1-1-2012

Developing Governance Capability to Improve Information Security Resilience in Healthcare

Rachel Mahncke

Patricia Williams
Edith Cowan University

Originally published in the Proceedings of the 1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

DEVELOPING GOVERNANCE CAPABILITY TO IMPROVE INFORMATION SECURITY RESILIENCE IN HEALTHCARE

Rachel J. Mahncke[1], Patricia A H Williams[2]
[1]School of Computer and Security Science, Edith Cowan University
[2]eHealth Research Group, School of Computer and Security Science and Security Research Institute,
Edith Cowan University
[1]rmahncke@our.ecu.edu.au, [2]trish.williams@ecu.edu.au

Abstract

General medical practices' in Australia are vulnerable to information security threats and insecure practices. It is becoming well accepted in the healthcare environment that information security is both a technical and a human endeavour, and that the human behaviours, particularly around integration with healthcare workflow, are key barriers to good information security practice. This paper develops a holistic capability approach to information security by completing a preliminary iteration of mapping operational capabilities to governance capabilities. Using an operational backup capability matrix exemplar, the approach is analysed against the governance policy capability matrix. The resultant mapping between the operational and governance capability frameworks demonstrates that resilience can be promoted through sound governance. This implies that improved security performance and compliance contributes to measurement and oversight of the governance processes thereby making the organisations demonstrably more resilient to security threats. This paper proposes the need for a holistic capability approach to information security.

Keywords
Information security, operational capability, governance capability, performance improvement.

INTRODUCTION

General medical practices, as the primary point of care, need to ensure that the healthcare information they collect, is secure. It is becoming well accepted in the healthcare environment that information security is both a technical and a human endeavour, and that the human behaviours, particularly around integration with healthcare workflow, are key barriers to good information security practice (Mahncke & Williams, 2011). The Ponemon Institute survey (2011) found that healthcare is one of the most breached industries. Healthcare information is becoming more lucrative to thieves as it could contain sensitive information, financial data and other identifying data that could be used for identity theft or on sold (Allen, 2012; Privacy Rights Clearinghouse, 2011). Securing healthcare information is becoming significantly important in the developing electronic healthcare environment.

General practices are becoming more cognizant of their responsibilities in the information security area, as is evident by bodies such as the Royal Australian College of General Practitioners (RACGP) who, in 2011 published the Computer and Information Security Standards for General Practices'. Further, technical best practice standards and guidelines needed to secure information, are well documented by international standards, professional bodies, and best practice guidance from national and government agencies (International Standards Organisation (ISO); General Practice Computing Group (GPCG); Department of Health and Ageing; National E-Health Transition Authority (NEHTA); ISACA's CobiT 5 (2012); The IT Governance Institute (ITGI); National Institute of Science and Technology (NIST); Committee of Sponsoring organisations of the Treadway Commission (COSO); and Hertzog's OSSTMM 3). The operational aspects of a security capability approach are supported in various ways including frameworks such as that developed in 2007 by Williams. Williams' (2007) information security operational capabilities for general practices addresses the implementation and measurement of security practices and provides a framework for incremental improvement in day to day security practices.

Once operational policies and procedures have been implemented within practices, then the future management, or governance, of the information systems can be addressed. The governance component is arguably the most important, yet difficult to straightforwardly define and implement. Many organisations and indeed, even security professionals do not fully comprehend the relationship between governance and security programs (Harris, 2006). Whilst a security program must address the threat profile, it must also address the legal and jurisdictional requirements in relation to the organisational objectives and drivers. However, there are different interpretations of security measures needed in light of the roles and relationships that staff have to others in the healthcare environment, both colleagues and patients. There is no single security solution; instead, a multi-layered best

practice security strategy is required which includes operational, technical and governance guidelines and controls. Each of these components is integral to a holistic approach to effective information security protections, and must also address the ethical concerns present in the healthcare environment.

This paper proposes the mapping of operational capability to governance capability and the creation of the Mahncke-Williams Capability Framework. The performance measurement for this model is presented together with a worked example to verify the model.

Operational capabilities

Operational capability is defined as "the quality of possessing attributes, physical or mental, required for performance or accomplishment, and the competency is possession of the suitable or sufficient knowledge, experience or skill" (Williams 2008). An operational framework presents activities in simple non-technical terms, which is imperative as security becomes a necessary aspect of day-to-day pervasive computing, utilised by non-IT users. From the healthcare information security systems perspective this has been defined as covering ten key process areas of security: access, vulnerability management, perimeter controls, content filtering, encryption, backup, malware, physical, security management and reporting, and wireless and mobile.

Figure 1 shows the flow of influence from the bottom level of operational dependencies to the top level of governance an understanding of how the operational dependencies co-exist and influence the governance level and its activities is required.

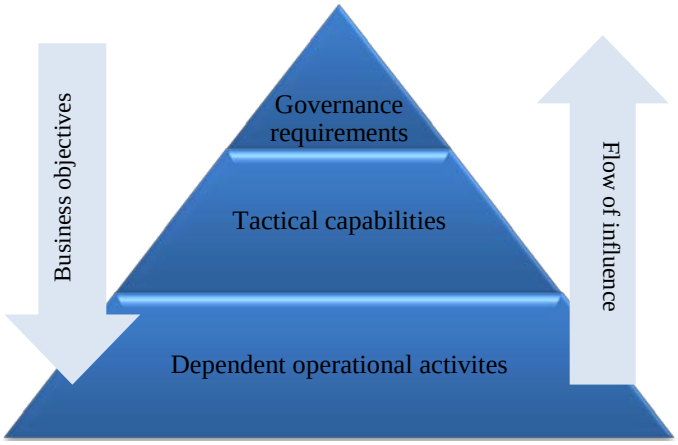

Figure 1: Flow of operationally dependent activities as a contribution to governance

At the base level, the capabilities of the staff to undertake and integrate security controls in healthcare, particularly primary care, have been shown to be poor (Williams, 2011). In the healthcare environment an elemental problem is the capabilities of those who need to implement security in their day to day activities. This in essence includes all people using information systems and anyone handling or responsible for healthcare information. It should be remembered that information security is not a core activity for healthcare and it is unreasonable to assume that staff are able to apply security measures consistently without effective integration into workflow (Snidaro & Foresti, 2007). Operational capability involves both education and awareness and context aware security controls. Practical security controls defined as clear and simply distinct tasks can provide a firm and measurable foundation upon which to base effective security. In addition, they provide a supporting path to measure the governance process.

Based originally on the Capability Maturity Model representations, Williams (2008) Operational Capabilities Framework comprises four elements:

1. Maturity levels. These provide a structured template for persistent improvement.
2. Key process areas and their associated goals. A key process area is a set of related activities that can achieve the stated goal of a key process area. The goals are important in that they provide a measure of the capability of the practice and maturity level reached.
3. Common operational features. These are characteristics which define the key process area contributing to the overall goals. They are used as a metric upon which comparison to maturity levels is made. The features are policy, standards, process, procedures, training and tools. Table 1 explains the relationship between these common operational features.
4. Key practices. A key process area is defined by the procedures, activities and communications implemented as follows:

Policy	Laws and regulations that govern and constrain operations
Standards	Accepted criteria for operation

Constrain	
Process	Activities used to conform to standards in accordance with policy
Implemented by	
Procedures	Instructions on how to implement an activity or process
Supported by	
Training	Identification of knowledge or training needed to use a procedure
Tools	Identification of automated support to implement a procedure

Table 1: Operational Common Features (adapted from University of Massachusetts Dartmouth, n.d.)

The construction of the relevant information security operational capabilities have been applied (RACGP, 2011) and have been published by Williams. The important contributions that operational capabilities provide are to underpin the governance requirements.

Governance capabilities

It is this governance component of information security that is currently problematic and mainly unaddressed within General Practice at the organisational and the wider national and state-wide levels. Information security governance is defined as:

> *"the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk"(NIST 800-100).*

The International Standards organisation's (ISO), ISO/IEC DIS 27014 Information technology – Security techniques - Governance of information security (DIS) standard, is yet to be released.

Developing information security governance processes requires planning and knowledge. The information security governance capabilities extend the research and publications conducted by the RACPG. Further, interpreting and applying ISACA's CobiT 5 (2012); International Standards Organisation's ISO/IEC 27001, 27002 (2005), ISO **27799-2008 and** ISO/IEC DIS 27014 (Draft); The IT Governance Institute (ITGI); National Institute of Science and Technology (NIST) Security Metrics Guide for Information Technology Systems - Special Publication 800-55 (2008); Hertzog's OSSTMM 3 (2010); Committee of Sponsoring organisations of the Treadway Commission (COSO) (2005); IsecT (2012); ISM3 (2007); Department of Health's Clinical Governance Standards for Western Australian Health Services (2005); U.S. Department of Health & Human Services - OCR HIPAA (2012); and William's TIGS-CMM (2007a). The resultant information security governance capability matrix comprises of thirty three governance control activities. An example of a governance control activity for Policy Coverage is provided in Table 2.

1.3 Policies				
1.3.1 Policy coverage				
Initial	Managed	Defined	Quantitatively Managed	Optimising
Information security policies are verbal, undefined and/or ad hoc.	Internal best practice policies are documented and are repeatable for all key operational activities in accordance with the RACGP computer security guidelines 3rd edition.	Policies and procedures are defined and conform to relevant legislation, RACGP regulations and accreditation requirements. Policies have been approved and are signed off on by management.	Number of implemented policies measured as a percentage of required policies in accordance with the RACGP Standards.	External best practice policies are applied (ISO/IEC 27002/ISO/IEC 27799) that extend those required within the sector.

Table 2: Example of a governance control activity

The governance control activities are logically divided into three main areas, that of Accountability, Governance Planning and Resource Management. A section of the Governance Capabilities matrix, Strategic Alignment, was published by Mahncke and Williams in 2011. Preliminary verification of the governance capabilities has

been conducted during two focus group interviews, comprising of both security experts and medical practitioners.

MAHNCKE-WILLIAMS CAPABILITY FRAMEWORK

The Mahncke-Williams Capability Framework (Capability Framework) has been developed as an information security process improvement instrument for use within general medical practice and associates the ten operational capability matrices and the governance capability matrix. The resultant Capability Framework is graphically demonstrated in Figure 2. Each of the ten operational capabilities matrices from the operational capabilities (Williams, 2008), are accessed against the governance capability matrix. A general practice implements the Capabilities Framework by firstly completing, or mapping their performance, against the ten operational matrices.

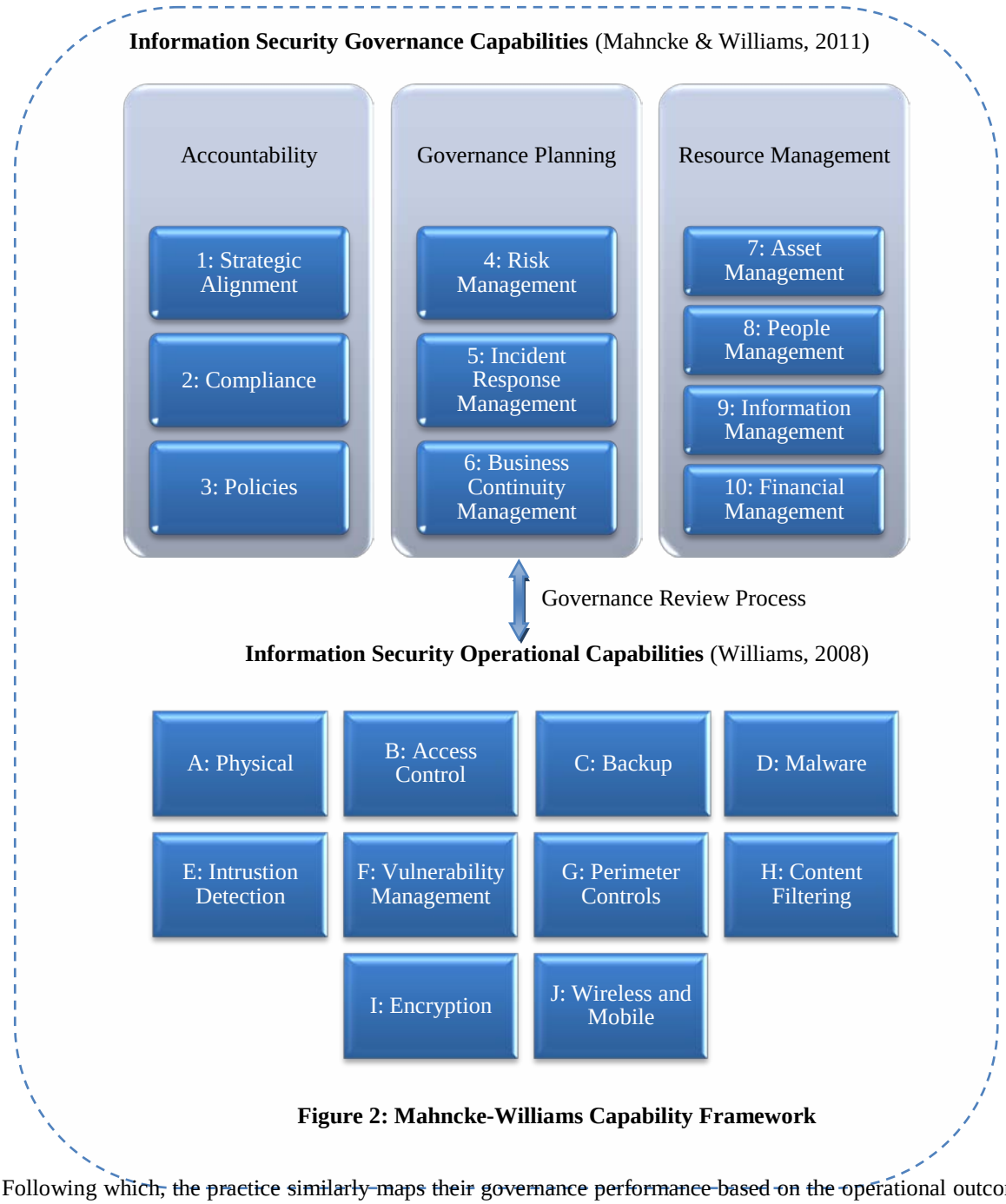

Figure 2: Mahncke-Williams Capability Framework

Following which, the practice similarly maps their governance performance based on the operational outcomes. Mapping the general practices operational and governance security performance establishes a security performance measure, or baseline, against which the practice can aim for incremental and sustainable improvement.

Measuring capability

The Capability Framework presented utilises the Software Engineering Institute's (2012) Capability Maturity Model® (CMM) and Capability Maturity Model® Integration (CMMI) approaches to measure information security performance improvement within general medical practice. This approach aims for systematic improvement in capabilities to demonstrate attainment of higher levels of capability maturity (Software Engineering Institute, 2009; Williams, 2007b). Maturity models provide an organisation with the ability to baseline their current capability, outline proposed strategies and to measure security progress over time (Poole, 2006). This maturity model approach is increasingly becoming evident in IT governance with reporting based on the COBIT *Security Baseline* guidance which allows organisations to establish the minimum security requirements in line with the IOS/IEC 27002 standards (Poole, 2006).

There are five capability maturity model CMM and CMMI levels as defined by the Software Engineering Institute (2009), ISM3 (2007) and Williams (2008) as demonstrated in Table 2. For each control activity, or 'row' in the operational and governance capability frameworks, the practice selects the appropriate minimum level applicable to the practices' performance from the range 1-5 (Initial to Optimised). The practice cannot move to a higher maturity level without having fulfilled all the conditions of the lower levels (CobiT 4.1, 2004). By selecting a level for each control activity in the Capabilities Framework, a performance measure of that activity is established.

Maturity Level Focus:				
Operational Capability Maturity Model (CMM) Levels				
1 Initial Best practices are followed and automated	2 Repeatable Processes are monitored and measured	3 Defined Processes are documented and communicated	4 Managed Processes follow a regular pattern	5 Optimizing Processes are ad hoc and disorganised
Governance Capability Maturity (CMMI) Levels				
Level 1 Initial Processes unpredictable, poorly controlled and reactive	Level 2 Managed Processes are monitored and controlled in accordance with policy	Level 3 Defined Defined processes characterised by continuity, incident resolution and prevention. Processes are proactive	Level 4 Quantitatively Managed Processes are measured and controlled for quality and performance	Level 5 Optimising Processes are continually improved based on a quantitative understanding of the practice's objectives

Table 2: Description of capability maturity levels applicable to operational and governance capability

At the first iteration, a performance level is assigned for each activity within the Capability Framework, thus an information security governance baseline is established. The practice should aim for incremental performance improvement from the established baseline to a higher level until the Level 3 – Defined measure, or above, has been achieved for each information security control activity in the Capability Framework.

The measurement outcome, i.e. the levels attained, is a governance capability summary which identifies governance competence (Beveridge, 2008). Further, a maturity model can be "used as a benchmark for comparison and as an aid to understanding" (Software Engineering Institute, 2009). For example, a comparative assessment can be undertaken of different practices where the information security governance capabilities are the common basis for comparison. This could assist in defining an industry standard.

Verification of the Capability Framework

A verification exemplar is the mapping of the operational backup capability matrix (Williams, 2008) to the governance capability matrix. The governance capability matrix is used to review backup by assessing the backup matrix against it. The six operational common features of the backup matrix are mapped to the governance capabilities as follows: The four operational common features that of Policy, standards, processes and procedures can be mapped to Accountability in the governance capability matrix; Training maps to People Management within Resource Management, and tools maps to Asset and/or Information Management. The performance measure levels of the six common operational features are passed up into the governance capabilities for review.

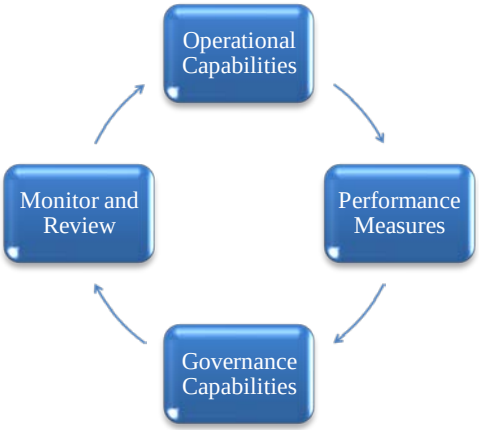

Figure 3: Governance review process

Questions are asked such as, are there any new developments that would necessitate the backup matrix to be updated, such as backing up to the cloud. If so, best practice processes and procedures are added to the backup policy and the backup matrix is updated accordingly. Next, the effectiveness of the backup policy is assessed. There are fourteen control activities in the backup matrix; each of which has been assigned a baseline CMM performance level. Each activity is assessed, and those with the lowest performance level are identified as in need of improvement. The practice then assign a performance level to the corresponding governance control activity.

Governance planning will further assess backup Risk Management, Incident Response Management and Business Continuity Management. Similarly, each of the governance activities map back to monitor and review the operational capabilities. If updates or changes are necessary within the backup matrix, then these are actioned accordingly. In a similarly manner, each of the remaining operational capability matrices are assessed at the governance level. In this manner, all operational and governance activities are assessed. It is anticipated that general practices' would need to organise three governance review meetings per annum, comprising of a minimum of three members of staff, including one member of staff from ICT.

DISCUSSION

Theoretically, at a governance review meeting the operational capability performance will be assessed by mapping them to the governance capabilities to determine if activity controls are below the required Level 3 performance. The governance meeting will need to assess all aspects of backup against the governance areas of Accountability, Governance Planning and Resource Management. For example, Business Continuity in regards to backup must be assessed. The governance control activity for Business Continuity as relates to backup is assessed. CMM performance level/s are assigned as appropriate. In this way the governance meeting decides if the practice backup governance performance needs improvement. If so, control activities from the governance activities are allocated to appropriate staff to action by the next meeting.

Subsequently, if a security breach occurs, for example it is discovered that the backup has not been encrypted prior to being taken off site for storage, then this incident is discussed at the governance meeting and the reasons for the breach ascertained, such as were staff too busy or is there a need for additional training on encryption processes. The governance meeting would refer to the governance capability criteria and review what actions are needed. Do procedures need to be changed? Could a better process be implemented, have the best practice activities been altered? If changes are required, then these changes are made to both the operational capabilities and governance capabilities as required. The meeting continues to review any other incidents.

If the governance meeting find it justified to adjust activities up a level, then this performance improvement measure is discussed and processes put in place to drive this. In this way continuous security feedback is achieved. The practice maps its performance against the original baseline to determine performance improvements. Has the practice improved since the last governance meeting? If not, the meeting focused on the lowest performing control activities and allocated the activity/activities to an appropriate staff member for actioning and review at the next governance meeting.

The purpose of focusing on the future management of security is to enter into a discussion of where the practice is at in terms of its aspirations to improve its information security practices. It may be that the practice desires to reach a high level of security in a certain timescale, and so a regular item at a governance meeting would be to track progress against that goal.

The resultant mapping between the operational and governance capability frameworks demonstrates that resilience can be promoted through sound governance. This implies that improved security performance and compliance contributes to measurement and oversight of the governance processes thereby making the organisations demonstrably more resilient to security threats. This paper proposes the need for a holistic capability approach to information security.

CONCLUSION

The use of the Capability Framework, which incorporates both the operational capabilities and governance capabilities, enables general practice to review their information security practices and establish policies and procedures to help meet their legal obligations, and if necessary, move the practice to a higher level of compliance. Due to the flexibility of the two frameworks (operational and governance), they can be customised to reflect the practices' specific situation, objectives and priorities.

The aim of the capabilities is to promote performance improvement in information security practice within general medical practice. This practical information security Capability Framework aims to assists practices' in establishing an information security governance baseline from which improvement in information security performance can be measured. The element of continuous improvement in governance, driven and supported by improvement in operational capability, is important as the capabilities should take into account breaches, weaknesses or failures which then become opportunities for improvement in the future.

It is the task of the governance review meeting to re-affirm or otherwise, the practices security governance performance and if necessary explore any implications for accountability, resource management and governance planning. Empowering staff with the supporting mechanisms to perform information security responsibilities, forms the basis of information security governance capability. Further, the Capability Framework could be implemented more broadly within the healthcare community, where the extrapolated methodology may similarly apply.

REFERENCES

Allen, C. (2012). *In Healthcare industry CIOs, CSOs must improve security*. Retrieved 8 March 2012, from http://ithealthcare.computerworld.com/health-care/42988/healthcare-industry-cios-csos-must-improve-security.

Carnegie Mellon University. (2003). *Systems Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document Version 3.0*. Retrieved 01 October 2005, from http://www.sse-cmm.org/docs/ssecmmv3final.pdf.

Department of Health. (1999). *Clinical governance baseline assessment tool*. Retrieved 16 February 2006 from http://www.health.gov.au/internet/main/publishing.nsf/Content/publications-C

Harris, S. (2006). *Information Security Governance Guide*. Retrieved 25 April 2012, from http://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide.

General Practice Computing Group (GPCG). (2004). *Security guidelines for general practitioners*. Retrieved 22 June 2009, from http://www.gpcg.org.au/index.php?option=com_content&task=view&id=128&Itemid=38

Hertzog, P. (2010). *Open Source Security Testing Methodology Manual (OSSTMM3*). Retrieved 20 April 2012, from http://www.isecom.org/research/osstmm.html

ISACA. (2004). *CobiT 4*. Retrieved 31 July 2012, from http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx

IASE. (2012). *Security Technical Implementation Guides*. Retrieved 25 April 2012, from http://iase.disa.mil/stigs/index.html

International Standards organisation. (2005). *ISO/IEC 27002-2005 International standard - Information technology - Security techniques - Code of practice for information security management*. Retrieved 15 May 2009, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 uis.georgetown.edu/departments/eets/dw/GLOSSARY0816.html

International Standards organisation. **(2008).** ***ISO 27799-2008*** *Health informatics — Information security management in health using ISO/IEC 27002.* Retrieved 15 June 2009, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41298

International Standards organisation. (2012). *ISO/IEC 27014 Information technology – Security techniques-Governance of information security (DIS).* Retrieved 31 July 2012, from http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43754

IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd Edition. Retrieved 10 Sept 2012, http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf

IT Governance Institute. (2007). *CobiT 4.1 Excerpt*. Retrieved 20 March 2009, from http://www.itgi.org/Template_ITGI.cfm?Section=Recent_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=45948

Mahncke, R. J., & Williams, P. A. H. (2011). *Australian primary care health check: Who is accountable for information security?* Proceedings of the 9th Australian Information Security Management Conference, (pp.48-54), SECAU Security Research Centre, Edith Cowan University, Perth, WA.

National Institute of Science and Technology (NIST). (2003). *Security Metrics Guide for Information Technology Systems*. Special Publication 800-55. Retrieved 10 April 2012, from http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Ponemon Institute. (2009). ***Electronic Health Information at Risk***. Retrieved 31 July 2012, from http://www.ponemon.org/data-security

Poole, V. (2006). *Why information security governance is critical to wider corporate governance demands – a European perspective*. Retrieved 22 February 2009, http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=30681&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Software Engineering Institute. (2009). *Capability Maturity Model for Software (CMM)*. Retrieved 12 March 2009, from http://www.sei.cmu.edu/cmm/

Snidaro, L. and Foresti, G.L. (2007). Knowledge representation for ambient security. *Expert Systems*, *24*(5), 321-333.

The Royal Australian College of General Practitioners (RACGP). (2010). *Computer Security Guidelines (3rd edition). A self assessment guide and checklist for general practice*. Retrieved 10 April 2012, from http://www.racgp.org.au/content/navigationmenu/clinicalresources/ehealth/computersecurityguidelines/computersecurityguidelines.pdf

University of Massachusetts Dartmouth. (n.d.). *SEI Capability Maturity Model*. Retrieved 01 January 2009, from www2.umassd.edu/swpi/processframework/cmm/cmm.html

Williams, P. A. H. (2007). *An investigation into information security in general medical practice*. PhD. Edith Cowan University, Faculty of Computing, Health and Science, School of Computer and Information Science. Perth, Western Australia.

Williams, P. A. H. (2008). The application of CMM to practical medical security capability. *Information Management & Computer Security, 16*(1),58 – 73. DOI: 10.1108/09685220810862751. Williams, P.A.H. (2011). Is the biggest threat to medical information security simply a lack of understanding? In D.P. Hansen, A.J. Maeder, & L.K. Schaper (eds.) *Health Informatics: The Transformative Power of Innovation*, pp. 179-187. IOS Press: Amste