THE PECULIUM MODEL:

INFORMATION SECURITY RISK MANAGEMENT FOR THE SOUTH AFRICAN SMME

Liesl van Niekerk
University of Johannesburg, South Africa
liesl.vanniekerk@kpmg.co.za

Les Labuschagne
University of Johannesburg, South Africa
leslabu@twr.ac.za

ABSTRACT

Small, medium and micro enterprises (SMMEs) in South Africa contribute over 40% to the gross domestic product. However, these organisations have a failure rate of 80%, mostly due to a lack of management skills. SMMEs also do not aspire to corporate governance standards for these management skills due to the lack of awareness of corporate governance best practice as well as the non-enforced implementation of King II by SMMEs. Risk management, as a component of King II, is consequently also optional, thus creating a lack of enforced information security risk management.

The Peculium Model has been created for the small business environment in South Africa, specifically for the analysis and management of information security risks.

The model is based on a framework derived from the examination of the risk management component of King II, CobiT for control of risk management, OCTAVE for asset-based risk management, CRAMM for monitoring of risk mitigation and ISO 17799 for cyclical risk management.

The composition of the model allows for SMMEs and also ensures a distinctive link between board-level management and the risk management team implementing the model. Nevertheless, the model is in a simplified format, allowing the layperson to achieve results. The model has been tested and validated using a case study.

The Peculium Model includes best practices from endorsed international standards. It provides a solution that offers a heightened awareness of risk in the organisation through staff involvement and board-level governance of the entire process. This paper presents the route followed in creating the model, and the validation performed to demonstrate its value.

KEYWORDS

Information security risk management; SMME; small business; South Africa; Peculium Model; corporate governance; IT governance; risk

THE PECULIUM MODEL:

INFORMATION SECURITY RISK MANAGEMENT FOR THE SOUTH AFRICAN SMME

1 INTRODUCTION

Small, medium and micro enterprises (SMMEs) in South Africa contribute over 40% to the gross domestic product [NATI 2003]. However, these organisations have a failure rate of 80%, mostly due to a lack of management skills [DAIL 2004, DISP 2003]. SMMEs also do not aspire to corporate governance standards for these management skills due to the lack of awareness of corporate governance best practice. The corporate governance standard King II is also not enforced for implementation by SMMEs [KING 2002, CLIFF 2004].

Risk management, as a component of King II, includes technology and business continuity risks. Information security risks can be found within technology and business continuity risks [KING 2002, CLIFF 2004]. Due to the lack of enforcement of corporate governance for SMMEs, managing information security risk is also optional. IT governance as an enabler of corporate governance in IT, which also includes the control of information security risks, is expensive to implement. As a result, many SMMEs are not encouraged, nor are voluntarily making the effort, to manage information security risks [COBI 2000].

The additional problem faced by SMMEs is that information security risk management methodologies that have been created for the international small business are not aligned with local legislative and regulatory requirements, and were not created for the unique South African SMME structures [OCTA 2003, CRAM 2005].

To develop a model that would address both the requirements of a South African small business and the legal and regulatory environment, a literature study was required. This study included the evaluation of the local SMME legislature and structures, local regulations, as well as the international methodologies for small businesses. It was supported by hypotheses structured to ensure the validity of each segmented literature study.

The results of the literature study were used to form a framework for the required model. The contents of the model were then created in alignment with the framework.

This model provides SMMEs with a combination of regulatory and legislative compliance and simplicity of implementation, such that no specialised resources and expenditure are required.

This paper presents the following:

- the assembly of the requirements framework based on the literature study;
- the Peculium Model; and
- the validation of the model by means of a case study.

2 THE ASSEMBLY OF THE REQUIREMENTS FRAMEWORK

The formulation of a framework that would support the creation of a model for information security risk management for South African SMMEs required a literature study of various standards of regulation, legislation and information security risk management.

The standards were evaluated for applicability to small businesses, as well as the capability of being used together. The standards range across the regulatory King II [KING 2002], CobiT [COBI 2000] and ISO 17799 [SABS 2000] the legislative National Small Business Act of 2003 [GOV 2005], and the existing information security risk management methodologies of OCTAVE-S [OCTA 2003] and CRAMM V Express [INSI 2005, CRAM 2005] aimed at the small business.

CobiT, OCTAVE-S and CRAMM V Express were created in developed countries, whereas the legislation for SMMEs and King II were formulated in South Africa, a developing country [CIA 2004, IMF 2004]. This posed a challenge as the makeup of small businesses in developing countries is different from the legislated structure of South African SMMEs [COMM 2003, SBA 2005, GOV 2005]. In addition, the locally accepted international standard for information security, ISO 17799, is locally endorsed, but not specifically created with small businesses in mind [SABS 2000].

2.1 Creation of the requirements matrix

A small business perspective was required to evaluate all of the standards listed above to extract requirements for an SMME-based information security risk management model. The requirements matrix in table 1 demonstrates a cross-section of each standard against the risk management process [ALBE 2003]. The National Small Business Act of South Africa (NSBA), King II, CobiT, ISO 17799 and the methodologies OCTAVE-S and CRAMM V Express (O&C) provide the requirements from each standard, divided into the phases of the risk management process.

Where no explicit requirements were provided by the standards, the intersection of the standard and phase is blank. The methodologies OCTAVE-S and CRAMM V Express, created for small businesses in developed countries, were evaluated for their advantages and disadvantages against South African SMMEs. The advantages resulting from the evaluation are listed in table 1 [VANN 2005]. The items that confirm those already listed by the other standards have not been included, but neither do they indicate a gap.

The matrix shows that no single standard can be considered as providing complete legislative and regulatory compliance, or all good information security risk management practices.

As table 1 demonstrates, the NSBA only addresses the structure of SMMEs. It can also be seen that CobiT and ISO 17799 do not address preparation for risk management, or its monitoring, as is required by King II regulations. Selecting King II, CobiT and ISO 17799 may resolve the gaps, but still does not address the structural requirements of SMMEs.

The unification of all the entries in the requirements matrix was used to create a requirements framework.

Table 1: The requirements matrix

	Literature				
Phases	**NSBA**	**King II**	**CobiT**	**ISO 17799**	**O&C**
Preparation	- Up to 200 employees - Any industry - Any structure	- Identify appetite for risk - Select risk management team - Define objectives - Define key performance indicators			- Obtain senior management involvement - Offer training
Identification		- Establish environment - Identify assets	- Determine scope of boundaries - Designate responsibilities - Identify tangible assets - Identify intangible assets	- Identify tangible assets - Identify intangible assets - Evaluate asset against value scale	
Assessment		- Determine likelihood of occurrence - Perform impact measurement	- Identify threats - Identify vulnerabilities - Add assessment to IT plan - Determine likelihood of occurrence - Perform impact measurement - Identify resources	- Identify threats - Identify vulnerabilities - Calculate risks	
Mitigation		- Perform proactive selection of mitigation strategies	- Create action plan - Identify mitigation solution - Create risk strategies - Select controls	- Select controls	- Create mitigation plan
Monitoring		- Include risk management in day-to-day activities - Update risk register - Measure performance - Create assessment reports - Perform monitoring measurement - Update business continuity plan			- Measure performance

2.2 The requirements framework

The requirements matrix in table 1 provides a list of items to consider for a model. Some of the items are, however, repeated throughout the matrix multiple times.

The organisation of the matrix into a single line of items that addresses the requirements has resulted in the requirements framework, to be used as a foundation for the Peculium Model as presented in figure 1.

The framework provides a cyclical approach to information security risk management, as required by King II and ISO 17799. It also contains all of the unique items derived from the requirements matrix in table 1. The framework provided the roadmap for the Peculium Model.

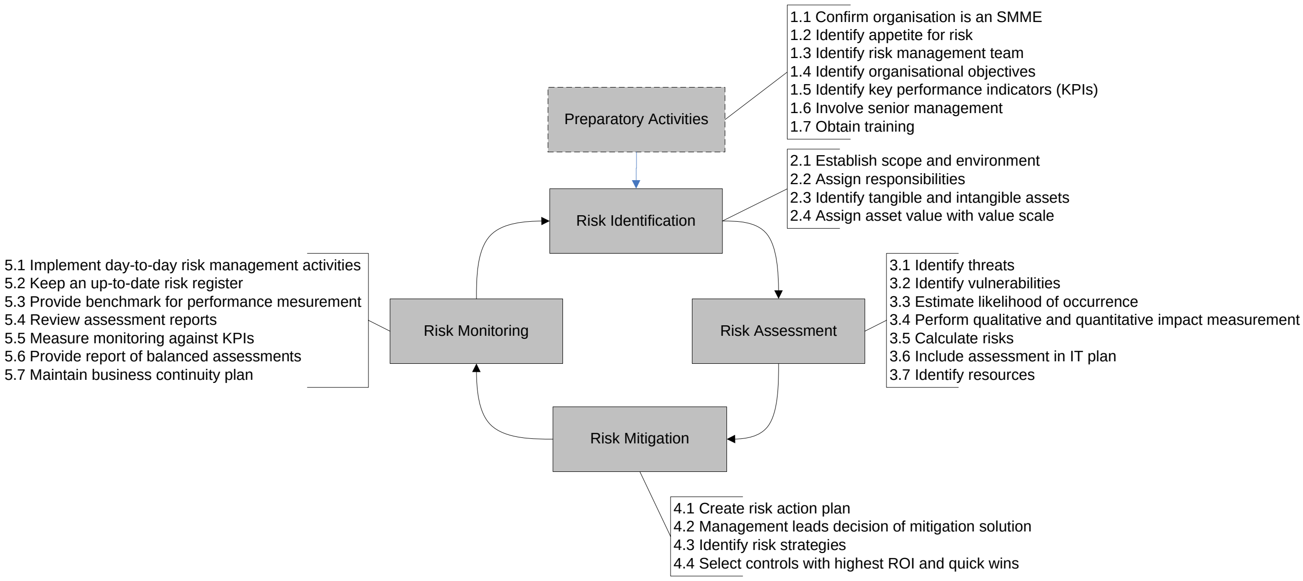
Preparatory Activities
1.1 Confirm organisation is an SMME
1.2 Identify appetite for risk
1.3 Identify risk management team
1.4 Identify organisational objectives
1.5 Identify key performance indicators (KPIs)
1.6 Involve senior management
1.7 Obtain training
Risk Identification
2.1 Establish scope and environment
2.2 Assign responsibilities
2.3 Identify tangible and intangible assets
2.4 Assign asset value with value scale
Risk Assessment
3.1 Identify threats
3.2 Identify vulnerabilities
3.3 Estimate likelihood of occurrence
3.4 Perform qualitative and quantitative impact measurement
3.5 Calculate risks
3.6 Include assessment in IT plan
3.7 Identify resources
Risk Mitigation
4.1 Create risk action plan
4.2 Management leads decision of mitigation solution
4.3 Identify risk strategies
4.4 Select controls with highest ROI and quick wins
Risk Monitoring
5.1 Implement day-to-day risk management activities
5.2 Keep an up-to-date risk register
5.3 Provide benchmark for performance mesurement
5.4 Review assessment reports
5.5 Measure monitoring against KPIs
5.6 Provide report of balanced assessments
5.7 Maintain business continuity plan

Figure 1: The requirements framework

3 THE PECULIUM MODEL

The requirements framework provides a step-by-step information security risk management process but does not provide the actual implementation to be performed.

The Peculium Model is a simplified model, enabling the organisation to use the resources available to it at no additional purchase cost. The model also follows the risk management process, and results in a risk register and a cyclical approach in mitigating those risks.

Due to the restrictions of this paper, the full content of the model is not presented. The following key concepts are presented to demonstrate the simple approach to information security risk management in the procedural cycle.

3.1 Step-by-step checklists

To ensure that SMMEs are offered guidance on completing all vital elements of the Peculium Model, a step-by-step checklist was developed for every deliverable in the process, as demonstrated in table 2. These checklists were required to be reported to the board or senior management forum as real-time proof that progress was being made in the endeavour. Each checklist is related to an item in the requirements framework. In the example used in table 2, the checklist is for phase 1, step 6. The step in the phase is noted as item 1.6 in the requirements framework.

Table 2: An example checklist for step 6 of phase 1

Phase 1: Preparatory Activities			
Step 6		**Senior management involvement**	
	1	Sponsor appointed by the board or management forum	□
	2	Sponsor roles and responsibilities explained to the sponsor	□
	3	Sponsor roles and responsibilities signed off	□

3.2 Asset weakness valuation (Risk Identification)

Due to the limited staff and time resources available to an SMME, prioritisation was vital in the Peculium Model. To effect prioritisation for asset identification, thus reducing the scope of the process per iteration, an asset weakness valuation model was created.

This asset weakness valuation model evaluates the asset against the key information security requirements of availability, confidentiality and integrity. An asset weakness is counted when the information security requirements are threatened. The counting of weaknesses is based on a binary yes/no and 1/0 system for simplification. Each information security requirement is equally weighted, but only considered if the requirement is applicable to the asset.

The resulting weakness value is calculated using the overall average of the three security requirement scores, converted to a percentage value. This weakness value allows the organisation to prioritise the assets based on their weakness (refer to table 3).

Table 3: Asset weakness valuation

Weakness Value Scale	Applicable	Yes/No	Value	Average	Weakness Value
Availability	✓				
Operations are affected when [asset] is unavailable.		Yes	1	0.66	
Unavailability creates a loss of revenue.		Yes	1		
[Asset] cannot be restored within reasonable time period.		No	0		
Confidentiality	✓				
[Asset] is confidential.		Yes	1	1	
Integrity	✓				
[Asset] is not encrypted or protected by secure access.		Yes	1	1	
				2.66	**88.67%**

3.3 Impact measurement (Risk Assessment)

The measurement of impact for the risk calculation of each threat and vulnerability identified considers the following:

- Monetary loss. For a small organisation, cash flow may be a great challenge, and monetary loss a great impact. The level of impact is compared to the appetite for risk identified in the preparatory activities and translated into levels of high, medium and low. (The appetite for risk is an amount based on the worst case scenario loss that the organisation can endure. The organisation may base the amount on a percentage of net profit, percentage of assets owned or revenue for a period.)

- Productivity loss. The loss of productivity in an organisation may be represented by the cost of payroll for the duration of the exposure. The impact is calculated using the following formula:

  $$\text{Impact (Productivity)} = \text{Days} \times \text{Payroll}$$

  The amount is compared to the appetite for risk to determine the impact level of high, medium or low.

- Reputation loss. SMMEs in South Africa account for a great number of enterprises [NATI 2003]. As such, outperforming the rest is vital for an SMME’s survival. The loss in reputation may cause loss of accreditation of an industry standard, customers and future growth. The impact level is determined using the Delphi method of consensus of perceptions [EAGL 2004].

Each impact of low, medium and high is converted to a value of 1, 2 or 3, respectively.

To obtain a total impact value for the three areas an average is calculated as illustrated in table 4. A qualitative value is assigned to the average based on a 9-point scale for use in calculating the risk value. The 9-point scale for each impact value is applied as 3 for a low impact, 6 for a medium impact and 9 for a high impact. The result of the calculation is related to a qualitative high, medium or low based on the 9-point scale of 1 to 3 for low, 4 to 6 for medium and 7 to 9 for high.

Table 4: Impact measurement

Threat: Theft of system hardware	
Monetary	The hardware for the system can be purchased for replacement. When compared to the appetite for risk, the monetary impact of the purchase is **medium**.
Productivity	Productivity is reduced due to the unavailability of the system. It takes 5 days to procure the hardware: I(Pr) = Days * (Payroll) I(Pr) = 5 * (R1 800) I(Pr) = R9 000 When compared to the appetite for risk, the impact of the reduction in productivity is **medium**.
Reputation	Many customers are lost due to the time delay in procuring the hardware. Customers fear the repercussions to their own business due to the wilful damage. Impact is **high.**
Impact (I)	

I = **Medium** + **Medium** + **High**
I = 2 + 2 + 3
I = 7
Impact is **High**
	Impact scale:
	1- 3 = Low
	4 - 6 = Medium
	7 - 9 = High

3.4 Risk calculation (Risk Assessment)

Due to the probable lack of risk analysis skills in the ordinary SMME, qualitative risk calculation was applied [DISP 2003, KARA 2004]. The standard risk calculation formula was used.

$$\text{Risk (R)} = \text{Probability (P)} \times \text{Impact (I)}$$

A 9-point scale is used to assign values to both probability and impact. Probability has been assigned using the Delphi method, and assigning values of 3 for low, 6 for medium and 9 for high [EAGL 2005]. Impact has been calculated as demonstrated in table 4. 9-point scales are assigned to both probability and impact to ensure that each carry equal weight in the risk calculation.

As a result, the risk calculation results in risk values at a maximum of 81 and a minimum of 9. The prioritisation of risks for further action is simplified by sorting the risks by highest value.

3.5 Cost benefit analysis (Risk Mitigation)

In order to assure the SMME board or senior management forum that various mitigating controls were considered for a risk identified for mitigation, a cost benefit analysis model was used. This analysis model was specifically for impact reducing controls and indicated the cost of the various controls, considering the impact of the threat of theft of an asset before and after implementation (refer to table 5).

Table 5: Cost benefit analysis

Threat: Theft of system hardware		
Impact before implementation	High	
Control options	**Security gates**	**Security alarm**
Impact after implementation	Low	Medium
Purchase cost	R2 000 for 2 gates	R7 000
Internal human resource cost	None	None
Total cost	R2 000	R7 000

The cost benefit analysis provides the decision maker with information related to cost both in terms of financial investment as well as productivity from involvement by staff. The analysis also lists the impact reduction of the control.

3.6 Risk management scorecard (Risk Monitoring)

The risk management scorecard provides the board or senior management forum with an up-to-date informative model of progress tracking. The scorecard measures the performance of the risk management process against a list of key performance indicators (KPIs) identified in the preparatory activities (refer to table 6).

This scorecard allows the process implementers to note the KPI’s status (not started, started or completed), as well as the due date for completion. It provides the board with a snapshot of progress to ensure that the process is completed with their support.

Table 6: Risk management scorecard

Risk Management Scorecard			
Key Performance Indicator		**Due Date**	**Status**
1	Achieve milestone at each step of the risk management process	31/08/2006	Started
2	Complete each deliverable at each step of the process	31/08/2006	Started
3	Present milestone summary to the board	31/08/2006	Started
4	Complete asset register at the end of risk identification		Completed
5	Complete risk register at the end of assessment	31/06/2006	Not started
6	Complete risk strategy at the end of risk mitigation	30/07/2006	Not started

The key concepts provided above show the simplicity of the Peculium Model, which nevertheless still results in valid information. A case study was used to test and validate the model.

4 CASE STUDY

A case study of the Peculium Model was performed on a real-world-based organisation. The organisation was studied for its organisational structure, information assets and management structures.

4.1 Description of the organisation

The organisation selected was a South African SMME with 15 members of staff in a retail-based industry with limited funds for IT. The organisation uses three systems for its retail sales, stock management and financial records. The three systems are based on three different infrastructure platforms, with the retail system a legacy system.

4.2 Validation of the Peculium Model

For the purpose of testing the Peculium Model, the concepts discussed in section 3 are shown. The checklists resulting from the case study are not displayed.

4.2.1 Asset weakness valuation

The legacy system is used to demonstrate the weakness valuation in table 7. This system has been valued as a 100% weak system. As a result, it has been ranked highest on the list of asset weaknesses.

4.2.2 Impact measurement

The unavailability of a crucial asset can cause major damage to the organisation. The impact of the failure of the legacy system was calculated as demonstrated in table 8.

Table 7: Legacy system weakness valuation

Weakness Value Scale	Applicable	Yes/No	Value	Average	Weakness Value
Availability	✓				
Operations are affected when [asset] is unavailable. Unavailability creates a loss of revenue. [Asset] cannot be restored within reasonable time period.		Yes Yes Yes	1 1 1	1	
Confidentiality	✓				
[Asset] is confidential.		Yes	1	1	
Integrity	✓				
[Asset] is not encrypted or protected by secure access.		Yes	1	1	
				3	**100.00%**

Table 8: Impact measurement for the threat of hardware failure

Threat: Hardware failure of the legacy system	
Monetary	The hardware for the system cannot be purchased for replacement. The organisation will be forced to continue manually or procure an entirely new system. Compared to the appetite for risk, the impact is **high**.
Productivity	Productivity is reduced due to the unavailability of the system. It will take 21 days to procure a new system: I(Pr) = Days * (Payroll) I(Pr) = 21 * (R1 800) I(Pr) = R37 800 When compared to the appetite for risk, the impact of the reduction in productivity is **medium**.
Reputation	Many customers are lost due to the time delay in procuring the system. Impact is **high.**
Impact (I)	

I = **High** + **Medium** + **High**
I = 3 + 2 + 3
I = 8
Impact is **High**
	Impact scale:
	1- 3 = Low
	4 - 6 = Medium
	7 - 9 = High

4.2.3 Risk calculation

Based on the standard risk calculation method used, the risk value for the legacy system, with the threat being the failure of hardware, is as follows (the probability has been derived to be medium):

Risk (R) = Probability (P) ✕ Impact (I)

R = 6 ✕ 8

R = **48**

The risk value of 48 can now be ranked against the other risk values for prioritisation for mitigation.

Table 9: An example prioritisation of risks for mitigation

Risk Description	Risk value
1. Theft of legacy system	54
2. Hardware failure of legacy system	48
3. Theft of financial system	48
4. Deterioration of storage media	45

4.2.4 Cost benefit analysis

The options available to the organisation for mitigating the risk of hardware failure of the legacy system are either to procure replacement hardware from specialist manufacturers, or to procure a new system. As demonstrated in table 10, although the purchase cost of a new system would be high, the effort required to procure replacement hardware from specialist manufacturers would take longer and would require internal human resource involvement in the search for a manufacturer.

Table 10: Cost benefit analysis for controls for hardware failure

Threat: Hardware failure		
Impact before implementation	High	
Control options	**Specialist manufacturing**	**New system**
Impact after implementation	Medium	Medium
Purchase cost	R100 000	R70 000
Internal human resource cost	R10 000	None
Total cost	R110 000	R70 000

4.2.5 Risk management scorecard

The scorecard was completed based on an understanding of the resource challenges faced by the case study organisation, and probably timeliness assigned to the mitigation of the risks.

The scorecard is shown in table 11. The case study verified that the simplified methods used in the Peculium Model yielded results.

Table 11: Risk management scorecard

Risk Management Scorecard			
Key Performance Indicator		**Due Date**	**Status**
1	Achieve milestone at each step of the process		
1.1	Preparatory activities milestone achieved		Completed
1.2	Identification milestone achieved		Completed
1.3	Assessment milestone achieved		Completed
1.4	Mitigation milestone achieved		Completed
1.5	Monitoring milestone achieved	28/02/2006	Started
2	Complete each deliverable at each step of the process		
2.1	Preparatory activities deliverables achieved		Completed
2.2	Identification deliverables achieved		Completed
2.3	Assessment deliverables achieved		Completed
2.4	Mitigation deliverables achieved		Completed
2.5	Monitoring deliverables achieved	28/02/2006	Started
3	Present milestone summary to the board	28/02/2006	Started
4	Complete asset register at the end of risk identification		Completed
5	Complete risk register at the end of assessment		Completed
6	Complete risk strategy at the end of risk mitigation		
6.1	Risk 1: Mitigation		Completed
6.2	Risk 2: Transfer		Completed
6.3	Risk 3: Mitigation		Completed
6.4	Risk 4: Transfer		Completed
6.5	Risk 5: Mitigation		Completed
7	Complete action plan		
7.1	Risk 1: Burglar bars and security alarm	03/01/2006	Started
7.2	Risk 2: HD Insurance		Completed
7.3	Risk 3: Burglar bars and security alarm	03/01/2006	Started
7.4	Risk 4: HD Insurance		Completed
7.5	Risk 5: Anti-virus and application	01/02/2006	Started
8	Complete assessment report	01/03/2006	Started
9	Update business continuity plan		N/A

5 CONCLUSION

This paper presents the process followed in developing the Peculium Model through a literature study of legislation and regulations, as well as existing information security risk management models aimed at small businesses. The model was created by forming the requirements matrix, based on the literature study, followed by condensing the matrix into a single list of items for the risk management process known as the requirements framework.

The requirements framework provided a foundation on which the Peculium Model was built. This model was aimed at South African SMMEs, and was created to be simple, valid and not resource-intensive. The model was then tested and validated using a case study.

The objective of creating a model that complies with legislative and regulatory requirements and that suits the resources and skills of South African SMMEs was achieved. The SMME market space is incredibly under-researched, which increased the difficulty of conducting the literature study for the foundation of the Peculium Model.

The Peculium Model provides the body of knowledge with an alternative solution to small business in South Africa for implementing information security risk management. The model has gone further than other models in focusing on compliance with local legislation and regulations. It also provides the traditional risk management outcomes, such as a risk register and mitigation strategies. The model supplies the board or senior management forum with vital information related to information security risks, and the benefits of managing those risks, possibly reducing lost revenue as a result of poorly controlled assets. This knowledge could also drive the board or forum into a process of awareness of other risk areas, thus reducing the probability of organisational failure.

This research was narrowly focused on the local, South African environment and did not consider international law, due to the myriad structures of small businesses in both developed and developing countries [COMM 2003, SBA 2005, GOV 2005, CW 2005, FUND 2004, LECH 2004]. Further research may be performed to create a Peculium Model that addresses a generic international framework of legislation and regulation. Further research may also be performed to alter the Peculium Model to suit local large enterprises, focusing less on the simplified nature of the model and more on the enforced governance standards that become compulsory for listed companies.

6 REFERENCES

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

[CIA 2004] CIA World Factbook; Accessed through TheFreeDictionary.com; http://www.encyclopedia.thefreedictionary.com; Accessed October 2004.

[CLIFF 2004] Review of the Corporate Governance in South Africa. Accessed through CliffeDekker.co.za; http://www,cliffedekker.co.za. Accessed October 2004.

[COBI 2000] IT Governance Institute; 2000; CobiT 3rd Edition; ISBN: 1-893209-14-8.

[COMM 2003] Commission Recommendation of 6 May 2003 concerning definition of micro, small and medium-sized companies; Official Journal of the European Union; May 2003.

[CRAM 2005] CRAMM.com; CRAMM Methodology; http://www.cramm.com; Accessed May 2005.

[CW 2005] The Commonwealth Website; http://www.thecommonwealth.org; Accessed November 2005.

[DAIL 2004] Daily News Homepage; Daily News Online; http://www.dailynews.co.za; Accessed April 2004.

[EAGL 2004] Eagle Forum; http://www.eagleforum.org; Accessed October 2005.

[DISP 2003] Dispatch Online; “SMMEs failure blamed on poor management”; Access through DispatchOnline.co.za; http://www.dispatchonline.co.za; Accessed September 2004.

[FUND 2004] Fundes.org; SME’s indicators in the FUNDES region; http://www.fundes.org; Accessed October 2004.

[GOV 2005] The South African Government; http://www.gov.org.za; National Small Business Amendment Act of 2003.

[IMF 2004] IMF List of Advanced Economies; Accessed through Reading.org; http://www.reading.org/membership/devel.countries.html; Accessed October 2004.

[INSI 2005] Insight Consulting; 2005; CRAMM V Express Walkthrough Flash Presentation – CRAMM V (Computer Program).

[KARA 2004] Karabarak, B., Sogukpinar, I.; ISRAM: Information Security Risk Analysis Method; Computers & Security 2005, 24.

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

[LECH 2004] Lecholo, DS.; Botswana’s Experience of Informal Traders, Sustainable Livelihoods and Economic Development through Trade. Presented at the SADC workshop on informal traders, February 2004.

[NATI 2003] The Relative Importance of SME’s in the South African economy: an analysis of issues and quantification of Magnitudes (requested by National Treasury).

[OCTA 2003] OCTAVE-S Implementation Guides, Version 0.9; Alberts, C., Dorofee, A.; James, C., Woody, C.; August 2003.

[SABS 2000] SABS ISO 17799; Information Technology Code of Practice for Information Security Management. The South African Bureau of Standards. 2000. ISBN 0-626-12835-8.

[SBA 2005] SBA.gov; United States Small Business Administration; http://www.sba.gov; Accessed November 2005.

[VANN 2005] Van Niekerk, L., Labuschagne, L.; 2005; A Framework for Evaluating Information Security Risk Management for SMME’s; Peer-reviewed Proceedings of the ISSA 2005 New Knowledge Today Conference. 2005. ISBN 1-86854-625-X.