COMPLYING WITH INFORMATION SECURITY MATURITY

Marthie Lessing (mlessing@csir.co.za) – CSIR

Hypothesis: Organisations complying with Information Security Governance guidelines present a high level of maturity

Best practice driven Information Security Governance (BPD ISG) model → maps onto → Security Maturity Model (SMM) → ensures → Information Security Maturity compliance

Step 1: Develop BPD ISG model

A combination of industry best practices relevant to Information Security and Information Security Governance. The implementation of the BPD ISG model should lead to proper organisational Information Security.

Best practice driven Information Security Governance drivers mapped on generic SMM levels
Asset management Security management Physical and environmental security Performance measurement Personnel security management
Control needs and objectives Critical business applications Business continuity management Organisation and management of Information Security Legal requirements Information system development
Security management Information system development Compliance management
Security management Risk management Compliance management
Business continuity management Compliance management Performance measurement Corporate and criminal accountability

Duplicate drivers emphasise model's thoroughness

Step 3: Map BPD ISG model onto generic SMM

Additional guidelines, supplementing the SMM:
- Disclosure mechanisms and shareholder treatment
- Digital Forensics
- Ethical aspects and certification

Security Maturity Model
Gartner's Security Model
NIST CSEAT IT SMM
IBM-ISF
ISM3
SUNY ISI
SSE-CMM
CERT/CSO
CSMM

A structured collection of elements that describe certain aspects of maturity in an organisation, creating a distinct security framework

Step 2: Analyse industry models and extract common characteristics

Develop generic SMM to present standard application

Generic SMM		
Level 1	**Blind trusting**	Physical and environmental security
Level 2	**Repeatable**	Front-end system security
Level 3	**Defined**	Back-end system security
Level 4	**Managed**	All-inclusive security awareness
Level 5	**Maintenance**	Definite security

Industry SMM + additional guidelines

= comprehensive BPD ISG model

≈ Information Security Maturity

MORE ALL-INCLUSIVE MODEL TO ENSURE INFORMATION SECURITY MATURITY

CONCLUSION:

SMM is a detailed compliance tool

Step 4: Implement BPD ISG model to comply with Information Security Maturity

The best practice driven Information Security Governance model conforms to all the requirements of a generic SMM.

The proper implementation of the BPD ISG model can lead to a high Information Security maturity level.

Benefits of implementing BPD ISG model :
- generate reproducible measurements
- determine actual progress in security
- benchmark against other organisations
- determine order in which to apply security controls
- determine resources needed to comply with security

AlAboodi, SS. 2006. *A New Approach for Assessing the Maturity of Information Security.* ISACA. Journal Online.

Allard, JL. 2001. *System Security Engineering - Capability Maturity Model.* ISACA Round Table.

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

Lessing, MM. 2006. *A Model for Best Practice Driven Information Security Governance.* M.Sc Computer Science dissertation. Johannesburg: University of Johannesburg.

Wikipedia, the free encyclopaedia. (2006). Information Security. Available from: http://en.wikipedia.org/wiki/Information_assurance (Accessed on 13 February 2006).

Wikipedia. 2008a. *Capability Maturity Model.* [Available from: http://en.wikipedia.org/wiki/Capability_Maturity_Model (Accessed 3 March 2008)].