A web-based information security management toolbox for small-to-medium enterprises in Southern Africa

Jacques Coertze, Johan Van Niekerk and Rossouw Von Solms
School of Information Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa

***Abstract*—Many small-to-medium sized enterprises are finding it extremely difficult to implement proper information security governance due to cost implications. Due to this lack of resources, small enterprises are experiencing challenges in drafting information security policies as well as monitoring their implementation and compliance levels. This problem can be alleviated by means of a cost effective "dashboard system" and automated policy generation tool. This paper will critically evaluate an existing policy generation tool, known as the Information Security Management Toolbox, and will propose improvements to this existing system based on changes in both information security standards and business needs, since the development of the original system.**

***Index Terms*—computer security, automation, computer software, information security, corporate governance, enterprise security, IT governance, managing information security, methodologies for securing small/medium size enterprises, security policy and procedures.**

I. Introduction

Information has become a critical business asset to any organization whether small, medium or large, and forms the life-blood of most organizations [1, p. 408], [2, p. 174]. Information today offers many benefits to an organization such as providing a competitive edge, allowing for economic prosperity or providing real-time reporting [3, p. 25]. There are however many security threats which could compromise information and information technology.

The threats against information and information technology are extensive and the necessity to protect against security threats is more and more eminent. The importance of managing security risks within an organization is very important, providing such protection is one of the key components of corporate governance [4, p. 5], [5, p. 5].

"Corporate governance can be defined as the system (policies, laws, customers etc.) by which an organization is directed and controlled" [5, p. 5]. A sub-component of corporate governance is IT governance that is defined as "consisting of the logical and organizational structures that ensure that an organizations' IT is sustained and extends the business strategy and vision" [6]. Information security is underpinned by IT governance and although a large part of information security governance is located within the realm of IT governance, some parts are found elsewhere as well [4, p. 18].

Information security is implemented within an organization to ensure that threats are mitigated to acceptable levels [7, p. viii]. Information security is a sub-component of information technology governance and, indirectly, of corporate governance [4, p. 18]. Establishing policies and ensuring that the necessary technical and non-technical controls are duly implemented, make up for a large portion of what information security governance and management entails [8, p. 120]. Considerable documentation exists to provide guidance and recommendations on what these controls and policies should entail.

Guidelines and standards have both come into existence to aid in establishing proper information security governance within organizations [7], [9], [10]. The international standard ISO/IEC 27002 [7] focuses most specifically on information security management. It provides for the minimum guidelines of what is expected to ensure proper information security management and it further indicates certain controls and implementation guidelines for an organization. Two guidelines that have grown in popularity are COBIT 4.1 [9] and the King 3 Report for South African based organizations [10]. COBIT 4.1 provides a best practice foundation for information technology governance within an organization and specifies what is expected. It also contains minimal information as to how the implementation should be done. Many South African based organizations are following the King 3 Report's recommendations and it has received considerable focus over the past few years. The above mentioned guidelines do not only apply to large organizations, as small-to-medium enterprises must also familiarize themselves with the contents of the above mentioned guidelines. Overall the general theme portrayed by all of these documents is that policy establishment and monitoring is core to information security governance and that it is vital for top management to provide direction as far as the protection of information is concerned within an organization. Many organizations, in particular small-to-medium enterprises struggle to draft such policies and procedures due to the lack of experience, and in many cases the lack of guidance from a well-qualified information security officer [11, p. 5].

Information security governance dictates that many policies and procedures should be drafted within an organization to ensure that the proper behavior is obtained and dictated to employees to ensure the secure usage of information and related technologies [8, p. 120], [12, p. 275]. This aspect is

a huge challenge for small-to-medium enterprises where the financial position of such organizations makes it very difficult to obtain the services of an expert on a part time or full time basis to develop policies and procedures and to guide management [11, pp. 5-6]. As a result, much research has been done in the past to assist these types of organizations in a cost effective and practical fashion with drafting policies and procedures to ensure proper information security governance [8], [13].

This paper specifically addresses the information security management system that was developed on the basis of a framework as proposed by Vermeulen and Von Solms in 2001 [8]. This system was software developed and accordingly documented by Hoppe, Van Niekerk and Von Solms in 2002 [13]. The original system was presented at the 2001 ISSA conference by Von Solms, Gerber, Van Niekerk, Hoppe, Vroom and Aenmey [14]. The paper will critically review the existing system, and the research on which it was based, and will propose changes to the existing work in order to remain current in terms of industry needs. The paper is presented in the form of a case study.

II. Methodology

This paper is presented in the form of a case study. The case study was focused on a particular framework, software implementation and usage of an information security management toolbox. Additionally, literature surveys and some arguing are used throughout the paper.

"Case studies represent intensive, detailed description and analysis of a particular project or program in the context of that project's environment. This makes case studies a valuable way to share the experiences of others who have travelled the road before. Case studies are extremely useful for encouraging discussion about best practices and problem-solving strategies" [15]. Case studies usually follow a specific structure and in this paper the guidelines and structure as set by Cresswell [16, pp. 73-80] will be followed.

The structure set out by Cresswell is as follows:

- Entry vignette;
- Introduction;
- Description of the case and its context;
- Development of issues;
- Detail about the selected issues;
- Assertions; and
- Closing Vignette

This paper will follow the structure of a case study. The next section will introduce the Information Security Management Toolbox. Subsequent sections will continue to describe the particular details of its implementation as well as the framework on which it was based and the limitations that have been identified pertaining to the toolbox will be highlighted and discussed in detail. The paper will conclude with the establishment of a set of criteria to be used for the "next generation" toolbox.

III. Introduction of the Information Security Management Toolbox

An original version of the toolbox was proposed and developed by Hoppe et al. [13]. The original version was demonstrated at the inaugural ISSA conference by Von Solms et al. [14]. This paper forms part of a project which critically reviews the earlier work in light of changes in both security standards and in business needs over the past decade. Hoppe et al.'s essential contribution is the concept that a stand-alone desktop application can be developed to assist small-to-medium enterprises in proposing the necessary information security policies and procedures as outlined by the mentioned standards and guidelines. It has become known as "The Information Security Management Toolbox" and was designed around the framework proposed for such a system, documented by Vermeulen and Von Solms [13, p. 12]. Both the framework and desktop implementation have become outdated due to the subsequent revision of BS7799 Part 1 and COBIT (due to the frequent enhancements in the information technology environment), but most of the original procedural concepts still apply and can be reused in future implementations.

It should however be noted that many limitations have come into existence due to the change seen within the requirements for small-to-medium enterprises when analyzing the framework and desktop implementation.

The following sections will provide more detail about the toolbox and framework and greater insight into the limitations that have been identified. It will end by providing a set of criteria that can be used for next generation toolbox implementations.

IV. Description of the Information Security Management Toolbox and its Context

As mentioned earlier, the Information Security Management Toolbox developed by Hoppe et al. was based on the framework established by Vermeulen and Von Solms [8]. It must however be mentioned that the toolbox aims at automation of steps within the analysis and development phases of a methodology that was developed by Vermeulen and Von Solms [8, p. 123]. The next section will provide an overview of the methodology and subsequently the framework will be discussed. The section will end with a detailed discussion of the current desktop implementation of the information security management toolbox.

A. The Information Security Management Methodology

The framework proposed by Vermeulen and Von Solms was based directly on a methodology that was created for the establishment and maintenance of an integrated information security management system. A model for it was presented within research in conjunction with the framework [8, p. 123].

The studied methodology is comprised of six phases for the implementation and management of information security, they include:

- Introductory Phase;
- Initial Phase;
- Analysis Phase;
- Development Phase;
- Implementation Phase; and
- Continuation Phase

These phases form an outline for the implementation of an information security management system. To comprehend the model it is necessary to determine the steps required for the completion of each of the phases and these steps will be identified next.

1) Introductory Phase: The objective of this phase is to put the core elements of information security management into place. These elements comprise the steps that will be required to support the entire information security management process, during its implementation and on an ongoing basis.

The Introductory Phase is comprised of two steps, they include:

- Gain top management commitment; and
- Consult information security standards

2) Initial Phase: The Introductory Phase is responsible for establishing steps that will contribute towards the introduction of information security. The objective of the Initial Phase is to complete the preparation stage of information security management and allow for its subsequent implementation in the organization.

In the initial phase, the implementation of information security is delegated to lower management. Taking this into account, the steps comprising the Initial Phase are:

- Appoint an information security officer;
- Establish an information security forum; and
- Define security vision and strategy

3) Analysis Phase: The Introductory Phase and the Initial Phase prepares the organization for implementation of information security management. Having created the foundation for the implementation of information security management, the Analysis Phase begins the process leading up to implementation. The objective of the Analysis Phase is to determine the security requirements of the organization.

The following steps are proposed as necessary for the accomplishment of the goals of the Analysis Phase:

- Determine scope of the ISMS;
- Determine key role players;
- Interview key role players; and
- Determine security requirements

Once all the above mentioned steps have been successfully completed, the objective of the Analysis Phase has been accomplished, namely to determine the security requirements of the organization.

4) Development Phase: The Analysis Phase identifies the security requirements that define the information security needs of the organization. Proper planning is required to ensure that a well-structured process is followed. For this reason the Development Phase of the proposed methodology is required. The objective of the Development Phase is to evaluate the security requirements and use this information to determine in what way information security management will be implemented in the organization.

The follow steps are proposed to allow for the accomplishment of the above mentioned objective:

- Planning the information security policy structure;
- Information security policy preparation;
- Risk management;
- Procedure preparation; and
- Develop an information security awareness programme

5) Implementation Phase: Upon successful completion of the Development Phase, the organization is ready for the implementation of some information security management system. The goal of the Implementation Phase is to implement information security according to the guidelines provided by the documents compiled in the previous phase.

Based upon these activities, the following steps are proposed for the realization of the Implementation Phase:

- Empower responsibility framework;
- Implement safeguards according to plan; and
- Offer security awareness programme

6) Continuation Phase: The previous five phases leads up to the implementation of an Information Security Management System within an organization. It is however vital that support be provided throughout the implementation of information security. For this reason, the Continuation Phase is necessary.

The following steps are proposed to fulfill the Continuation Phase:

- Maintain Information Security Management System;
- Monitor security situation;
- Audit Information Security Management System compliance; and
- Ensure proper incident handling

The six phases that were described in this section illustrate how an information security management system can be successfully implemented using the proposed Information Security Management Methodology. This is achieved by providing implementation guidance through a structured and phased approach.

Organizations often do not have the expertise or resources to follow such a detailed methodology [13, p. 11]. For this reason Vermeulen and Von Solms established a framework that could be used to create a software tool that can automate steps of some phases within the methodology. The framework proposed will be discussed in the following section.

B. The Information Security Management Toolbox Framework

The framework for an information security management toolbox was presented by Vermeulen and Von Solms [8, pp. 123-125]. The framework was based on the information security management methodology and it was highlighted that the framework helps to automate certain fundamental steps of the analysis and development phases of the methodology.

The first step of the framework is for the users of the toolbox to complete a questionnaire consisting of a series

of information security related multiple choice questions in order to conduct some high level business analysis. The degree of information security required by an organization is characterized by security requirements which the questionnaire will identify including confidentiality, integrity, availability, authenticity and audibility.

The results of the questionnaire would then be used to determine the extent of applicability of these five security requirements to the organization. Vermeulen and Von Solms suggested that these security requirements were to be measured according to a qualitative rating of low, medium or high. A weighted calculation process would be applied to the questionnaire and subsequently the ratings of the security requirements could then be calculated.

The second step is to use the calculated/established security requirements and to determine policy statements. Using the framework each security requirement, with its rating of low, medium or high, would cause the selection of one or more policy statements. Within the framework, the relationship between them is determined by using a security requirements/policy statements mapping matrix. The framework would then automate the selection of the policy statements that are to be included as a section of the corporate information security policy document.

The third step is automated and allows the security requirements to determine which safeguards are selected. Each combination of security requirement and rating would have a selection of one or more safeguards associated with it. The collection of safeguards, at the time of writing, was selected to come from BS 7799-1 [17]. Similar to the mapping between the security requirements and policy statement, a mapping matrix exists in the framework to allow for the automated selection of safeguards known as the security requirements/safeguard mapping matrix.

The fourth step is for users to complete a second questionnaire, referring to safeguard elimination. When completed and captured it will evaluate the applicability of certain safeguards by determining the systems and services present in the organization that may affect them. Again this will allow for the automated elimination of certain safeguards and the information concerning the elimination of these is stored in the security requirements/safeguard mapping matrix.

The fifth and last step is highlighted by the framework as being the automated establishment of procedures pertaining to the safeguards selected by the third and fourth step. Each safeguard has a set of one or more security procedures associated with it and the relationship between the safeguards and security procedures are static.

The overall goal of the framework is to automate certain steps of the information security management methodology, which was discussed previously and more specifically to address the automation of proposing of policies and procedures. It must however be mentioned that it is merely a high-level framework/model and is simply a conceptual idea for use by small-to-medium sized enterprises.

Hoppe et al. identified that the framework could be used by a stand-alone desktop application to afford the automation of proposing information security policies and procedures for SME's [13, pp. 11-12]. An implementation was attempted within the same year as which Vermeulen and Von Solms established the framework and a successful prototype was developed for a live-demo at the ISSA conference in 2001 [14]. In the next section the history and implementation details of the application will be discussed.

C. The Information Security Management Toolbox Desktop Implementation

The methodology and framework discussed proposed an implementation model that was used as the basis for the development of an automated software tool to guide the establishment and preservation of information security management in an organization.

The software package carries the working title of the Information Security Management Toolbox (ISMTB). The package provides services in assisting information security management and is an electronic aid providing both interactive elements and textual elements. The content included within the ISMTB was provided by several other research projects [13, p. 17]. The primary objective of the ISMTB is to assist in ensuring the realization of the proposed methodology, thereby effectively addressing the identified security requirements of the organization in a structured and integrated manner. The ISMTB assists in this regard by allowing the automation of the process of identifying and selecting security safeguards and thereby dynamically generating the appropriate security documents required to enforce information security.

The ISMTB was implemented as a stand-alone desktop application using a three-tier software architecture within a file sharing environment [13, p. 12]. The primary reason for the architecture was to obtain the benefits of a client/server implementation while executing the ISMTB within a local desktop environment. It must however be mentioned that such a client/server communication architecture was never implemented.

The ISMTB was later provided to a local software development firm to update and in some cases redevelop to conform to best practices in the field of computer programming. Even though the software package was updated in this manner, the actual workings remained the same. The standard on which the ISMTB was based was initially BS 7799 Part 1, but it has subsequently been updated to ISO/IEC 17799 [18]. The questions within the business analysis questionnaire have also been refined over time to be clearer and to map more clearly to the security requirements.

It must be noted that Hoppe et al. did not document in detail the overall workings of the toolbox, although one can argue that the framework provided by Vermeulen and Von Solms described the workings, but the complex mechanisms that were designed to automate the various phases of the proposed methodology has been. Due to this fact the next section will discuss these complex mechanisms.

The ISMTB consists of an introduction module that is responsible for introducing the application users to the concept of information security as well as emphasizing the importance of adhering to a structured and disciplined process when implementing an Information Security Management System. This was implemented using a hypertext approach, presenting the information as a series of hyperlinked web pages that are installed, with the ISMTB, on the client's local desktop environment [13, p. 13].

Although the Introduction module introduces the application users to the concept of information security, it does not provide a means for identifying and proposing a set of security controls. This aspect is implemented in terms of an interactive wizard that serves to automate the steps of the Analysis and Development Phases of the methodology [13, p. 13]. The primary objective of the wizard is to propose a set of modifiable security safeguards to address information security needs of the organization.

For the process of security requirements analysis it was determined that business requirements could be gained using interviews [13, p. 14]. The interviews were to entail key role players within an organization. These interviews would be performed using a high level business analysis questionnaire. Based upon the outcome of the questionnaire, the security requirements would be determined.

Hoppe et al., Vermeulen and Von Solms agreed that in order to assess the importance of security requirements, each security requirement should be referred to by a number of questions in the questionnaire [8, p. 123], [13, pp. 13-14]. Due to this reason a many-to-many relationship exists between security requirements and business analysis questions. The answers selected for each of these questions will determine what rating each associated security requirements will have.

A weighted value system was introduced due to the fact that there is no direct relationship between the ratings of security requirements and the answers of the questions. The weighted value system allows for a calculated process to determine the security requirements for the organization.

Once the security requirements are identified, a series of security controls are presented to the organization. These security controls, as proposed by BS7799-1, are formulated by means of a lookup matrix which maintains a mapping between the various security requirements and their associated security controls. Each security control contains a set of associated security procedures which serve as a guideline for achieving the objectives of each security control. It must however be mentioned that when secondary policies are drafted by the toolbox, that these procedures are all presented. This has led to the confusion that all procedures must be followed and implemented, which may not always be the case.

It was determined that users must be able to select or de-select security controls from the set automatically selected by the toolbox [13, pp. 14-15]. For this reason the toolbox provides an interface that allows users to achieve this, but they must provide a legitimate reason in accordance to the statement of applicability proposed by BS7799-1 when performing such actions.

As mentioned earlier due to changes in the requirements of small-to-medium sized organizations for information security and software development technologies have led to the realization that limitations exist within the framework and toolbox. Now that the background information of the toolbox and framework is known, these limitations will be explored in the following section and a more detailed analysis will follow.

V. Limitations Identified with the Information Security Management Toolbox

The effectiveness of the framework and desktop implemented toolbox has been proven to address the information security management system requirements of small-to-medium sized organizations in the past [8, p. 125]. Today these requirements however have substantially changed and therefore limitations and changes have been identified to fit the current technology framework and business approach.

The framework was aimed towards management of information security. Due to this fact it produced information security policies and procedures based on security requirements established through a business risk analysis. This provides the direct component of governance/management to be present within an organization, but without a control component such a framework is highly limited in its effectiveness today [1, p. 411]. To be effective, a policy must be supported by some way of measuring compliance [1, p. 411], [4, p. 44]. For this reason the framework requires a control component that can assist in this matter. This issue is also present within the toolbox.

The toolbox developed and subsequently updated has seen some minor changes, but the essential functionality offered has remained the same. As mentioned above one of the issues that are present is the lack of a control component, but additional limitations have also been identified with it. It was developed as a stand-alone desktop application for security reasons and it was envisioned that a client/server architecture were to be established. The installation and updating of the application has been identified to be a problem, because individuals using the application need to manually install and update the application. A further limitation is the fact that it is statically developed against the BS 7799-1 standard. Although it has been updated to provide policies and procedures in accordance to ISO/IEC 17799, no effort has been made to afford dynamic changing of the standard. The limitation therefore is that the standard on which it is based cannot easily be changed and the effectiveness of the application has become troublesome. It was originally developed to be used by consultants in the information security field when assisting organizations. Due to cost implications for small-to-medium organizations, and the limited reach of such an approach, it has been decided that a new "self-help" web-based version would be more desirable.

In view of the limitations now identified, the next section will offer an in-depth analysis of these and provide possible solutions or enhancement to mitigate them.

VI. In-Depth Analysis of the Limitations of the Information Security Management Toolbox

It has been clearly mentioned that limitations have been identified with the framework and the information security management toolbox. The aim of this section is to provide a detailed description of each limitation and to propose possible solutions that can be introduced into a "next generation" version of the toolbox. This is regarded as essential to ensure that the current requirements are met for a information security management system in small-to-medium sized organizations.

This section is divided into two subsections, whereby the first portion addresses the framework's limitations and the second the toolbox's limitations.

A. The Information Security Management Toolbox Framework

The framework is very comprehensive and has been proven to be effective [8, p. 125]. As already mentioned it offers functionality for automating the proposing of information security policies and procedures, which directs an organization in terms of information security by providing a clear vision and dictating behavior. Although the framework excels in this regard, it does not address any control aspects.

Governance consists of two components namely: directing and controlling [1, p. 409], [5, p. 5]. Directing ensures that a vision is defined and that behavior is prescribed to the parties involved. Control is necessary to ensure that the vision and dictated behavior is followed and if not that corrective actions are taken. For this reason it can be seen essential that the framework incorporates control aspects.

Due to the fact that the framework is based on a standard and automates safeguard selection makes it somewhat simple to introduce aspects of control/compliance. A possible solution that can be followed is to utilize the safeguards and company standards or procedures. Each safeguard and company standards or procedure will dictate that specific information can be captured to determine compliance. Normally such information is included in compliance clauses present within these company standards, the information security policies and statements. Some might require manual capturing methods and other electronic methods. Irrespective the concept would be to capture such information and then to use the standard and company defined compliance specifications to determine whether compliance is being met. Such an approach has been researched[1] and it is envisioned that a similar system can be established for the framework and toolbox implementation.

The analysis and improvement of the current framework forms part of the same larger research project as this paper. However, these issues fall outside the scope of the current paper which focuses specifically on the toolbox itself. It must however be mentioned that future research specifically focusing on the framework itself will be of a high value to bettering the toolbox implementation.

[1]A prototype proof of concept system that was developed based on an open software approach. All development was done by Francois Meyer.

The framework primarily has only one major limitation currently and that has been identified as being compliance measuring and control. The next section will address the limitations of the desktop implemented toolbox.

B. The Information Security Management Toolbox Desktop Implementation

Many limitations have been identified with the current toolbox implementation. These limitations span from the vision of usage to the computer architecture that was used and beyond. This section aims to provide insight into these limitations.

The previous section outlined that the framework is lacking in providing any control mechanism(s) and this limitation is also present within the toolbox since the inner workings was based upon this framework. As indicated, the safeguard selection and information security procedures and policies can be used to devise a compliance measuring and monitoring system.

For future toolbox implementations it was decided to create a dashboard system that will work in tandem with the proposing of policies and procedures. The dashboard system allows users to enter compliance metrics to indicate what the organization would prefer in order to achieve a specific compliance measurement (as a score out of 10). This information will be captured during the process of safeguard selection and the automation of proposing relevant procedures and policy statements. For each metric a monitoring interval time will be established and when that interval is reached, the dashboard system will indicate that the information for compliance must be gathered. Using the information the dashboard system will prompt the user to enter a rating score out of 10 in respect of compliance. Take note that the dashboard system does not automate the gathering of this information, but simply depends on the manual entry thereof. The overall goal of the dashboard system is to generate simple graph reports for management, which will indicate the current compliance levels versus its information security vision. The result of analyzing such reports will allow management to easily determine whether the organization as a whole is following the vision for information security and to take corrective action where necessary.

The original vision was for consultants to use the toolbox as a tool during one-on-one consultations with organizations. Organizations are experiencing it very costly to hire consultants on a regular basis in order to assist them with their information security requirements [11, p. 6]. For this reason, the cost effectiveness of the current format and use of the toolbox is no longer adequate for small-to-medium sized organizations and a change in the vision of usage is certainly required. This "new" vision is for the toolbox to become an affordable, easy to access, "self-help" tool, that is always up to date in terms of the latest information security standards and controls. Although it can be argued that the current desktop implementation can be adapted to conform to such requirements, the desktop architecture has additional limitations as well which makes it feasible to re-evaluate the architecture. After careful consideration, it was decided to change the current architecture to a

web application architecture. The web application architecture provides advantages that are not necessarily obtainable by desktop application architecture.

Some of these advantages include [19]:

- No special configuration or changes are needed on user's computers;
- Lower costs;
- Centralized data is secure and easy to backup;
- Updates can be made quickly and easily;
- Information is accessible to a wide audience anywhere in the world;
- Available 24 hours a day, 7 days a week;
- Always up-to-date; and
- Cross-platform capability

The web application architecture addresses another limitation that was identified with the toolbox. The toolbox installation and maintenance is currently problematic due to the fact that a consultant needs to manually install it onto either his/her own computer or onto an organization's computer(s). This leads to organizations or the consultant using an outdated version, even though a newer version might be available. Mainly this is caused by the fact that there is no centralized access point where updates and installations are stored. In the event of a new version being introduced, the consultant currently has to update the application manually on his own computer and subsequently onto the computer(s) at the organization. Using the web application architecture, this tedious process will in future be eliminated due to the fact that updates to the toolbox will be made at a central location and users accessing the web application subsequently will automatically view the latest updated version. The only problem that might influence the automatic view of the updated version might be when the website is cached on a local server at an organization or on the user's computer, but modern web technologies allow for this to be mitigated to a large extent. Additionally the web application architecture will offer a user-centric solution for the toolbox, since organizations will have direct access to it. This will also make the toolbox cost effective, since a consultant will not be required on a frequent basis for updating it. This will reduce the dependence on consultants, although the aid that they offer will still be required from time to time.

Additionally, the toolbox is currently statically developed against ISO/IEC 17799 [18]. It will be updated to the new revised version of ISO/IEC 27002 [7], but it must be emphasized that the requirement for dynamic changing of the standard is currently a limitation. Currently the toolbox does not offer any means for changing the standard other than changing the actual source code. Design patterns in software development have become very popular and their usage can greatly increase the dynamic nature of the toolbox and assist greatly in future maintenance as well [20]. It is advisable in future that design patterns should be introduced and followed during the web application implementation of the toolbox. This introduces the advantage of dynamically changing the standard on which the toolbox is based and further the maintenance required for the upkeep of the toolbox will be simplified and cost effective.

As indicated by this section, the desktop implementation of the toolbox has some limitations that have come to be known, similarly the framework on which it was based also has a major limitation in terms of compliance monitoring and measuring. It was highlighted that these limitations will be mitigated by means of implementing a newly improved toolbox using web application architecture. The next section will briefly summarize the improvements envisaged as far as the framework and toolbox is concerned and will address criteria to apply to "next generation" toolbox implementations to ensure that the requirements of small-to-medium sized organizations are embraced.

VII. Criteria for an Information Security Management Toolbox

As discussed in the previous section, improvements are foreseen to be made to both the framework and toolbox. This section will provide a summary of the proposed improvements that will be implemented as well as the key criteria that should be put in place to ensure the successful implementations of the envisaged enhanced toolbox.

The toolbox should be web-based in order to ensure easy maintenance and access to it. Possible technologies that can be used in this matter are: ASP.NET MVC, Silverlight and/or possibly Flash. Overall the goal of changing the architecture to a web based architecture will be to allow for a user-centric solution and to address the cost effectiveness of usage thereof.

The need that the toolbox must be part of a larger information security web portal has been identified. The reason for this realization is that the toolbox alone cannot function adequately at addressing all the organizations information security requirements. It is important that a holistic approach is to be followed by means of a web portal to ensure that all aspects of information security are addressed e.g. the introduction process, the awareness by means of training and education, the implementation of policies and procedures and subsequent compliance level monitoring. This can be seen as essential to ensure that the toolbox is not envisaged as being a stand-alone solution for the above mentioned matters, but is an integral part of a larger product.

Due to the fact that a web based solution will be introduced it is envisaged that access to certain areas of the toolbox will have no cost implications, but access to other levels may require a subscription fee in order to cover maintenance and administration costs. This will ensure the toolbox to be cost effective in comparison to acquiring the services of a consultant, hence resulting in more organizations becoming more compliant in the field of information security management.

The following key aspects have now been identified as important criteria to be followed for the future implementations of the toolbox:

- It must be cost effective and user-centric;
- It must be web-based instead of desktop oriented;
- It must be part of a larger information security web portal; and

- Compliance monitoring and evaluation must be implemented

It is essential that these issues are kept in mind and addressed during the development of future toolboxes to ensure the success thereof at addressing the requirements in respect of information security management of small-to-medium sized organizations.

VIII. Conclusion

To conclude this paper outlined a problem that exists with small-to-medium sized organization where they lack the cost effective resources to implement proper information security management and governance.

It indicated that research was done in the past to assist in this regard and specifically highlighted a framework that was established for the automated proposing of policies and procedures for an information security management system. It continued by providing insight into an information security management toolbox that was developed based on the framework.

Certain limitations were discussed that have been identified with the framework and toolbox due to changes seen in the requirements of small-to-medium sized organization and also in the development technology. These limitations included compliance monitoring and measuring, the development architecture of the toolbox, the vision of usage and usage of design patterns for offering dynamic changes.

Recommendations were made as to how these limitations could be addressed and criteria were provided to be followed in future toolbox implementations to ensure the success thereof. Mainly the proposal entailed changing the desktop implemented toolbox to a web-based application that forms part of a larger web portal. Emphasis was also placed on the fact that future toolbox implementations must be cost effective and user centred.

References

[1] R. Von Solms and B. Von Solms, "Information Security Governance: A model based on the DirectControl Cycle," *Computers & Security*, vol. 25, no. 6, pp. 408–412, Sep. 2006.

[2] R. Von Solms, "Information security management (1): why information security is so important," *Information Management & Computer Security*, vol. 6, no. 4, pp. 174–177, 1998.

[3] 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.

[4] S. H. V. Solms and R. V. Solms, *Information Security Governance*. Springer, 2008.

[5] P. Williams, "Information Security Governance," *Information Security Technical Report*, vol. 6, no. 3, pp. 60–70, Sep. 2001.

[6] IT Governance Institute, *Board Briefing for IT Governance, 2nd Edition*. Information Systems Audit and Control Association, 2003.

[7] *Information technology - Code of practice for information security management*, ISO/IEC Std. 27 002, 2005.

[8] 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.

[9] IT Governance Institute, *Cobit 4.1*. ISACA, 2007.

[10] Institute Of Directors in Southern Africa, *King III Report on Corporate Governance*, Parklands, 2009.

[11] E. Yeniman 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*, Nov. 2010.

[12] R. Von Solms and B. Von Solms, "From policies to culture," *Computers & Security*, vol. 23, no. 4, pp. 275–279, Jun. 2004.

[13] O. A. Hoppe, J. Van Niekerk, and R. Von Solms, *The Effective Implementation of Information Security in Organizations.* Massachusets: Kluwer Academic Publishers, 2002, ch. Information Security Management, pp. 1–18.

[14] R. Von Solms, M. Gerber, J. Van Niekerk, O. Hoppe, C. Vroom, and K. Aenmey, "The information security management toolbox: A practical guide," 2001.

[15] "Case studies," *[WWW document]. URL "http://www.freedomtoaster.org/CaseStudies" Cited 27 April 2011.*

[16] J. W. Creswell, *Qualitative inquiry & research design: choosing among five approaches*, 2nd ed. Sage Publications, 2007.

[17] *A Code of Practice for Information Security*, British Standards Institute Std. 7799-1, 1995.

[18] *Information technology - code of practice for information security management*, ISO/IEC Std. 17 799, 2000.

[19] P. Stanley, "Advantages of web applications," *[WWW document]. URL http://www.pssuk.com/AdvantagesWebApplications.htm Cited 26 April 2011.*

[20] E. Freeman, E. Freeman, K. Sierra, and B. Bates, *Head First design patterns*. O'Reilly Media, Inc., 2004.