A Software Gateway to Affordable and Effective Information Security Governance in SMMEs

Jacques Coertze
Institute for ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Email: jacques.coertze@gmail.com

Rossouw von Solms
Institute for ICT Advancement
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
Email: rossouw.vonsolms@nmmu.ac.za

***Abstract*—It has been found that many small, medium and micro enterprises (SMMEs) do not comply with sound information security governance principles, specifically those principles involved in drafting information security policies and monitoring compliance, mainly as a result of restricted resources and expertise. Research suggests that this problem occurs worldwide and that the impact it has on SMMEs is great. In previous research an information security governance model was established to assist SMMEs in addressing information security governance issues and concerns. In order to provide SMMEs with a practical approach for applying this model, further research was conducted to establish a software program that demonstrates the model's practical feasibility. The aim of this paper is to introduce this software program, called *The Information Security Governance Toolbox (ISGT)*, by means of its various components, workings and benefits. Furthermore, a focus-group study's evaluation results are offered that suggest that the program is useful to SMMEs in addressing their information security governance implementation challenges and offer value for industry.**

***Keywords*—automation, information security, corporate governance, enterprise security, IT governance, information security governance, managing information security, security policy and procedures, methodologies for securing small/medium size enterprises**

I. Introduction

Information is known to be one of the most critical assets of the modern-day business [1, p. iv]. Businesses nowadays use information for a plethora of concerns, ranging from production and decision making to gaining competitive advantage over rivals to name but a few [2, p. viii]. Similarly, information technology (IT), acting as the custodian of information, is gaining ever-increasing importance in the modern marketplace [3, p. 13] as it today may account for as much as two-thirds of the value or capital of an enterprise [4]. Unfortunately, this high dependence on information and IT also brings with it many responsibilities that have to be addressed [1, p. iv], in particular that of information security and the proper management thereof [6].

Although information security management plays a vital role in ensuring that adequate measures are taken to protect information in a business, the fact that it has become imperative for information security and its management also to be well governed should not be overlooked [8, pp. 1-6]. Hence, a process commonly termed ”information security governance” has been proposed [6].

Unfortunately, many small, medium and micro enterprises (SMMEs)[1] are struggling to address information security governance adequately, owing to the volatile economic challenges around the world including recessions, wars and poverty, as well as a general lack of resources and expertise [9]–[11]. In order to alleviate this difficulty, previous research [12] has established an information security governance model (see Fig. 1) that could facilitate the implementation of sound information security governance principles in these enterprises.

It has, however, been realised that although the newly established model provided many benefits, it may supply countless more if used to develop an automated or semi-automated software program. Accordingly, a software program has been developed to demonstrate that such an implementation is feasible.

The software program mentioned forms the primary concern of this paper and will be detailed as follows: Firstly, the program and an elaborate discussion of its workings will be introduced. Secondly, a discussion of the benefits that accrue from this program will follow. Thereafter the results of an evaluation that was performed on the program will be discussed.

II. Introduction to the ISG Toolbox

Previous research [12] described the process leading to the establishment of an information security governance model for the implementation of information security governance in organisations with limited resources and expertise. This model was subsequently used as a basis for the development of a semi-automated software program to guide and assist SMMEs in their information security governance efforts.

In this context, the goal of the program was to demonstrate the feasibility of implementing the model in a software product.

[1] This paper focuses specifically on small and medium enterprises when referring to SMMEs, as their management structure more closely supports and recommends the components of the model and the supportive software program. It should be noted that micro enterprises may still benefit from the contribution of this paper, although their management structure may require some customisation and selective usage.

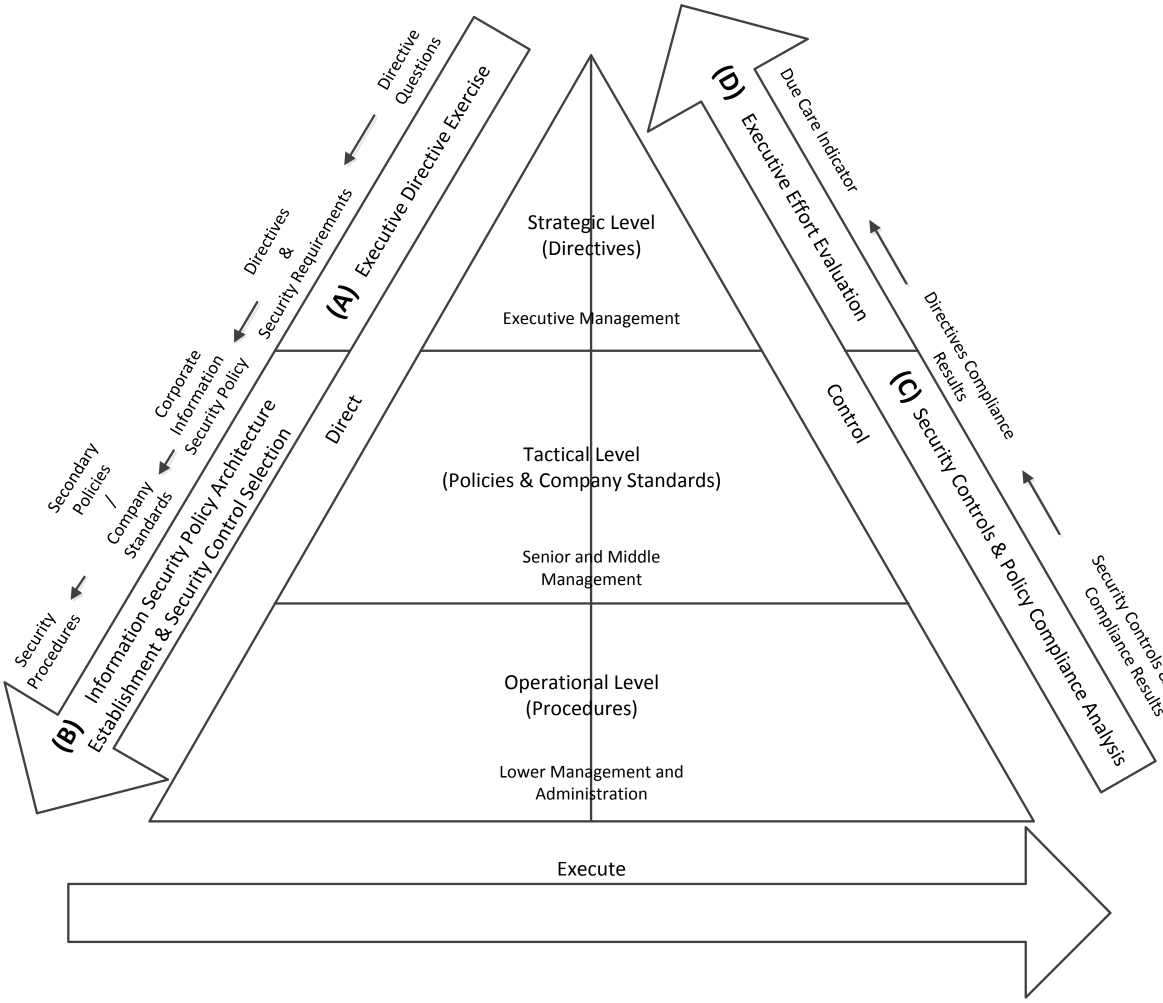
Directive Questions
Directives & Security Requirements
Corporate Information Security Policy
Secondary Policies / Company Standards
Security Procedures
(A) Executive Directive Exercise
(B) Information Security Policy Architecture Establishment & Security Control Selection
Direct
Strategic Level (Directives)
Executive Management
Tactical Level (Policies & Company Standards)
Senior and Middle Management
Operational Level (Procedures)
Lower Management and Administration
Control
(D) Executive Effort Evaluation
Due Care Indicator
(C) Security Controls & Policy Compliance Analysis
Directives Compliance Results
Security Controls & Policy Compliance Results
Execute

Fig. 1. The Information Security Governance Model

As already mentioned the software program carries the title of *The Information Security Governance Toolbox (ISGT)* and was implemented as a stand-alone desktop application using three-tier software architecture in a file-sharing environment. This program extends the functionality offered by an existing information security management software program developed by Hoppe, Van Niekerk and Von Solms [16] based on research conducted by Vermeulen and Von Solms [17] amongst others.

Having introduced the software program, it now becomes necessary to examine its internal workings and components.

III. Mechanics of the ISG Toolbox

The software program consists primarily of two phases, namely, a *direct* and a *control phase*, each of which consists of two components. These four components in turn map directly onto the requirements embedded in the information security governance model (see A, B, C & D in Fig. 1).

The following subsections introduce the two phases of the program in addition to the four components. This will be followed by a section in which each component will be elaborated on individually.

A. Toolbox phases

The program exhibits two distinct phases a *direct* and a *control phase*.

The *direct phase* aims to facilitate, among other things, the establishment of board directives, propose a set of modifiable security controls and dynamically draft corresponding information security policies.

In contrast, the *control phase* affords the user a compliance analysis exercise in respect of the security controls and company standards established during the *direct phase*, as well as the possibility of conducting a further executive involvement evaluation exercise to evaluate executive management's involvement and efforts in relation to information security governance.

B. Toolbox components

The above-mentioned phases are made possible by the many components embedded in the program.

The components that map onto the phases of the program are as follows:

- the *direct phase* consists of

  - an executive directive exercise (refer A in Fig. 1)
    - ∗ which assists executive management in the establishment of sound information security board directives indicating their involvement, commitment and strategic vision for information security.
  - the establishment of information security policy architecture (ISPA) and a security control selection process (refer B in Fig. 1)
    - ∗ which facilitates the establishment of an information security policy architecture in the user organisation by means of the identification of security requirements, the proposal and selection of security controls, and the drafting of dynamic policy. Thus, strategic- and tactical-level management is guided by the establishment of security requirements for the user organisation. Furthermore, applicable security controls are proposed for selection by the user in addition to allowing the user to indicate the desired compliance or adherence level that is sought for each of these controls. Subsequently, supporting security procedures are presented for selection based on the security controls selected. All of these measures facilitate the ultimate goal, that is, the dynamic drafting of the security documentation required to enforce the information security measures of the user organisation.
- the *control phase* consists of
  - company standards and a security controls compliance analysis exercise (refer C in Fig. 1)
    - ∗ which allows the user to perform a compliance analysis exercise in respect of the security controls and company standards established during the *direct phase*; thus, identifying any weaknesses or improper implementation of the proposed security controls.
  - an executive effort or due care analysis exercise (refer D in Fig. 1)
    - ∗ which empowers executive management to evaluate its information security governance involvement and efforts; thus, allowing for the identification of a lack of due care or due diligence concerning its information security governance duty.

In addition, two additional components were introduced, namely, a knowledge base component added to give users of the program background information on information security and its proper management and governance, and secondly, a user details capturing component allowing the user to enter his/her personal and/or company details for subsequent use by the program.

Each of these program components will be discussed in more detail in the following section.

IV. Toolbox Components in Detail

A. Knowledge base

The program operates in terms of an interactive wizard with the purpose of accompanying users step by step through the process flow specified in the model. The wizard starts by introducing the user to the knowledge base component. As previously mentioned, this component is responsible for educating the user on the core concepts and principles of information security, its management and governance, as well as emphasising the importance of adhering to a structured and disciplined process when implementing it in an organisation. This module was implemented using a series of pre-established MS PowerPoint slide shows which are embedded in the program. Although embedded in nature, these slide shows are nonetheless free standing and could be frequently updated independently of the program to offer the user the latest facts.

Thus, by completing this component it can be said that the user of the program will be sufficiently educated on the core concepts and principles of information security, as well as its management and governance.

B. Capturing of user details

Once the user has been made aware of the contents of the knowledge base, the next step is for the user to enter his/her personal and/or company details in the fields provided for use during the drafting of information security documentation by the program. These may include the company name, logo, telephone number, email address, chief executive officer (CEO) and name of the party responsible for information security.

Thus, by completing this component it can be said that the program now has in its database the user's personal and/or company details for use when drafting information security documentation at a later stage.

Subsequently, the wizard offers the user the option to either engage the *direct* or the *control* phase. The former is discussed in the following subsection.

C. The direct phase

1) Executive directive exercise: The *direct phase* starts with an executive directive exercise (refer A in Fig. 1). Executive management is hereby asked a series of eleven thought-provoking security-related questions which were adapted from the research conducted by Von Solms and Von Solms [18], per example: *"Information is an important business asset to your organization. Do you agree with this statement?"*

As seen, each of the questions from the research by Von Solms and Von Solms [18] was adapted to facilitate either a positive (yes) or negative (no) response. In the event of a negative response being submitted, a pre-set information security governance awareness statement and question follows in order to afford executive management an opportunity to re-evaluate and possibly change its initial response. Should the initial negative response remain, the wizard then indicates that executive management should seek guidance and education on the matter of information security and its proper governance and will not allow the respondent to progress further. As soon as all the questions have been answered with a positive response, the program uses reasoning and inference to establish corresponding board directives.

It is worth mentioning that, during the development of this component; this and various other approaches were effectively investigated and considered. The above-mentioned approach was, however, deemed the most feasible as it requires minimal expertise and knowledge and is not overly complex; thus it is ideal for use by SMMEs.

In conclusion, when this component has been completed it can be said that a series of board directives will have been established, thus indicating executive management's commitment to and vision for information security in the organisation, which will then form the input for the information security policies that will subsequently be drafted.

2) ISPA establishment:

a) Security requirements analysis: The next step of the *direct phase* entails the establishment of an information security policy architecture (refer B in Fig. 1) using security requirement identification, security control proposal and selection, and dynamic policy drafting.

The identification of an organisation's security requirements forms the first step, which aims to assist strategic- and tactical-level management in the user organisation with the establishment of security requirements.

It was determined that an organisation's security requirements may be formulated by making use of a pre-established business analysis questionnaire consisting of 64 questions based on a security requirements analysis approach, as established by Von Solms and Gerber [19]. Each of the questions included in the business analysis questionnaire refers to a specific security requirement, namely, confidentiality, integrity, availability, authentication or auditability. However, in order to assess the importance of security requirements properly, each security requirement is addressed by a number of questions in the questionnaire. The answer selected for each of these questions in turn determines a rating (e.g. low, medium or high), which is then assigned to each security requirement.

It should be noted that during the development of this component, the possibility of performing a traditional risk analysis exercise was also investigated. However, this approach was shown to require extensive knowledge of an organisation's information and IT assets, and the specific threats and vulnerabilities they are faced with, which can vary considerably from organisation to organisation. Further, such a risk analysis involves a great deal of expertise, effort and time, which most SMMEs simply do not have [20]. Hence, it was deemed unfit for use in the program. Instead, the security requirements analysis approach [19] was adopted, as mentioned above, since it is simpler and allows for greater flexibility and scalability. In retrospect, however, it should be stated that an organisation could still supplement the approach used in the program with a risk analysis exercise or other approach, if necessary.

In summary, by completing this component it can be said that the security requirements of the organisation will have been identified, which subsequently allows for the identification and proposal of suitable security controls to address these requirements.

b) Security control selection: Based on the identified security requirements and their ratings, the wizard subsequently presents the user with a series of modifiable security controls. These security controls originate from *ISO/IEC 27002* [2] and indicate an appropriate baseline protection for the organisation in line with their security requirements. It should, however, be noted that the security controls presented merely serve as a guide for implementing information security in accordance with the organisation's operational environment. Thus, the user can select or de-select security controls, provided that a legitimate reason is provided in accordance with the statement of applicability proposed by *ISO/IEC 27001* [21, p. 8].

Thus, following the completion of this component a set of applicable security controls will have been presented to the user and subsequently selected or de-selected for use in the organisation.

c) Security control compliance target setting: Concurrent with security control selection, the user is also prompted to indicate the desired compliance or adherence level that is sought for each security control. This constitutes compliance target setting (set at a certain percentage level) for each control. In this regard, the level of compliance ranges from 0 to 100%. The ideal would be to enforce 100%, but since some enterprises using the program are only starting to initiate their information security governance implementation, it may be ill-advised to expect such a high compliance level. The desired compliance or adherence level for each security control is in turn stored by the program for use during the *control phase*.

The completion of this component thus indicates that an ideal compliance/target indicator will have been determined for each selected security control, which will be used during one of the later components.

d) Security procedure selection: After the completion of the security control selection step, the user is presented with a series of security procedures for each of the security controls. The set of selectable security procedures originates from a variety of sources, of which the implementation guidance clauses of *ISO/IEC 27002* [2] are the primary contributor. This step, that is, the selection of security procedures, is deemed necessary as it serves as a guideline for achieving the objectives of each security control [22, p. 54]. It should be noted that currently only security procedures pre-established during the program's development can be selected; however, it is envisaged that users may in future add customised security procedures according to their needs or circumstances.

Thus, following the completion of this component a set of applicable security procedures for each security control will have been proposed to the user and subsequently selected or de-selected for use in the organisation.

e) Dynamic generation of information security documentation: Following the establishment of the organisation's security requirements and the selection of appropriate security controls and supportive security procedures, the program dynamically drafts the security documentation required to enforce these information security measures.

This documentation includes the drafting of the following:

- a corporate information security policy, both a short and long version
- secondary-level policies in the form of various supportive company standards that reflect the identified security controls
- corresponding, policy-linked, security procedures
- a statement of applicability.

This set of documentation is offered to the user as personalised tailor-made Word documents, which may be modified and adjusted to suit the specific needs of the organisation. The program also stores a copy of this documentation, which may be accessed at any time unless new documentation is drafted.

Hence, by completing this component, that is, the establishment of information security policy architecture, a corporate information security policy will have been drafted, supported by a series of secondary-level policies or company standards which, in turn, is further endorsed by applicable security procedures.

Von Solms and Von Solms [1, pp. 74-75] indicate that an organisation's information security policy architecture comprises the components, or documents, that facilitate the directing of information security. Thus, through the dynamic generation of this documentation by the program, the information security policy architecture of the user organisation is established, as well as the appropriate selection of information security controls.

These aforementioned components in their entirety constitute the *direct phase* of the program, and may be performed whenever the operational environment of the user organisation changes, including when new information and IT assets are purchased or new threats and/or vulnerabilities are identified. It may also be necessary to repeat this phase periodically to ensure that the documentation that has been generated is kept up to date.

D. The control phase

In support of the model's requirements and the program's *direct phase*, the *control phase* of the model should also be initiated quarterly, bi-annually or at least annually.

Owing to the dynamic nature of compliance and adherence, it is advised that this phase should not be neglected [23]. Since documentation produced during the *direct phase* does not automatically guarantee compliance and adherence [18], it is essential that regular monitoring and control take place in the organisation. Hence, the primary goal of the *control phase* of the program is to evaluate compliance with the documentation produced and then institute corrective action if required.

1) The analysis of company standards and security control compliance: The commencement of the *control phase* is marked by a company standards and security controls compliance analysis exercise (refer C in Fig. 1). This exercise starts with the user choosing to perform either a full or limited-scope compliance analysis of the established security controls and company standards. In the event that a limited scope is selected, the user is given the option to select the company standards and accompanying security controls that need to be analysed. This step allows for flexibility, as an organisation may choose to analyse only specific security controls or company standards at a given time in order to reduce costs and interruptions.

Once a full or limited scope compliance analysis has been selected and an indication provided of the security controls and company standards to be analysed, the user is presented with a questionnaire, which contains a series of security control-related compliance analysis questions, with at least three questions for each security control. A minimum of three questions was decided in order to allow for triangulation to occur and a more accurate compliance assessment to be made, especially since SMMEs are often not knowledgeable about security controls and guessing might occur otherwise.

As the security controls that can be selected during the *direct phase* originate from *ISO/IEC 27002* [2], *ISO/IEC 27001* [21] compliance analysis questions made available by the InfoSec Institute [24] were used for this purpose. Although other sets of questions exist, this set was chosen as it is one of the few that offer more than one analysis question per security control. This was deemed vital for making the compliance analysis process understandable and for ease of use.

Each of the questions in this set are presented in the form of a five-point Likert scale, on which users indicate the level of security control compliance or adherence achieved, ranging from no adherence or implementation to complete fulfilment and adherence.

When the responses to these questions have been submitted, a graphical compliance analysis report is produced using a series of complex mathematical equations and weighted calculations. This report is specifically aimed at tactical and executive management and makes use of colour coding and key performance indicators (KPIs) to offer a clear indication of the compliance level being achieved for the selected security controls, the company standards and the corporate information security policy as a whole. It is worth mentioning that this report also makes use of the security control compliance target indicators that would have been captured during the security control selection process in order to indicate whether the desired outcome has been achieved.

Thus, following the completion of this component a full or limited compliance analysis will have been performed on the security controls instigated in the organisation and a graphical compliance analysis report produced which could be used for taking corrective action.

2) Executive due care analysis: On completion of the compliance analysis exercise, the next step is to give executive management an opportunity to perform a due care analysis exercise (refer D in Fig. 1). A series of eleven thought-provoking questions are hereby posed that allow executive management to investigate and evaluate its information security governance efforts in terms of the due care and diligence required by the model, per example: *”Do you accept that information is a critically important business asset to your organisation?”*

As seen, each question that executive management is asked elicits a positive (yes) or negative (no) response. In turn, the responses indicate executive management’s efforts as regards the due care checklist that was developed by Von Solms and Von Solms [18], which was also used to construct the executive directive exercise component found in the *direct phase*. Thus, a clear correlation exists between the board directives established by the aforementioned component, the documentation that is generated and the checklist used in this exercise. For example, one board directive reads ”a Corporate Information Security Policy (CISP) must be defined, introduced and maintained to guide all efforts to mitigate risks threatening business information”. Using the program, a CISP is generated and maintained that satisfies the board directive; furthermore this in turn satisfies the due care analysis question, ”Did you create and express a clear vision to mitigate business information risks to an acceptable level using a CISP?”

In summary, following the completion of this component it can be said, according to Von Solms and Von Solms [18], that executive management will have been offered a due care and diligence indicator perhaps pointing to a possible lack of due care, which can subsequently assist management in taking corrective action.

These components in their entirety constitute the *control phase* of the program. This phase may be performed on a periodic basis as required by the organisation and/or suggested by best practices. The *direct* and *control phases* which constitute the workings of this program thus combine to form the direct-control action cycle that is exhibited by information security governance [6].

The program therefore acts as an aid for organisations, in particular SMMEs, when implementing or improving information security governance. This is achieved by the program, as it provides actionable/practical components and processes to guide organisations through the information security governance implementation and/or improvement process. The program includes the development of relevant information security documentation as well as the maintenance and compliance analysis of such documentation.

As SMMEs are often neither aware of nor knowledgeable about the above-mentioned components and processes [13, pp. 82-83], this program offers significant benefits for addressing and possibly alleviating this problem.

V. Benefits of the ISG Toolbox

The development of this program holds many benefits for organisations with limited expertise and resources. This section highlights just a few of the benefits that is associated with this program.

Affordability. The fact that freely accessible technologies and components were used for the construction and operation of this program renders it affordable while also being comprehensive in nature.

Simplicity. During the construction of this program, components and techniques were identified and subsequently implemented that are not overly complex and that can be used and interpreted easily. This refers specifically to the security requirements analysis and executive directive exercise.

Scalability. SMMEs are characterised by their varying size and flexibility in terms of resources and expertise [13, pp. 82-83]. With this in mind, all the techniques and components introduced in this program are scalable. Hence, the output of the program adapts according to the specifics of the organisation using it.

Applicability. Many off-the-shelf information security solutions are available on the open market, but they cater mainly for large organisations [20]. This program is tailored specifically for SMMEs and takes note of their limitations and restrictions. This also applies to the output and input that this program offers and requires.

Flexibility. SMMEs are characterised by their flexibility and adaptive nature [25, p. 9]. This includes their size, financial standing and management structures [26]. As this program allows for flexibility and a degree of customisation, it does not limit or restrict the user organisation from using only specific security controls or documentation and so on. It acts merely as a guide offering the best practice-driven baseline applicable to the user organisation.

Compliance with international management and governance standards/best practice. International management and governance standards and best practice offer specific guidance to organisations in order for successful information security governance implementation and continued operations to be assured. This program is based specifically on and adheres to the guidance offered by *ISO/IEC 27002* [2], *ISO/IEC 27001* [21], as well as *ISO/IEC 38500* [27] and *CobiT 5* [3].

VI. Evaluation of the ISG Model and Toolbox

During the development of the software program, a fully-functional and complete evolutionary desktop application proof-of-concept prototype featuring all the program’s finer workings and components and the model it was based on were evaluated to determine the program’s future usage in and value for the SMME community. The evaluation of this prototype took the form of a focus group-like study, given the availability of three respected SMMEs and the fact that the potential industry users of the program wanted to be reached for feedback and commenting. Furthermore, the focus group-like study facilitated answers to questions that the development of the program could not resolve.

As mentioned, three respected SMMEs were identified at an IT and security (ISACA) conference based on size, that is, one in each size category (micro, small, and medium enterprise), and were invited to participate in the evaluation study. This was deemed critical as the program's audience included all sized enterprises within the SMME domain and allowed for a collective SMME group or domain consensus to be reached.

Each participant was visited and underwent a short informative workshop session conducted by the authors and developer at their premises in order to provide them with details on the purpose of the study, as well as an overview of the research and the use of the prototype. Afterwards, this prototype was made available to each of the SMMEs on a trial basis and a questionnaire was provided to be completed within a specified time in order to evaluate the feasibility of the components and workings of the prototype and, indirectly, the model.

The feedback and comments that emanated from the responses to this questionnaire indicated, although not the primary aim, that some usability issues were present in the implementation of the prototype. Comments in this regard include among others:

> ”The process I had to follow throughout the program was at times not clear.”

> ”I found the slides in the knowledge base to be basic and not visually appealing at times.”

Nevertheless, these usability issues were shown to have very little effect on the overall use of the prototype. Moreover, these issues were subsequently addressed in the development of the final software program.

One comment made by a participant in response to an item on the questionnaire read:

> ”I found that the amount of documentation generated was too much. If a company would go with the standard suggestions there would be too many policies and procedures and would actually make management difficult.”

This comment was acknowledged; however, it should be kept in mind that the program is not size-orientated, but rather security requirements-orientated. Accordingly, the security requirements of each individual SMME directly influence the amount and coverage of the documentation generated by the software program.

Another questionnaire respondent raised the following vexation:

> ”I was concerned at times that the Protection of Personal Information Bill (POPI) had not been taken into account.”

This comment had merit as these regulatory issues are becoming more prominent in industry. In response it can be said that the software program does cater for some regulatory elements to be addressed as part of the security requirements analysis component. However, this could certainly be enhanced in future versions of the software program by means of intensive research in this field.

The following suggestion and/or comment also originated from the questionnaire responses:

> ”Better technology such as Software-as-a-Service (SaaS) could have been used in addition to a web-based platform for the implementation of the program.”

This suggestion was noted and corresponds with the initial vision for the operation and development of the software program [28]. Unfortunately, given that the program stores and utilises confidential business information, this particular approach was deemed unfeasible upon implementation as the safety of the information could not be guaranteed. Similarly, an issue arose as to who would own the information once it has been captured on a web-based platform. Hence, to avoid these concerns, the three-tier desktop application architecture model was adopted instead.

Although many comments, suggestions and concerns were raised, the respondents of the study did come to a consensus, supported by subjective observations, that the information security governance model, and the supporting software program, are indeed feasible and hold many benefits for SMMEs in terms of assisting them with the implementation of information security governance. Responses supporting this conclusion read:

> ”A super, innovative product which I believe has a lot of potential - especially for smaller organisations that do not have a lot of resources to commit to something like information security.”

> ”On the whole, I think the concept is good. It does provide many organisations with a cost effective way to put information security policies in place.”

It can thus be stated on the basis of this feedback that the software program and model certainly proves to be valuable to SMMEs, but they can probably be further enhanced in the future to provide even more effective support.

VII. Conclusion

Information and IT, as an enabler, is of great importance to the success of nearly all modern-day businesses. However, as these businesses continue to place an ever higher dependence on information and IT, so too should their protection be considered. Nevertheless, the literature suggests that for information security to be successful in defending information, it must be well managed and governed. Thus, the requirement for information security governance in all organisations, irrespective of their size, is becoming of grave importance.

Regrettably, as a result of a general lack of resources and expertise, many SMMEs are struggling to address information security governance adequately. In order to alleviate this difficulty, previous research has established an information security governance model that could facilitate the implementation of sound information security governance principles in these enterprises.

Unfortunately, it was subsequently realised that SMMEs currently require practical rather than theoretical assistance in the form of processes, procedures and aids that they can use in a real-world setting. Thus, it was realised that many more benefits could be achieved if the model were to be used to develop an automated or semi-automated software application. Accordingly, a software program was developed to demonstrate that such an implementation was feasible and it was introduced in this paper as *The Information Security Governance Toolbox (ISGT)*.

This paper introduced the software program in conjunction with a detailed discussion of its components and finer workings. Afterwards, the benefits exhibited by this program were also highlighted.

The evaluation results of a focus group-like study performed on the program using a proof-of-concept evolutionary prototype, specifically on its finer workings and embedded components, were also shared. The feedback and comments, per respondent consensus, suggest that the program is feasible and justify the expectation that it holds many benefits for SMMEs in their information security governance implementation.

It is envisaged that this program will continue to receive attention and enhancements in the future, which may one day lead to the availability of a fully-fledged commercial product. Areas for future research include the performing of a security analysis on the program to determine whether the proposed solution enforces security protection within the SMME setting and to verify that the proposed solution actually guarantees the same or better levels of security than any existing solutions. Furthermore, comprehensive usability testing could be performed on the program and corrections made.

It is suggested that, since SMMEs form such an important part of the economic structure of countries around the world, information security researchers should remain vigilant in their attempts to assist them with both theoretical models and practical aids.

Acknowledgment

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

[1] S. Von Solms and R. Von Solms, *Information Security Governance*. Springer, 2008.

[2] ISO/IEC 27002, *Information technology: Code of practice for information security management*. Switzerland: International Organization for Standardization (ISO), 2005.

[3] ISACA, *COBIT 5*, 2012.

[4] K. Melymuka, "IT does so matter!" 2003. [Online]. Available: https://www.computerworld.com/s/article/82738/IT_does_so_matter_

[5] R. Nolan, "Ubiquitous IT: The case of the Boeing 787 and implications for strategic IT research," *The Journal of Strategic Information Systems*, vol. 21, no. 2, pp. 91–102, Jun. 2012. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0963868711000801

[6] R. Von Solms and S. Von Solms, "Information security governance: A model based on the direct-control cycle," *Computers & Security*, vol. 25, no. 6, pp. 408–412, 2006.

[7] M. Whitman and H. Mattord, *Principles of information security*, 4th ed. Course Technology, 2012.

[8] K. Brotby, *Information Security Governance: A Practical Development and Implementation Approach*. Honoken, New Jersey: John Wiley & Sons, 2009.

[9] S. Goodman and A. Harris, "The coming African tsunami of information insecurity," *Communications of the ACM*, vol. 53, no. 12, p. 24, 2010.

[10] E. Yildirim, G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey," *International Journal of Information Management*, 2010.

[11] C. Upfold and D. Sewry, "An investigation of information security in small and medium enterprises (SMEs) in the Eastern Cape," in *Proceedings of the ISSA 2005 New Knowledge Today Conference*, H. S. Venter, J. H. P. Eloff, L. Labuschagne, and M. M. Eloff, Eds., 2005, pp. 1–17.

[12] J. Coertze and R. Von Solms, "A model for information security governance in developing countries," in *AfriComm*. Springer, 2012, pp. 1–8.

[13] H. Koornhof, "A framework for IT governance in small businesses," Treatise, Nelson Mandela Metropolitan University, 2009.

[14] J. Coertze, "A framework for information security governance in SMMEs," Master's Dissertation, Nelson Mandela Metropolitan University, 2012.

[15] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.

[16] O. Hoppe, J. Van Niekerk, and R. Von Solms, "The effective implementation of information security in organizations," in *Proceedings of the IFIP TC11 17th International Conference on Information Security. Visions and Perspectives*. Deventer, The Netherlands: Kluwer, B.V., 2002, pp. 1–18.

[17] C. Vermeulen and R. Von Solms, "The information security management toolbox - taking the pain out of security management," *Information Management & Computer Security*, vol. 10, no. 3, pp. 119–125, 2002.

[18] R. Von Solms and S. Von Solms, "Information security governance: Due care," *Computers & Security*, vol. 25, no. 7, pp. 494–497, 2006.

[19] M. Gerber and R. Von Solms, "From risk analysis to security requirements," *Computers & Security*, vol. 20, no. 7, pp. 577–584, 2001.

[20] Y. Barlette and V. Fomin, "Exploring the suitability of IS security management standards for SMEs," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. Ieee, 2008, pp. 308–308.

[21] ISO/IEC 27001, *Information technology: Security techniques - Information security management systems - Requirements*. Switzerland: International Organization for Standardization (ISO), 2005.

[22] S. Bacik, *Building an Effective Information Security Policy Architecture*. CRC Press, 2008.

[23] S. Posthumus, R. Von Solms, and M. King, "The board and IT governance : The what, who and how," *South African Journal of Business Management*, vol. 41, no. 3, pp. 23–32, 2010.

[24] InfoSec Institute, "ISO27002 security framework audit program template," 2012. [Online]. Available: http://resources.infosecinstitute.com/iso27002-template/

[25] L. Megginson, M. Byrd, and W. Megginson, *Small business management: an entrepreneur's guidebook*, 5th ed. New York, USA: McGraw-Hill/Irwin, 2006.

[26] J. Devos, H. Landeghem, and D. Deschoolmeester, "Rethinking IT governance for SMEs," *Industrial Management & Data Systems*, vol. 112, no. 2, pp. 206–223, 2012.

[27] ISO/IEC 38500, *Corporate governance of IT*. International Organization for Standardization (ISO), 2008.

[28] J. Coertze, J. Van Niekerk, and R. Von Solms, "A web-based information security management toolbox for small-to-medium enterprises in Southern Africa," in *Information Security for South Africa*. IEEE, 2011, pp. 1–8.