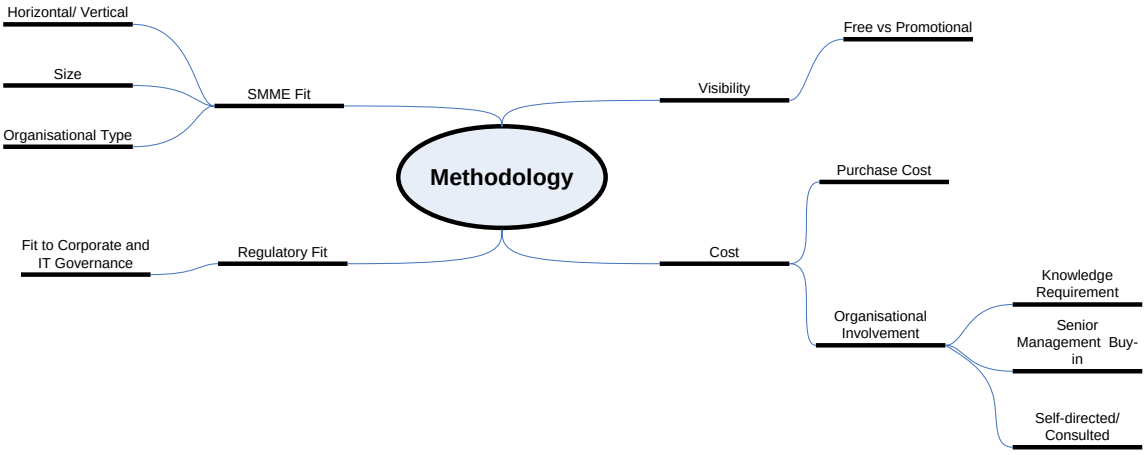

Figure 2: The framework, its elements and factors

The framework has thus far been explained in two dimensions. The third dimension, the weighting, is assigned as follows.

2.2 The Weighted Dimension

Weights have been assigned to each element, factor and sub-factor. The weights have been assigned, based on estimated importance of the element.

Cost has been assigned the highest weight due to the cost-focus of SMME's. A high purchase cost alone, could dissuade the SMME owner or decision maker from implementing a methodology. However, cost is not the only consideration. Lack of SMME or regulatory fit will result in a very low return on investment, even though the cost is low.

Visibility also carries a great importance. The remaining weights become of no consequence if the decision maker cannot obtain an initial understanding of the methodology. Avoidance of visibility would create a 'blind' implementation of the methodology.

The remaining weights are also go/ no-go weights. If the methodology scores low on SMME and regulatory fit, the organisation can be assured that, for their enterprise, it will not be the optimum solution. A score of zero in both are immediate dismissals.

As the result of these arguments, the highest weight is assigned to cost, as the primary concern for the SMME owner, with equal distribution of weight over the remaining elements.

The total of the weights when added will provide a score out of 100. This is then easily compared to other evaluations for decision making. Should two options score equally, the elements themselves should be compared, using go/ no-go decision blocks.

Tables 1-4 present the elements, factors and sub-factors with their assigned weights. A description of the assigning of weights for each factor is provided, creating guidance for quantification. Each elemental table has a decision point. All decision points are also highlighted, providing the evaluator with the option to dismiss a methodology. The score for the element is calculated by selecting the rule (rules are in *Italic* font) in the table with best fit to the methodology, and adding the rule weights for an element score.

The final decision is based on a framework score higher than a reasonably conservative 30.

Table 1: The weights of visibility

Element, factors and sub-factors		**Assigned weight**
Visibility		**20**
The methodology is freely available and user-friendly	*20*	
Promotional information is freely available with details for further information	*10*	
No information is freely available	*0*	
SCORE		**____**
GO/NO GO DECISION – HIGH RISK OF FUTILE IMPLEMENTATION		

Table 2: The weights of cost

Element, factors and sub-factors		**Assigned weight**
Cost		**40**
Purchase cost		20
The methodology is free	*15*	
The methodology is free but has a tool that reduces organisational involvement available at a cost	*5*	
The methodology has a cost attributed	*0*	
The methodology has a cost attributed that includes a tool that reduces organisational involvement	*5*	
Organisational involvement		20
Knowledge requirement		5
The organisation is expected to already have all knowledge required for the methodology	*0*	
There is training available for the organisation at a cost	*5*	
No previous knowledge is required	*5*	
Senior management buy-in		5
The methodology promotes senior management buy-in or sponsorship	*5*	
The methodology requires senior management execution	*0*	
The methodology does not promote or require senior management buy-in	*0*	
Self-directed or consulted		10
The methodology is self-directed	*5*	
The methodology is self-directed with consulting available	*10*	
The methodology is consulting based with no operational involvement from the organisation	*5*	
SCORE		**____**
GO/NO GO DECISION: IS THE COST TOO HIGH?		

Table 3: The weights of regulatory fit

Element, factors and sub-factors		**Assigned weight**
Regulatory fit		**20**
The methodology conforms to the steps in table 2	*10*	
The methodology does not conform to the steps in table 2, but does include at least planning and arranging	*5*	
The methodology does not conform to the steps in table 2 at all	*0*	
The methodology is cyclical and promotes reviewing	*10*	
The methodology is not cyclical and does not promote reviewing	*0*	
SCORE		**_____**
GO/NO GO DECISION: HIGH RISK OF ANTI-REGULATORY SOLUTION		

Table 4: The weights of SMME fit, the final score

SMME fit		**20**
Horizontal/vertical		5
The methodology is restricted to a horizontal or vertical industry	*0*	
The methodology is not restricted to any industry	*5*	
Size		10
The methodology restricts the size of the organisation to a range within the parameters of the South African SMME	*0*	
The methodology is restricted to the parameters of the South African SMME	*10*	
Organisational type		5
The methodology is restricted to a specific type of organisation, e.g. hierarchical structure	*0*	
The methodology is not restricted to a specific type of organisation	*5*	
SCORE		**_____**
GO/NO GO DECISION: HIGH RISK OF INAPPROPRIATE SOLUTION		
TOTAL SCORE		**100**
GO/NO GO DECISION: IS THE SCORE HIGHER THAN 30?		

The framework has been established in all three dimensions. The following section uses the framework to evaluate the OCTAVE-S Information Security Risk Management methodology.

3 OCTAVE-S EVALUATED

OCTAVE-S is discussed in summary to create the foundation from which information is extracted for the framework evaluation that follows later. OCTAVE-S is based on the OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) Approach [Alberts & Dorofee] designed specifically for the unique constraints experienced by small organisations [Software Engineering Institute]. OCTAVE-S was developed by the Technology Insertion, Demonstration and Evaluation program of the Software Engineering Institute (SEI).

The framework of OCTAVE was retained, with simplified implementation of the detail. OCTAVE-S v0.9 is summarised below and subsequently evaluated.

3.1 OCTAVE-S Summarised

OCTAVE-S is a self-directed information security risk evaluation. It requires a 3- to 5-member interdisciplinary team to lead the methodology, and also requires that these staff members have a broad insight into the organisation's business and security processes. The ultimate outcome of the methodology is an organisation-wide protection strategy and risk mitigation plans.

The OCTAVE-S approach is divided into three phases. These phases are:

1. Build asset-based threat profiles
2. Identify infrastructure vulnerabilities
3. Develop security strategy and plans

3.1.1 Build Asset-based Threat Profiles

The team uses this phase to create a set of criteria against which risks will later be evaluated. All organisational assets are identified and the existing security practice is defined. No external consulting is offered in this phase, as all operational tasks are completed by the team itself.

A selection process is used to select 3 to 5 critical assets, on which the remainder of the evaluation will be conducted.

Finally, security requirements are defined, and threat profiles created for each critical asset. The threat profile is based on 3 levels: the asset, followed by all connected aspects that may expose a threat and the outcomes if the threat is realised.

3.1.2 Identify Infrastructure Vulnerabilities

The team analyses the computing infrastructure in this phase, focusing on the access means to the critical assets, for example systems and data. The team also analyses which parties are responsible for the maintenance of these assets, in many cases with small businesses, an outsourced party.

3.1.3 Develop Security Strategy and Plans

This phase requires the team to identify risks to the critical assets and what may be done to mitigate these risks. Risks are measured on a qualitative scale of high, medium or low. All this information is collated into a protection strategy for the organisation's critical assets, and mitigation plans to reduce the risks. The worksheets provided are a structured benchmark for creating these plans. No expectation of when these plans are executed is provided.

3.1.4 Scope of Application

OCTAVE-S is aimed at organisations ranging from 20 to 80 staff members. This excludes the majority of South African SMMEs (91%). The organisational structure is flat, with people from different departments being accustomed to interdepartmental projects.

An organisation such as this is expected to be able to assign 3 to 5 people that have broad knowledge of the organisation and its security practices.

OCTAVE-S is not recommended for an organisation that cannot create a team of knowledgeable staff members, for example an organisation that consists of independent business units, or dispersed groups of staff that do not interact much.

The team members are expected to have problem-solving abilities, analytical skills, teamwork ethic and time, described as a few days. It is not indicated whether the few days are full days, or the total of various short sessions.

3.1.5 Preparation Guidelines

OCTAVE-S provides a module containing all preparation activities that are suggested before kicking off the methodology.

- The first notable preparation is senior management sponsorship. OCTAVE-S makes it very clear that senior management sponsorship is vital, but cannot clearly define how to obtain it.
- The next preparation activity is selection and training of the team. The team should be made up of individuals with the skills listed above, containing at least one leader in the group, and a staff member with close links to IT, either through working closely with IT, or the third-party provider.
- The use of managers on the team is encouraged, but managers should not be the majority of the team as this may restrict open communication.
- Training of the team is addressed by promoting the training of at least one team member on OCTAVE-S.
- Setting the scope of the evaluation allows the team to identify which areas of the organisation will be evaluated. A subset of the organisation's business units may be selected. OCTAVE-S recommends at least 4 business units, one of which must be the IT department or IT management department.
- The schedule for the methodology is created next. Worksheets are provided to offer guidelines of workshop durations, depending on the experience of the team. The duration of the methodology in phases ranges as follows:

Table 5: Duration of OCTAVE-S

Phase	From	To
Preparation	4 days	8 days, 4 hours
Build asset-based threat profiles	1 day	2 days, 6 hours
Identify infrastructure vulnerabilities	3 hours	1 day
Develop security strategy and plan	1 day	5 days, 1 hour
Total	**6 days, 3 hours**	**17 days, 3 hours**

The worksheets also provide a checklist at each process to ensure that all steps have been completed. Guidance is also provided on managing logistics for all workshops.

3.1.6 Implementation Guidelines

OCTAVE-S provides a set of guidelines for each process in each phase with step-by-step instructions of what information is to be gathered and which worksheet is to be completed as well as definitions of any terminology used.

3.2 OCTAVE-S Evaluation Outcomes

The evaluation of OCTAVE-S based on the implementation guide is presented in the table below.

Table 6: OCTAVE-S framework evaluation

Elements, factors and sub-factors	Score achieved
Visibility	**20**
OCTAVE-S is freely available online and is easy to understand	20
SCORE	**20**
Cost	**40**
Purchase cost	
OCTAVE-S is available at no cost	15
Vulnerability tools may be obtained at a cost but are not required	5
Organisational involvement	
There is training available for the organisation at a cost	5
OCTAVE-S requires senior management buy-in or sponsorship	5
OCTAVE-S is self-directed	5
SCORE	**35**
Regulatory fit	**20**
OCTAVE-S does include at least planning and arranging	5
SCORE	**5**
GO/NO GO DECISION: HIGH RISK OF ANTI-REGULATORY SOLUTION	
SMME fit	**20**
Horizontal/vertical	
OCTAVE-S is not restricted to any industry	5
Size	
OCTAVE-S restricts the size of the organisation to 20 to 80 staff members	*0*
Organisational type	
OCTAVE-S restricts the organisation to a flat hierarchy with more than 4 business units	*0*
SCORE	**5**
GO/NO GO DECISION: HIGH RISK OF INAPPROPRIATE SOLUTION	
TOTAL	**65**

OCTAVE-S achieves an average score on total, but ranks very low in the regulatory and SMME fit elements. It is a high risk methodology for ISRM.

4 CRAMM V EXPRESS EVALUATED

CRAMM V Express is discussed in summary to create the foundation from which information is extracted for the framework evaluation that follows later. CRAMM V Express [Insight Consulting], similar to OCTAVE-S, is based on the large organisation version CRAMM V Expert. The software has been developed by Insight Consulting based on the CRAMM methodology.

CRAMM V Express is a tool for rapid yet effective risk assessments that require limited time and human resources.

4.1 The CRAMM V Express Tool

The tool follows a very simple process for assessing the risks facing an organisation's systems, and proposing mitigating controls, or as CRAMM describes them, countermeasures to reduce the risk.

The tool presents user-friendly screens that allow input from a single user, with reporting available for review. The process followed by the tool is presented in figure 3.

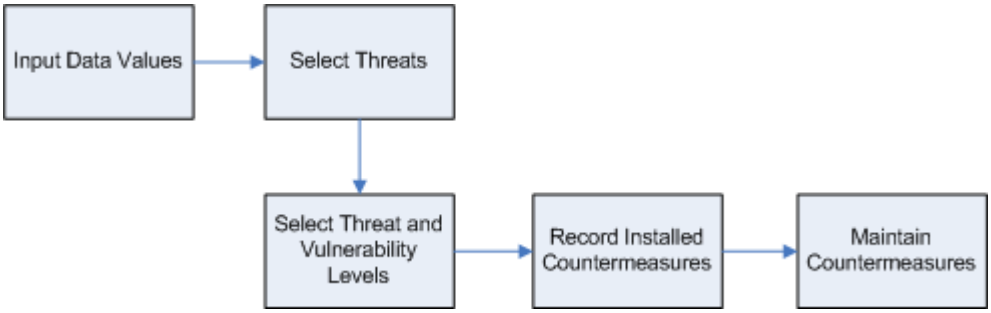

Figure 3: The CRAMM V Express process

4.1.1 Scope of Application

The tool may be used for any system; there is, however, no distinction of which systems should be assessed. There is also no promotion of an organisation-wide assessment or assessment on departments or business units only.

There is no guidance offered regarding who is responsible for managing the assessment, for example who is required to enter the information, and who is responsible for ensuring that the mitigating controls are applied.

The tool does not offer any training on identifying threats, vulnerabilities etc., or assessing the level of vulnerability once the risk has been identified. The tool assumes that the user is knowledgeable of this specialist information, but still requires a tool to present the countermeasures.

4.1.2 Preparation

The tool itself does not require any preparation, but does assume that the user is aware of all systems that should be entered into the tool. The onus lies on the user to nominate which systems are to be assessed, and gain the assessment skill beforehand as well.

4.1.3 Implementation

Implementation of CRAMM V Express does not take place *per se*, as the use of the tool takes very little time, but no guidance is offered on when or how the proposed mitigating controls are to be implemented. The onus again lies on the user to make those decisions.

4.1.4 Cost

The CRAMM V Express tool is available at a cost of £1 500,00 excluding tax, with an additional annual licensing fee of £250,00. In rands, this translates to a purchase cost of R17 205,00 excluding taxes, and R2 867,50 per year (calculated at the current exchange rate of R11,47 per British pound).

This is not an extremely large sum of money, but may be contested if the tool is not used to its full potential. It is, however, fast to use and has low cost in organisational involvement.

4.2 CRAMM V Express Evaluation Outcomes

The evaluation of CRAMM V Express based on the implementation guide is presented in the table below.

Table 7: CRAMM V Express framework evaluation

Elements, factors and sub-factors	Score achieved
Visibility	**20**
Promotional information is freely available with details for further information	10
SCORE	**10**
Cost	**40**
Purchase cost	
CRAMM V Express has a cost attributed that includes a tool that reduces organisational involvement	5
Organisational involvement	
The organisation is expected to already have all knowledge required for the methodology	*0*
The methodology does not promote or require senior management buy-in	0
The methodology is self-directed	5
SCORE	**10**
GO/NO GO DECISION: IS THE COST TOO HIGH?	
Regulatory fit	**20**
CRAMM V Express promotes reviewing by offering a record of countermeasures used and still to be implemented	10
SCORE	**10**
SMME fit	**20**
Horizontal/vertical	
The CRAMM V Express is not restricted to any industry	5
Size	
CRAMM V Express has no restrictions on organisational size at all	10
Organisational type	
CRAMM V Express is not restricted to a specific type of organisation	5
SCORE	**20**
TOTAL	**50**

CRAMM V Express scores below average and fails in the cost element. This is surprising as very little organisational involvement is required, although a purchase cost is attributed. The double edge of the sword is the lack of a requirement of senior management involvement. This has been stipulated by King II as vital, as well as CobiT, which also supports the low regulatory score. The high score in SMME fit is inconclusive, as CRAMM V Express does not specifically cater for small businesses, nor does it exclude them.

The inference has to be made that although the above approaches may offer some benefits to a South African SMME, there are risks that they become difficult to apply and are abandoned before completion. There is no support available for either of these approaches should the organisation grow weary of self-direction.

5 CONCLUSION

This article has presented a framework that may be used to evaluate any methodology by an SMME concerned with information security risk management. The framework focuses its greatest weight on the cost concern of the SMME, but also considers the visibility of the methodology, fit to the South African structure of an SMME, and fit to the regulations of the South African environment.

The framework was applied to OCTAVE-S and CRAMM V Express. The framework has found that neither of these approaches is ideal for the South African SMME, with mediocre scores of 65% and 50%, respectively.

The framework has provided a weapon in the SMME's armoury for forewarning inappropriate implementation of a methodology that may cost the organisation resources it cannot afford, or provide a solution it cannot use.

An outcome of these evaluations was the realisation that a new, South African SMME-based information security risk management methodology needs to be developed that scores high on the evaluation framework, and thus meets all the requirements of an SMME.

It is however acknowledged that the framework is experimental and has not been tested on all information security risk management methodologies for small businesses and that further research into methodologies is planned for the future. Further research is also planned into the abovementioned creation of the methodology for the South African SMME.

6 REFERENCES

1. South Africa. 2003. *South Africa Business Guidebook 2002/2003*. Writestuff Publishing.
2. National Treasury. 2002. *The Relative Importance of SME's in the South African Economy: An Analysis of Issues and Quantification of Magnitudes*.
3. Dispatch Online. 2003. *SMME's failure blamed on poor management.* http://www.dispatchonline.co.za.
4. King Commission on Corporate Governance. *King Report of Corporate Governance for South Africa – 2002*.
5. IT Governance Institute. 2000. *CobiT Framework 3rd edition 2000*.
6. South Africa. 2003. *National Small Business Amendment Act 2003.* Government Printer.
7. Alberts, CJ & Dorofee, AJ. June 2002. *Managing Information Security Risks. The OCTAVE Approach*. Pearson Education Limited.
8. Software Engineering Institute. 2003. *OCTAVE-S Implementation Guide Version 9.0; Volume 1: Introduction to OCTAVE-S.*
9. Software Engineering Institute. 2003. *OCTAVE-S Implementation Guide Version 9.0; Volume 2: Preparation Guidance.*
10. Software Engineering Institute. 2003. *OCTAVE-S Implementation Guide Version 9.0; Volume 3: Method Guidelines.*
11. Insight Consulting. 2004. *CRAMM V Express Walkthrough Flash Presentation.* http://www.insight.co.uk.