Best practices show the way to Information Security Maturity

MM Lessing

Council for Scientific and Industrial Research, South Africa

Summary: *The importance of Information Security cannot be emphasised enough. It is therefore necessary to ensure that organisations comply with Information Security guidelines. This compliance ensures a high level of maturity.*

An amalgamation of a number of industry best practice documents relevant to Information Security and Information Security Governance forms a best practice driven Information Security Governance model. Theoretically, the implementation of the best practice driven model should lead to excellent Information Security within an organisation.

A Security Maturity Model (SMM) provides an organisation with a distinct Information Security framework. Organisations that conform to these models are likely to pursue satisfactory Information Security. Additionally, the use of Security Maturity Models promotes the use of best practice standards that generally lead to proper Information Security Governance.

Based on these two assertions, the hypothesis of this article is that the best practice driven Information Security Governance model is analogous to a Security Maturity Model. Accordingly, organisations can implement the best practice model as a sole tool to ensure Information Security Maturity. This article proves the hypothesis by extracting characteristics from various industry Security Maturity Models and developing a generic Security Maturity Model. The best practice driven model then maps onto the generic Security Maturity Model to prove the analogy. The premise of this study is that the best practice driven Information Security Governance model conforms to all the requirements of the generic Security Maturity Model. The conclusion is that the proper implementation of this model leads to a high Information Security Maturity level.

1. Introduction

In today's working environment, information is not only a key organisational asset, but also a crucial ingredient in gaining competitive advantage. In many cases, information drives most business processes, and involves employees from all rankings: from top management to entry-level employees [1]. Many organisations have a growing dependence on their information systems, ensuring that Information Security Governance has an increasingly important part of the organisational management [2]. As a result, Information Security is very important and cannot be emphasised enough.

The hypothesis of this article is that a best practice driven model for Information Security Governance is similar in features and characteristics to a Security Maturity Model. Therefore, the implementation of the best practice model as the sole tool in an organisation can ensure Information Security Maturity.

To show that best practices can indeed show the way to Information Security Maturity, it is necessary to define some of the concepts.

2. Definitions

2.1 Information Security Governance

Information Security Governance is a broad but poorly understood discipline. EBS [3] provides the following definition: *"... A subset of enterprise governance that provides strategic direction, ensures achievement of objectives, manages risks appropriately, uses organisational resources in a responsible way, and monitors the success of* (the) *enterprise security programme"*. A more refined definition is *"... the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems"* [4].

Due to its omnipresent nature, Information Security Governance seems a very broad discipline. The discipline covers a number of specific organisational aspects, including:

- complexity associated with both IT and associated security;
- widespread use of technology;
- interconnectivity between systems;
- growing potential for misuse of information systems;
- rapid rate at which new technology is developing and old technology is becoming obsolete;
- the influence of Information Security on the organisation's public image;
- growing relation between the financial sector and Information Security;

- increased mobility of the workforce, increasing speed and flexibility with which tasks are performed;
- legal liability for securing information assets;
- increased consumer involvement in technology operations; and
- increasing number of vulnerabilities in security products and technology [5].

Information Security Governance leans strongly on both Corporate Governance and Information Technology Governance.

2.2 Best practice driven Information Security Governance model

Best practice documents contain the best practices as set out by prominent discipline leaders, both organisations and individuals. They make these documents available to govern the Information Security environment successfully. Many of these documents allow for internationally recognised certification following complete guideline implementation.

Best practice documents guide organisations in establishing an effective governance structure. It also helps to measure compliance against the document's guidelines. The implementation of a best practice document therefore ensures that an organisation covers all relevant aspects that can influence Information Security. An organisation following best practice guidelines is more prone to a successful Information Security Governance structure. Organisations are also more likely to succeed in the corporate environment when they build on the experience of other organisations [6]. Organisations can save large amounts of resources by implementing best practices [7].

In a previous study [8], a model for best practice driven Information Security Governance was developed. This is in direct response to the benefits a comprehensive best practice driven Information Security Governance model can provide. The best practice driven model is an amalgamation of a number of industry best practice documents relevant to Information Security, covering all possible angles of Information Security and Information Security Governance. This Information Security Governance model is compiled from the most prominent aspects of a number of best practices, acts and regulations from a number of related governance frameworks.

In the *Corporate Governance discipline*, the King II Report, Organisation for Economic Co-operation and Development (OECD) and the Sarbanes-Oxley Act (SOX) serve as basis documents. In the *Information Technology Governance discipline*, the Control Objectives for Information and related Technology 3 (COBIT) and the Information Technology Infrastructure Library (ITIL) serve as basis documents. The last governance framework is the most important for this model: in the *Information Security Governance discipline,* the ISO/IEC 27002:2007 and the Standard of Good Practice for Information Security serve as basis for the best practice driven model. The final best practice driven Information Security Governance model includes the following drivers:

- asset management;
- business continuity management;
- certification;
- compliance management;
- control needs and objectives;
- corporate and criminal accountability;
- critical business applications;
- digital forensics;
- disclosure mechanisms;
- ethical aspects;
- information system development;
- legal requirements;
- organisation and management of Information Security;
- performance measurement;
- personnel security management;
- physical and environmental security;
- risk management;
- security management; and
- shareholder treatment.

An organisation's Information Security is considered adequately managed once all these aspects are covered. An implementing organisation can be assured of comprehensive Information Security Governance.

2.3 Security Maturity Model

A maturity model is a structured collection of elements that describe certain aspects of maturity in an organisation. This type of security model indicates the degree of development and the strength of the organisation's security measures, and provides an organisation with a distinct security framework. The development and application of Security Maturity Models enable organisations to:

- generate reproducible and valid measurements;
- establish actual progress in the security milieu;
- rank themselves against a range of organisations;

- determine the order in which security controls should be applied; and
- determine the resources needed to apply to the security programme [9].

In essence, Information Security Maturity is present when a continuous assessment of maturity ranking indicates a distinct level of full development concerning Information Security. Additionally, an organisation with Security Maturity can be expected to respond to any Information Security related circumstances in an appropriate manner.

Allard [10] developed a generic characterisation of maturity levels, with Level 1 being the most undeveloped level and Level 5 the most mature level. Level 1, *Blind Trusting*, is the initial start-up stage. Level 2, *Repeatable*, may present a disciplined process towards Information Security. This level is characterised with *ad hoc* tries. Level 3, *Defined*, shows standard, consistent processes and the development of policy documents. Level 4, *Managed*, is an evolutionary stage. This level allows management to predict the outcomes of most processes. Level 5, *Maintenance*, reveals the maintenance activities to ensure Information Security Maturity. Although this is a generic representation, it can easily be applied to security maturity as well.

The objective of a maturity model is to decrease the amount of risk together with the amount of effort put in by the organisation. Figure 1 presents this relation.

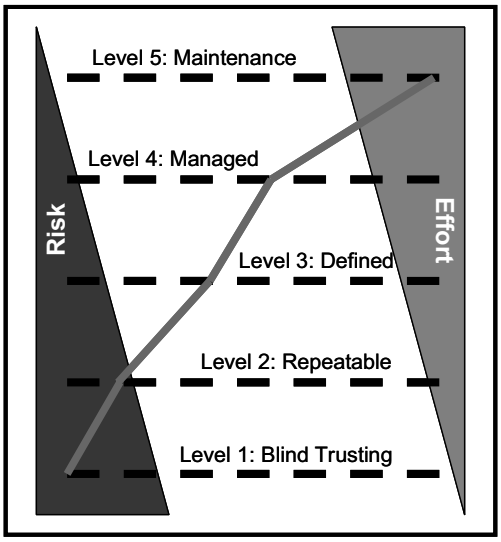

Figure 1: A generic Security Maturity Model [11]

The importance of a maturity model is that it allows organisations understanding of where skill gaps may exist. It allows them to fill those gaps in an efficient manner [12]. In addition, a maturity model allows organisations to benchmark themselves against diverse organisations and indicates the order in which to implement security elements. Maturity models promote the use of best practice standards. An organisation's maturity level is a good predictor of e-governance preparedness [13].

The benefits of implementing a Security Maturity Model are far ranging. The most prominent benefit is an improved customer and stockholder's trust in the organisation. This helps organisations to avoid non-technical security risks, thus setting an environment where there are no weak links [14].

3. Motivation

The best practice driven Information Security Governance model is an existing guidance model for organisations. This model is a comprehensive integration of industry best practice documents relevant to Information Security and Information Security Governance. To promote the adoption of this model into industry, the author compares this model to a Security Maturity Model.

The hypothesis of this article is that the best practice driven Information Security Governance model is analogous to a Security Maturity Model. Therefore, the best practice driven model does not only have its own advantages as inherited from the base best practice documents, but now also present advantages from a Security Maturity Model perspective.

To do a comprehensive analogy, this article constructs a generic Security Maturity Model from a number of randomly selected industry Security Maturity Models. The best practice driven model then maps onto this generic Security Maturity Model to determine the degree of overlap between the models. The intention of this article is not to create yet another Security Maturity Model, but rather to prove that the existing best practice driven model can be classified as a Security Maturity Model. Therefore, the objective is not to promote the use of the generic Security Maturity Model, but to use this model only for comparison reasons.

Leading to the idea of classifying the best practice Information Security Governance model as a Security Maturity Model, was the Cadbury Report of 1992 (Financial Aspects of Corporate Governance Report). This report was the first series of guidance documents designed to encourage a governance structure by adhering to guidelines set out in best practice documents.

The concept of using either a best practice document or a SMM re-enforces Gary McGraw's idea that security should be build into a system, and not only considered once the system is completed. Technically, the SMM should form an integral part of the software engineering cycle, to ensure that Information Security and security maturity are considered right from the beginning of the development stages and incorporated consistent with the purpose of the organisational software [15].

4. Creating a generic Security Maturity Model

A number of industry Security Maturity Models exist and will be used as the foundation for the generic Security Maturity Model. These models first need to be introduced, then compared and finally analysed to create a comprehensive Security Maturity Model that represents the average industry Security Maturity Model.

4.1 Introducing industry Security Maturity Models

The goal of Information Security Management is to prevent and mitigate Information Security attacks, errors and accidents. These incidents can expose information systems and the organisational process supported by them [16]. Since the management and governance of Information Security is of such importance to most organisations, a number of industry related Security Maturity Models were developed. Table 1 shows the Security Maturity Models considered for this process, with their respective focus areas.

Table 1: Security Maturity Model focus

Security Maturity Model
Information Security Management Maturity Model (ISM3) ***Focus**: Process integration*
IBM Information Security Framework (IBM-ISF) ***Focus**: Gap analysis*
National Institute of Standards and Technology Computer Security Expert Assist Team Security Maturity Model (NIST CSEAT IT SMM) ***Focus**: Documentation*
Gartner's Security Model ***Focus**: Large organisations*
SUNY's Information Security Initiative (SUNY ISI) ***Focus**: Information protection*
Systems Security Engineering Capability Maturity Model (SSE-CMM) ***Focus**: Security engineering and software design*
Computer Emergency Response Team/Chief Security Officer Security Capability Assessment (CERT/CSO) ***Focus**: Quality relative to documentation*
Community Cyber Security Maturity Model (CSMM) ***Focus**: Community effort and sharing*

Table 1 shows eight industry Security Maturity Models, each with a different focus area. This comprehensive representation of focus areas ensures a well-represented, inclusive generic Security Maturity Model.

4.2 Comparing industry Security Maturity Models

This section compares the levels of the respective models' levels. The comparison can be merged into a single comprehensive table, but is split into five separate tables to present only one level at a time. Most of these models have five levels, whilst two models only have four levels. In these instances, Level 4 is the highest available maturity.

Table 2: Security Maturity Models – Level 1

Security Maturity Model	Industry model Level 1 description
ISM3	Undefined
IBM-ISF	Initial
NIST CSEAT IT SMM	Policy
Gartner's Security Model	Blissful ignorance
SUNY ISI	Responding to basics
SSE-CMM	Performed informally
CERT/CSO	Exists
CSMM	Security aware

Table 3: Security Maturity Models – Level 2

Security Maturity Model	Industry model Level 2 description
ISM3	Defined
IBM-ISF	Basic
NIST CSEAT IT SMM	Procedure
Gartner's Security Model	Awareness
SUNY ISI	Building protections
SSE-CMM	Plan and track
CERT/CSO	Repeatable
CSMM	Process growth

Table 4: Security Maturity Models – Level 3

Security Maturity Model	Industry model Level 3 description
ISM3	Managed
IBM-ISF	Capable
NIST CSEAT IT SMM	Execution
Gartner's Security Model	Corrective
SUNY ISI	Security programme
SSE-CMM	Well defined
CERT/CSO	Designated person

Security Maturity Model	Industry model Level 3 description
CSMM	Information enabled

Table 5: Security Maturity Models – Level 4

Security Maturity Model	Industry model Level 4 description
ISM3	Controlled
IBM-ISF	Efficient
NIST CSEAT IT SMM	Testing
Gartner's Security Model	Operational Excellence
SUNY ISI	Maintaining security
SSE-CMM	Control
CERT/CSO	Documented
CSMM	Tactics growth

Table 6: Security Maturity Models – Level 5

Security Maturity Model	Industry model Level 5 description
ISM3	Optimised
IBM-ISF	Optimising
NIST CSEAT IT SMM	Integration
Gartner's Security Model	
SUNY ISI	
SSE-CMM	Continuous improvement
CERT/CSO	Reviewed and updated
CSMM	Operational security

Although the respective industry Security Maturity Model levels do not correspond exactly, many of these levels overlap in either the level description or the level content. The next section analyses this level content.

4.3 Analysing industry Security Maturity Models

By investigating each of these eight Security Maturity Models, it is possible to develop a comprehensive idea of Security Maturity Model principles. The next sections show the content of the industry models mapped to the generic Security Maturity Model, shown in Figure 1.

This discussion sets out to find a cross-section of the average Security Maturity Model, and accordingly not all statements will be wholly applicable to all discussed models. Additionally, due to the comprehensive coverage of a complete comparison and analysis of eight individual industry models, not all aspects of the comparison are mentioned below. Only those aspects that are present in more than one industry model are presented as part of the mean depiction of a generic Security Maturity Model.

4.3.1 Level 1: Blind Trusting

The general idea of the first level is one of *ad hoc* actions and little organisation. Most organisations focus only on physical security at this stage. Additionally, security personnel have a lack of confidence regarding their duties and their abilities to conform to these. The SUNY ISI focuses on basic computer and network protection [17].

The Gartner Security Model estimates this level at about 25% maturity [17]. It is rare to find any formal Information Security programme or relevant documentation at this level. However, the NIST CSEAT IT SMM places policies on the initial level. It recommends the use of organisation wide documents that state dictatorially how employees need to ensure Information Security [18].

In CSMM Level 1, basic security measures include access controls and encryption. The NIST CSEAT IT SMM delineates the IT security management structure at this level [18]. According to a study done by Mutula [13] in 2002, Botswana, Malawi, Lesotho and Angola are all on Level 1 maturity.

4.3.2 Level 2: Repeatable

The Gartner Security Model estimates an organisation at Level 2 at 75% total maturity. During this stage, organisations critically review their status. If there is no appointed security team, the organisation appoints one. As a result, organisations develop a formal policy set to address vital areas [17].

ISM3 Level 2 ensures that organisations document and use Information Security processes [16]. NIST CSEAT IT SMM also adds the use of procedures in Level 2. These procedures provide the security controls identified by the defined policies. It clearly defines IT security responsibilities and expected behaviours [18]. Similarly, SSE-CMM reaches a commitment to perform. This decision leads to planning and executing of performance [12]. However, SUNY ISI does not introduce any formal Information Security programme. At this stage, security personnel have gained some level of confidence, but there is no documentation to provide any guidance [17].

IBM-ISF Level 2 introduces a basic commitment to develop the capability with informal standards and processes. This SMM confines capability to specific parts of the business. No organisational strategy or awareness exists. The security section defines some basic roles and responsibilities [12]. CSMM recommends security controls such as secure websites, firewalls and backups [18]. Mutula's study indicates that Namibia,

Mozambique, Tanzania, Zimbabwe and Zambia are all still on Level 2 [13].

4.3.3 *Level 3: Defined*

The Gartner Security Model estimates this level at 95% total maturity. This stage starts with the initiation of the strategic security programme. The design architecture follows this step [17].

For the third level, SUNY ISI focuses on building and initiating an Information Security programme. It is possible to see some results from the previous stages' effort [17]. NIST CSEAT IT SMM promotes implementation of IT security procedures and controls in a consistent manner [18]. SSE-CMM introduces a standard process to ensure Information Security. This process includes real data from the organisation [12].

IBM-ISF Level 3 endorses common principles, policies and processes throughout the organisation. The entire organisation adopts standards and uniform products [12]. ISM3 Level 3 defines all Information Security processes. Organisations use the results of the processes to improve the individual processes [16]. CSMM introduces security controls such as intrusion detection and prevention mechanisms [18]. Mutula's study [13] indicates that Mauritius and South Africa are currently on Level 3 maturity.

4.3.4 *Level 4: Managed*

The Gartner Security Model estimates this level at 100% maturity. At this point, it is necessary to point out that the Gartner Security Model only has four levels. However, the percentage distribution on each level gives a clear indication of the intensity of each of the respective levels. Organisations continuously track technology and business change. This is also the beginning of continuous process improvement [17].

NIST CSEAT IT SMM endorses testing. This level sees that employees take corrective action to address identified weaknesses. Additionally risks are also mitigated [18]. SUNY ISI perfects the implementation of the Information Security programme. At this stage, information management becomes self-sustaining [17]. SSE-CMM establishes measurable quality goals. This level also sees a plan to achieve goals [12].

In CSMM Level 4, security threats are structured. Security controls support 24/7 staffed operations [18]. ISM3 sets specific milestones and can accurately predict the need for resources at this stage [16].

4.3.5 *Level 5: Maintenance*

NIST CSEAT IT SMM promotes integration on Level 5. This level ensures that all policies and procedures implement the appropriate IT security level [18]. ISM3 sees Level 5 as a controlled environment. The Information Security improvement leads to significant savings in resources [16].

SSE-CMM Level 5 establishes a quantitative process for effectiveness [12]. For IBM-ISF, it is possible to observe the results from the previous levels. Processes and procedures are highly optimised to produce consistent and expected outcomes [12]. In CSMM Level 5, security threats are highly structured. All security controls are fully automated [18]. At this stage, organisations should be able to handle all Information Security incidents. At the highest level, organisations move from the traditional reactive approach to a more proactive approach to Information Security.

4.3.6 *Industry SMM comparison result*

Although most SMMs correspond in level characteristics, there is the occasional characteristic present in more than one level. For example, the use of organisational policies is present at both Level 1 and Level 2. Table 7 shows basic results from the model comparison.

Table 7: Generic Security Maturity Model level mapping

Generic Security Maturity Model	
Level 1	Physical security Lack of confidence Basic computer and network protection
Level 2	Critical review of organisation Appoint security team Some level of confidence Formal security policies/procedure
Level 3	Initiation of security programme Security architecture Stricter security controls Organisation-wide policies/procedures
Level 4	Security testing Mitigate security weaknesses Information management Identity security threats
Level 5	Full implementation of policies/procedures Consistent outcomes Automated security controls

When the analysis of the respective industry models is considered, it is possible to subtract some overlapping characteristics from the models to create a separate generic security model (presented in Table 7).

This generic model resolves that Level 1, *Blind Trusting*, focuses more on physical and environmental security.

Level 2, *Repeatable*, focuses mainly on front-end system security. Level 3, *Defined*, focuses on back-end system security. Level 4, *Managed*, focuses on all-inclusive security awareness and Level 5, *Maintenance*, focuses on definite proactive security.

5. Best practices comply with Information Security Maturity

Section 2.2 introduced the best practice driven Information Security Maturity Model, whilst Section 4.3.6 presents the generic Security Maturity Model. This section focuses on drawing a parallel between these models to show that the best practice driven model conforms to the generic Security Maturity Model.

Many of the Security Maturity Models build on best practices and certification standards. Accordingly, there exists a large overlap between the best practice driven model and any Security Maturity Model. For example, ISM3 builds on standards such as ISO 20000, ISO 9001, the Capability Maturity Model, ISO/IEC 27001 and general information governance and security concepts.

The NIST CSEAT IT SMM considers the Federal Information Processing Standards and Special Publication documentation. These Security Maturity Models provide implementing organisations with standardised and approved configuration checklists [18]. This ensures adequate Information Security Governance. Section 2.2 introduced the best practice documents incorporated into the best practice driven model.

To illustrate the compliance of the best practice driven Information Security Governance model to Information Security Maturity, it is necessary to map the model against the generic Security Maturity Model. Due to the elaborate nature of the mapping process, Table 8 shows only the results of the mapping.

Table 8: Mapping the best practice driven model onto the generic SMM level mapping

Generic Security Maturity Model	
Level 1	Asset management Security management Physical and environmental security Performance measurement Security management
Level 2	Control needs and objectives Critical business applications Business continuity management Organisation/management of Information Security Performance measurement Security management Personnel security management Information system development Legal requirements
Level 3	Security managements Information system development Security management Compliance management
Level 4	Security management Risk management Compliance management
Level 5	Business continuity Compliance management Critical business applications Performance measurement Security management Corporate and criminal accountability

In Table 8, most of the Information Security Governance drivers listed in Section 2.2 maps either fully or partially onto the level entries shown in Table 7. Due to the comprehensive nature of the best practice driven Information Security Governance model, a number of the drivers appear several times in the mapping. This indicates that some drivers are applicable on more than one level of the generic Security Maturity Model, similar to some characteristics of various industry Security Maturity Models are applicable on more than one level (refer to Section 4.3.6).

The drivers listed overlap largely with the generic Security Maturity Model level entries, and extend to include additional aspects relevant specifically to Information Security Governance. Drivers that are covered by the best practice driven model, but not mapped directly onto the Security Maturity Model, include:

- disclosure mechanisms;
- shareholder treatment;
- digital forensics;
- ethical aspects; and
- certification.

This article shows that the best practice driven Information Security Governance model shows many of the Security Maturity Model characteristics. The best practice driven model therefore complies with Information Security Maturity according to Security Maturity Model standards. The Information Security

Governance model therefore presents a more all-inclusive model to ensure security maturity.

6. Conclusion

Without Information Security Governance, an organisation has no guarantee of any long-term success. However, when an organisation properly implements Information Security, many advantages may flow from the implementation. Organisations need to protect themselves against the inherent risks associated with the use of information systems, balancing these risks with the associated benefits. Accordingly, this interdependence necessitates the use of effective Information Security Governance [2].

On the other hand, organisational maturity leads to a better understanding of an organisation's security programme. To exploit an organisation's competitive advantage further, it is necessary to compare its position in industry with competitors and best practice standards. Additionally, it guides organisations to implement security measures in the correct order to ensure maximum Information Security [9].

This research focused on the comparison of a best practice driven Information Security Governance model with the traditional Security Maturity Models. Both models pursue appropriate security measures in organisations. The mapping presented in Section 5 shows that the best practice driven model adheres to all the requirements necessary to classify as a Security Maturity Model, and presents a number of additional aspects not covered within industry Security Maturity Models. As a result, organisations can implement the best practice model as a sole tool to ensure Information Security Maturity.

7. References

[1] Von Solms, SH. & Von Solms, R. 2006. Information Security Governance: Due Care. *Computers & Security.* Volume 25, Issue 7. Pp. 494 - 497.

[2] Anderson, PW. 2001. Information Security Governance. *Information Security Technical Report.* Volume 6, Number 3. Pp. 60 - 70.

[3] EBS. 2008. *Glossary.* Available from: http://newweb.ebs.bg/page.php?tab_id=72&item_id=112&class=portfolio (Accessed 15 July 2008).

[4] Moulton, R. & Coles, RS. 2003. Applying information security governance. *Computers & Security.* Volume 22, Issue 7. Pp. 580 - 584.

[5] Etsebeth, V. 2005. Information Security. In: *ICT Honours Information and Communication Technology (ICT) Law,* edited by MM. Watney. Johannesburg: University of Johannesburg. Pp. 91 - 103.

[6] Hunter, B. (2000). *Information Security: Raising Awareness, Version 1.0*. Submitted to: The Public Sector Chief Information Officers' Council by the Subcommittee on Information Protection. Available from: www.iwar.org.uk/comsec/resources/canada-ia/ infosecawareness.htm#7 (Accessed on 27 March 2006).

[7] Oud, EJ. 2005. The Value to IT of Using International Standards. *Information Systems Audit and Control Association*. Information Systems Control Journal. Volume 3. Pp. 1 – 5.

[8] Lessing, MM. 2006. *A Model for Best Practice Driven Information Security Governance*. Unpublished dissertation. Johannesburg: University of Johannesburg.

[9] Chapin, DA & Akridge, S. 2005. How Can Security Be Measured? *Information Systems Control Journal*, Volume 2.

[10] Allard, JL. 2001. System Security Engineering - Capability Maturity Model. Information Systems Audit and Control Association. ISACA Round Table.

[11] Fraunhofer. 2002. *Security Maturity Model (SMM).* Institut Software- und Systemtechnik. Germany.

[12] IBM. 2007. *Information Security Maturity Models - How can we grow from ISO17799/27001 certification?* Available from: www.oceaniacacs.org/presentations/S10%20-%20Alan%20 Heward%20-%20%22How%20old%20are %20you:%20Security% 20maturity %20 models%22.ppt (Accessed 6 March 2008).

[13] Mutula, SM. 2007. E-governance – Citizens' gap in Southern Africa. In: *Proceedings of the 9th annual conference on world wide web applications.* Editor: PA van Brakel. Available from: staging.uj.ac.za/www2007/documents/proceedings/Mutula_E-governance.pdf (Accessed 10 April 2008).

[14] Chege, S. N.D. *Security Maturity Models.* Lafarge Cement.

[15] McGraw, G. 2002. On Bricks and Walls: Why Building Secure Software is Hard. *Computers & Security.* Volume 21, Issue 3. Pp. 229 - 238.

[16] ISM3 Consortium. 2007. ISM3 - Information Security Management Maturity Model. ISM3 Consortium: Spain.

[17] Phelps, T. 2005. *SUNY Information Security Initiative - A Model to Map Our Information Security.* Available from: www2.itec.suny.edu/wizard/2005/fall/SUNY_Information_Security_Model/Maturity_Model.ppt (Accessed 6 March 2008).

[18] Dykas, W. 2007. *Cyber Security… A Circular Maturity Model*. 3rd Annual Cyber Security Summit 2007. Knoxville.

8. Author Contact Details

Marthie Lessing

Marthie Lessing is a Cyber Security Specialist at the Council for Scientific and Industrial Research. She currently works as researcher in the Defence, Peace, Safety and Security division. Marthie obtained an M.Sc Computer Science in Information Security Governance *cum laude* from the University of Johannesburg in 2006.

At present, she is busy with a PhD in Computer Science at the University of Johannesburg. This study focuses on Cyber Forensics, and the possibility of doing live forensic acquisition on electronic systems, and producing forensically sound evidence that is admissible in a court of law. Marthie is specifically interested in Information Security Governance and Cyber Forensics.

Contact:

mlessing@csir.co.za

marthie.lessing@gmail.com

■