1-1-2014

Developing And Validating A Healthcare Information Security Governance Framework

Rachel J. Mahncke
Edith Cowan University, r.mahncke@ecu.edu.au

Patricia A. Williams
Edith Cowan University, trish.williams@ecu.edu.au

electronic Journal of Health Informatics
www.eJHI.net
2014; Vol 8(2):e12

Developing and Validating a Healthcare Information Security Governance Framework

Rachel J Mahncke and Patricia A H Williams

eHealth Research Group, School of Computer and Security Science, Edith Cowan University, Perth, Western Australia

Abstract

General medical practices' in Australia are vulnerable to information security threats and insecure practices. It is 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. The Royal Australian College of General Practitioner's (RACGP) Computer and Information Security Standards (CISS) 2013 are the best practice standards for general practices, against which information security is assessed during practice accreditation. With the release of ISO/IEC 27014:2013 Information technology - Security techniques - Governance of information security in May 2013, it is this governance component of information security that is insufficiently addressed within General Practice at present. This paper documents the development and validation of an information security governance framework for use within general medical practice. The aim of the proposed Information Security Governance Framework is to extend current best practice information security management to include information security governance.

Keywords: Information Security Governance; General Practice; Action Research; Focus Group Interviews; ISO/IEC 27014:2013; RACGP CISS (2013)

1 Introduction

General medical practices, as the primary point of care, need to ensure that the healthcare information they collect, is secure. It is 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 [1]. The Ponemon Institute survey [2] found that healthcare is one of the most breached industries. Healthcare information is becoming lucrative for thieves as it may contain sensitive information, financial data and other identifying data that could be used for identity theft or on sold [3, 4]. Securing healthcare information is becoming vitally important in the developing electronic healthcare environment.

General practices are increasingly cognizant of their responsibilities in information security, evidenced by professional bodies such as the Royal Australian College of General Practitioners (RACGP) who publish the Computer and Information Security Standards (CISS) for General Practices [5]. Further, technical best practice standards and guidelines needed to secure information, have been well documented by international standards, professional bodies, and best practice guidance from national and government agencies, such as:

- International Organisation for Standardization (ISO) [6];
- General Practice Computing Group (GPCG) [7];
- Department of Health and Ageing [8];

- National E-Health Transition Authority (NEHTA) [9];
- ISACA's CobiT 5 (2012) [10];
- The IT Governance Institute (ITGI) [11];
- National Institute of Science and Technology (NIST) [12];
- Committee of Sponsoring organisations of the Treadway Commission (COSO) [13];
- Hertzog's OSSTMM 3 [14].

The operational aspects of security capability are supported in various ways by practitioners in the field including frameworks such as that developed by Williams [15] in 2007. Williams's information security operational capabilities for general practice, address the implementation and measurement of security practices and provide a framework for incremental improvement in day to day security practice.

Once operational policies and procedures are 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 define and implement. Many organisations do not fully comprehend the relationship between governance and security programs [16]. Whilst a security program must address the threat profile, it must also address the legal and jurisdictional requirements in relation to organisational objectives and drivers. However, different interpretations of security measures are needed in light of the roles and relationships of staff 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 needs to address the legal and ethical concerns present in the healthcare environment.

Research has been undertaken into information security governance and this paper reports on the first stage, which develops and validates a preliminary information security governance framework. The second phase of the research will apply and test the framework within general medical practices utilising iterative cycles of participant observations.

2 Methodology

The aim of the research is to develop an Information Security Governance Framework (ISGF), and to apply and test the resultant framework within the general practice environment. As such a flexible qualitative research approach was adopted. The method chosen was Action Research, as it would enable iterative changes to the framework to be made throughout the research process. All forms of qualitative research are known for their ability to learn about and understand the "perspectives of others rather than imposing the researcher's own views, biases, and theories in explaining differences across populations or communities in beliefs and behaviours" [17].

An action research approach was considered the most appropriate for this research as active participation would be required as part of the 'information system' (inclusive of people as a social constituent of the information system) under investigation. Studies suggest that the action research approach is suitable for information security and general practice research [18; 19]. In action research, the action researcher is concerned about creating change whilst simultaneously studying the process [20]. Through collaboration both the researcher and the subjects learn from the context being studied [20]. In its traditional form, action research involves cycles of "investigation, action planning, piloting of new practices, and evaluation of outcomes" [21; 22; 23]. At each stage of the collection and analysis of data, knowledge is generated [24; 22]. The outcomes of action research are both practical and theoretical [24; 23]. They are practical in the sense that the outcomes will inform security practice, and theoretical in that the knowledge generated will continue to have a lasting impact on changing practice through the publication of the research [24]. In practice, improvements in the action plan are incorporated into the next cycle by reflecting on participant feedback together with the experience of the previous cycle [19].

2.1 Research Design

The research comprises of two stages.

2.1.1 First Stage - Development and Validation of the Framework

Focus group interviews provide a means of validating the proposed governance framework. These interviews provide an opportunity to focus discussions and to examine, resolve, or come to a conclusion in relation to a particular problem under investigation [26]. The focus

group method is a valid and tested qualitative research method.

During the focus group interviews, participants were asked to evaluate a preliminary goverance framework, and asked the same set of ten semi-structured questions. Six participants, plus the researcher, were considered to be an ideal number of participants for each focus group interview. Following ethics approval and participant consent, focus group interviews were recorded with two electronic devices, an iPhone and Audacity software recorded on a laptop. The focus groups were each one hour in length.

2.1.2 Second Stage – Iterative Cycles of Participant Observations

Whilst the first stage of the research is reported on in this paper, a brief outline of the subsequent participant observation method that will be used in stage two is provided for clarification. The purpose of the second research cycle is to apply the framework within Australian general practice. During the participant observations, general practices will be asked to: map the governance framework to their actual practice, participate in a semi-structured interview and provide copies of their de-identified information security polices for triangulation analysis. The triangulation method will be further applied utilising the framework outcomes, interview answers and documented policies.

Participant observations provide an appropriate environment in which to apply the proposed framework. It is a method of data collection in which the researcher takes part in the activities related to the area studied through the observation of events in their "natural contexts" [27]. Each second stage cycle will require at least four general practices to participate in participant observations. The second stage of this research will involve as many iterations of the Action Research cycles as required until saturation of consistency in applying the framework within general practices is achieved.

Utilising multiple methods and multiple participants within the research, increases the rigour of the collected data by allowing the findings to be crosschecked and triangulated [25]. This paper reports on the first three focus group interviews.

3 Results

This section addresses the outcomes of the First Stage and first cycle of the research. Included in this stage are the development of the preliminary framework and three focus group interviews.

3.1 Development of the preliminary information security governance framework

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"*[28]. It is this governance component of information security that is arguably insufficiently addressed within General Practice at the organisational and the broader national and state-wide levels.

Developing information security governance processes requires planning and knowledge. The preliminary information security governance framework extends the research and publications by the RACPG. Further, it interprets and applies: ISO 27799:2008 [29]; IsecT, 2012 [31]; ISM3, 2007 [32]; Department of Health's Clinical Governance Standards for Western Australian Health Services [33]; U.S. Department of Health & Human Services - OCR HIPAA, 2012 [34]; and Williams' TIGS-CMM [35]. The International Standards organisation's (ISO), ISO/IEC 27014:2013 Information technology – Security techniques - Governance of information security standard [30], was released on the 15th of May 2013, after the first three focus group interviews were conducted. There are no known intentions by ISO to release an information security governance standard specifically for healthcare, such as ISO 27799:2008 — Information security management in health using ISO/IEC 27002 was released [29]. The release of this pivotal governance standard will be addressed in the second cycle of the research.

3.1.1 Measuring Governance

Implementing governance processes alone without a measurement of capability does not provide assurance that governance processes are effective [36]. An extensive search of the literature identified models, frameworks and guidelines that proposed assessment tools for measuring governance, that were considered applicable to this research. These approaches for measuring governance were published by Mahncke, McDermid & Williams in 2009 [37]. The literature review found an absence of fit-for-purpose information security governance frameworks that could be directly implemented within general practice. A review of healthcare measurement frameworks revealed that the Capability Maturity Model® approach had previously been successfully implemented in this environment [38; 39]. It was thought

that this approach would provide an appropriate governance measure that may assist practices to improve their security governance performance.

The preliminary governance framework therefore utilises the Software Engineering Institute's 2012 [40] Capability Maturity Model® Integration (CMMI) approach to measure information security governance within general medical practice. This approach aims for systematic improvement in capabilities to demonstrate attainment of higher levels of capability maturity [41; 38]. Maturity models provide an organisation with the ability to baseline their current capability, outline proposed strategies and to measure security progress over time [42]. 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 minimum security requirements in line with the IOS/IEC 27002 standards [42].

There are five capability maturity CMMI levels as defined by the Software Engineering Institute [41; 32]. For each control activity, or 'row' in the governance framework, the practice selects the appropriate minimum level of performance applicable to the practices' capability from the range Level 1 to Level 5 (Initial to Optimising). The practice cannot move to a higher maturity level without having fulfilled all the conditions of the lower levels [10]. By selecting a level for each control activity in the governance framework, a performance measure of that activity is established.

At the first iteration, a performance level is assigned for each activity within the governance 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 framework.

The measurement outcome, ,that is the level attained, is a governance capability summary which identifies governance competence [44]. Further, a maturity model can be "used as a benchmark for comparison and as an aid to understanding" [41]. For example, a comparative assessment can be undertaken of different general practices where the information security governance framework is the common basis for comparison. This could assist in defining an industry benchmark standard.

It is proposed that general practices, during the Participant Observations, meet to review their information security. Those meetings are referred to as Governance Review Meetings. It is the task of the meeting to reaffirm or otherwise, the practices information security governance performance, and if necessary, explore any implications for the practice in terms of accountability, resource management and governance planning. The Governance Review Meeting provides a link between those responsible for information security and those accountable for information security, by providing relevant reporting. Theoretically at a Governance Review Meeting, the practice will self-assess information security by mapping their security performance to the proposed governance framework, to determine if governance controls activities are at the required performance level.

The purpose of focusing on the future management of security is to enter into discussions relating to, where the practice is positioned in terms of its aspirations to improve its information security practice. 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.

3.1.2 The Preliminary Information Security Governance Framework

The preliminary Information Security Governance Framework is an instrument to enable general practices to review their information security practices and to establish policies and procedures to meet their legal and accreditation obligations, and if necessary, move the practice to a higher level of compliance. The framework can be customised to reflect the practices' business objectives and priorities.

The preliminary Information Security Governance Framework (Figure 1) is organised into three main areas, that of Accountability, Governance Planning, and Resource Management. Within these three main areas are ten capability dimensions. Each capability dimension has numerous governance control activities associated with it. The practice maps its information security performance against the governance control activities.

The resultant information security governance framework comprises of thirty-three governance control activities with five CMMI level headings associated with each. An example of a governance control activity for Policy Coverage is provided in Table 1.

The governance framework has been combined with Williams' 2008 [46] operational capability framework to form the Mahncke-Williams Capability Framework [45]. The Mahncke-Williams Capability Framework has been developed as an information security process improvement instrument for use within general medical practice [45]. Each of the operational capabilities matrices from the operational capabilities [46], are accessed against the governance capability framework. However, this research and this paper, are concerned

Figure 1: Information Security Governance Framework [45]

1.3 Policies	
	1.3.1 Policy coverage
Initial	Information security policies are verbal
Managed	Internal best practice policies are documented and are repeatable for all key operational activities in accordance with the RACGP Computer and Information Security Standards (CISS, 2013)
Defined	Policies and procedures are defined, conform to relevant legislation and accreditation requirements. Policies have been approved and are signed off on by management.
Quantitatively Managed	Number of implemented policies measured as a percentage of required policies in accordance with the RACGP CISS (2013) standards.
Optimising	External best practice policies are applied (ISO/IEC 27002:2005 and ISO/IEC 27799:2008) that extend those required within the healthcare sector.

Table 1: Example of a governance control activity [45]

with verification of the governance framework.

3.2 Validating the Preliminary Information Security Governance Framework

Participants were invited to participate in the focus group interviews based on their information security expertise and/or their association with general practice. The focus group interview research method allows for purposeful sampling of participants [26].

3.2.1 Recruitment of participants

Recruiting security expert participants for the focus group interviews began in September 2012. The first focus group, Focus Group 1, comprised of identified academic information security experts. The purpose of the Focus Group 1 was to gain expert opinion on whether the preliminary framework was considered complete, useful and valid, based on industry best practice.

The second focus group participants, Focus Group 2, were recruited from key healthcare organisations, and included an e-health manager and general practitioners. The first two focus groups each comprised of three participants and the researcher. Focus Group 3 comprised of one healthcare security expert, due to participants work commitments on the day. The purpose of these focus groups was to assess whether healthcare information experts thought the framework would be useful and practical for use within Australian General Practice.

3.2.2 Focus Group Outcomes

Three focus group interviews were conducted on the 29th of October 2012 (in Perth), the 2nd of November 2012 (in Melbourne) and the 18th of February 2013 (in Sydney). The themes identified from analysis of the three focus group interviews are listed in Table 2.

Participants in Focus Group 1, whilst familiar with capability levels such as the five levels of physical security benchmark, unanimously did not believe the CMMI, 5 Level approach was appropriate for this research. All participants understood the framework and the sequential nature of the levels, that lower level conditions must all be met before higher levels can be obtained. Participants did not agree with the sequence of the CMMI levels as they felt that one could not manage something that has not yet been defined. Therefore, participant could not understand how Level 2: Managed came before Level 3: Defined within the CMMI method. Participants experience in physical security indicated that it is hard to implement quantitative management. Therefore, they did not believe that it would be possible to achieve Level 4 Quantitatively Managed due to the KPI

Focus Group 1	Focus Group 2	Focus Group 3
Objections to the CMMI approach	CMMI approach is desirable	CMMI approach inconclusive
Framework is too complex	Complexity, quite involved with 31 things to rate. A simplified version may be possible to do every three years before accreditation	Framework is too complex
Framework needs an efficacy based approach as opposed to a compliance based approach	Suggest removing the word governance, and replacing it with management	Framework must have a risk-based approach, and risk should be the first item assessed
It has to be policy driven	Policies - some areas well understood such as, disaster recover backup etc.	It has to be policy driven
Trusted vetting of staff	Comprehensive vetting and training of staff to comply with obligation	Trusted vetting of staff
Incentives and motivation to do governance	Why should GPs do it? What is the problem we are actually trying to solve? Lack of time and resources within general practice to take on these additional duties. Can't see practices doing this.	Possibly needed given the PCEHR roll out
What happens when people don't understand the technology?	Best practice is the RACGP CISS (2013) standard	Cloud based technologies should be utilised by general practices
Ease of use and perceived ease of use	Hard to find healthcare trained IT support staff	Healthcare IT trained staff are difficult to find
Suggested a toolbox approach	Accreditation – current information security requirements	Use the frameworks established by the Australian government as a basis, such as the NESAF
Implication of aggregation of information	Computer security is probably poorly done	Computer security is probably poorly done
Remove risk and implement ISO risk standard separately	Hard for all practice staff to understand the risks	All practice staff need to be aware of the risks
Need a prescribed standard, a benchmark.	-	Possibly some value in having a benchmark
Worst case scenario is that people stop trusting their GP	It would be an issue for GPs if breaches became public knowledge	Risk are increasing and that is why GPs should trust the cloud

Table 2: Major themes identified from the first three focus group interviews

approach. Participants felt that Level 4 should be removed, and that the framework should only have three levels, Initial, Defined and Managed, and Optimum. These results and other major themes are discussed under the analysis section of this paper.

The general practice and healthcare participants, in the second focus group, acknowledged that information security was an important issue within general practice, but were largely focused on whether implementation of the framework would be achievable. Currently RACGP CISS (2011) standards apply if practices use electronic health records, and are involved in electronic communications outside the practice. Participants thought that practices might complete the framework prior to accreditation. General practitioners confirmed that their staff training, including orientation was thorough: *"When new staff are employed, we have the Practice Manager go through in great detail about general issues of confidentiality and patient process, and there are specific documents that they have to read and sign on computer use and appropriate internet access and how you can't use standard email to send clinical information. This is reinforced on a day-to-day basis because we often get people requesting information to be sent by email and we say, no"*.

The Focus Group 3, an interview, advocated using the National eHealth Security and Access Framework (NESAF) and having a risk-based approach. Further, the participant believed that general practices should place their data in the cloud, with experts who understood the risk to healthcare data. Discussion of these identified themes follows.

4 Discussion

It was initially anticipated that two focus group interviews would have been sufficient to validate the proposed preliminary governance framework. The framework was however, not validated during the first two focus group interviews, and therefore a third focus group interview was conducted. The framework was updated based on the following outcomes and reflections.

4.1 Analysis

Six major themes were identified during the focus group interviews, and are presented as follows.

4.1.1 Complexity

Participants from all focus group interviews felt that the framework was too complex for its intended purpose. The framework was viewed as a high level policy by Focus Group 2, and it was considered to be a substantial undertaking to introduce it into day to day operational use by non IT trained general practice staff. *"Smaller practices will really struggle to implement these in the way they are meant to. A larger practice might, if they were forced to"*. It was considered easier, from a practice point of view to have prescribed security requirements. Participants expressed that *"security needs to be simple and work, and it must be to their benefit to do it"*. *"The framework needs to be an efficacy based approach as opposed to a compliance based approach"*. Ease of use and perceived ease of use, was an issue. *"Because I've got my firewall, I am perfectly fine"*. Whereas, for effective protection a firewall needs to be correctly configured. The preliminary information security governance framework was designed to practical and implementable. The researcher has experience implementing a similar type of e-learning matrix [47] under similar circumstances that is, with time, knowledge and financial resources. The complexity will be addressed through testing the framework during the second stage participant observations.

4.1.2 CMMI Approach

Participants in Focus Group 1 did not believe CMMI was the best measurement approach, whilst participants in Focus Group 2, felt it was intuitive and understandable. Consideration was given to reducing the number of levels to three, as advised by Focus Group 1. However, it meant that too many instructions were needed in each level, and that five levels allowed for a clearer and simpler spread of information. Participants in Focus Group 1 advised reviewing the Technology Acceptance Model (TAM), which *"challenges the notion that because you understand the lower level processes, you may not necessarily understand the higher level processes"*. *"What happens when people don't understand the technology?"* *"CMMI assumes you understand the technology, therefore you trust it"*. *"That means that you can't have assurance"*. A solution would be to establish a companion set of explanations and directions to training and implementation resources applicable to the proposed framework. Another approach was the Task Technology Fit (TTF), which challenges CMMI *"saying it doesn't go far enough"*. These concerns will be further addressed in the next stage of the research, the Participant Observations.

4.1.3 Governance

Participants in Focus Group 2 were quite convincing in their argument to drop the word governance from

the framework. The difference between management and governance is not always apparent although both are equally important [48; 49]. Management refers to the "activities of planning, organising, staffing, leading or directing, and controlling an organisation for the purpose of accomplishing the business objectives" [48]. According to Guldentops [49] management focuses on addressing the effectiveness of current information security practices that address the current organisational objectives. Governance however, relates to decisions that "define expectations, grant power, or verify performance" [48]. Governance therefore is a far broader definition than management and includes measuring governance performance and determining and adjusting practices to the future needs of the organisation [48]. The preliminary framework therefore is a governance framework. However, the feedback from Focus Group 2 was sufficiently persuasive to justify removing the word governance completely from the General Practice handbook and to refer to the research in future data collection interviews as information security management.

4.1.4 Policy

Information within General Practice is not just digital, it is also paper-based information. Therefore, the proposed framework would need to be policy focused. *"Focus has to be on establishing the appropriate information security policy, only then can you move forward with establishing the other levels of control"*. During Focus Group 2, participants were asked about the degree of implementation of the ten RACGP CISS operational policies. The two general practice participants, who were familiar with CISS and its implications, said they only had one general information security policy and implied they were not likely to implement all ten policies. Further questioning established that they required training support and policy templates in order to comply with these policies. A discussion in regards to the Practice Manager being responsible and the assumption that the Practice Manager would be skilled enough to write these policies ensued.

4.1.5 Risk Approach

Information security literature proposes a risk based approach to information security. It was therefore unanticipated that the Focus Group 1 felt that risk should be removed from the framework as it was considered to be a repeat of what has been addressed in other ISO standards. *"In terms of the standard you are trying to achieve, the risk has already been done and security needs to be functional and risk management referred to, as opposed to a rehash of risk management"*. *"To achieve what you want to achieve, you need to move away from risk and say this is about risk mitigation at a functional level"*. Focus group 3 confirmed that risk management is a governance activity, and therefore needs to be incorporated into the framework. Additionally, the assumption that the risk ISO standards have been implemented separately is not correct. The RACGP CISS (2013) standard includes risk management.

Participants in Focus Group 2 felt that *"practice staff themselves, don't understand the risk"*. *"How do we get staff to be aware of the risks and what the risks are?"* Participants felt that the risks would need explanation within the framework, *"So computer security on my sort of rating scale about things that I think are really really important, is actually quite low"*. Consideration then under each of the ten headings in the governance framework, an explanation of the risk and why it needs should be mitigated is required.

4.1.6 IT support

Participants in the Focus Group 2 raised an important issue, the difficulty in recruiting knowledgeable healthcare trained IT professionals. Without trained IT staff, whether outsources or directly employed, many of the technical and operation security measures would not be implemented. Self-assessment, as this framework largely is, addresses human behaviours as relates to security. Being RACGP CISS (2011, as 2013 was yet to be released) compliant (or ISO/IEC 27002:2005 compliant), is an entirely different issue. General practices are reliant of IT staff understanding and doing security procedures. During the second stage of this research, IT staff will be encouraged to participate in the Governance Review Meetings (now known as Information Security Review Meetings). When participants were asked about IT consistently reporting to them about IT issues, participants said only *"mostly with the usual issues. They tend to fix problems as they come up"*.

4.2 Focus Group Reflections

Three participants per focus group was an ideal number of participants given the complexity of discussions in these interviews. The six participants per focus group as detailed in the research proposal, would have been difficult to facilitate. One hour, was an appropriate time frame in which to ask ten open-ended questions and the resultant discussions. In future focus group interviews, the researcher will aim to recruit three participants per interview.

An Information Security Governance Guideline handbook was circulated to all three focus group participants prior to the focus group interview. The handbook contained the complete framework and required explanations. As information security governance is emerging, and ISO had yet to release their ISO/IEC 27014 Draft standard, it was considered unreasonable to expect participants to know what governance aspects should be included in the framework. During Focus Group 3, the researcher sought verbal confirmation as to what aspects of information security governance should be included, or excluded from the framework. The outcome was inconclusive, as it was far too broad and complex a question to answer without the necessary documents at hand.

Example of a Capability Control Activity	
Level 1	Initial: Processes unpredictable, poorly controlled and reactive
Level 2	Defined: Processes are monitored and controlled in accordance with policy
Level 3	Managed: Defined processes characterised by continuity, incident resolution and prevention.
Level 4	Established: Processes are measured and controlled for quality and performance
Level 5	Optimised: Processes are continually improved based on a quantitative understanding of the practice's objectives

Table 3: Updated Maturity Level Focus

4.3 Framework Development Reflections

The Australian Government launched the Personally Controlled Electronic Health Record (PCEHR) in July 2012 [50]. PCEHR is *"a secure, electronic record of your medical history, stored and shared in a network of connected systems. Information in a PCEHR will be able to be accessed by you and your authorised healthcare providers"* [50]. PCEHR is a separate electronic health record system, different from the electronic health records a General Practitioner may record during a consultation, as it is intended for a different purpose. The implementation of the PCEHR will impact on the RACGP CISS standards. Therefore, this information security governance framework will need to take three important documents into account as they are directly applicable to Australian General Practice, they are: the RACGP CISS Standards [5]; NESAF (National E-Health Security and Access Framework) [9] and the new ISO/IEC 27014:2013 Information technology - Security techniques - Governance of information security standard. Following the first focus group, the researcher become cognisant of the fact that the completed RACGP CISS checklist included in the CISS standards, are sighted together with relevant documentation during General Practice accreditation. Consequently, the proposed framework was modified as in Table 3.

The updated CMMI framework headings for each capability control activity was amended as described in Table 4.

Further, in response to focus group participant requests, companion training and resources are under development.

The development of the preliminary Information Security Governance Framework has been a significant undertaking in the first cycle of this research. The second cycle, part of the First Stage of the research, will amend the framework taking into account the new ISO/IEC 27014:2013 standard and the release of the RACGP CISS (2013) in June 2013. As such, the governance framework will be adapted to include measuring adherence to the policies and processes as provided within the CISS (2013) standard. Further, revisions to the ISO/IEC 27001:2005 [52] and ISO/IEC 27002:2005 [53] standards, are proposed for release later in 2013, which may therefore require the CISS (2013) to be further updated. Further focus groups will need to be conducted in order to validate the amended framework. The participant observation research data may assist in providing an insight into the implementation of the CISS standards within Australian General Practice.

5 Conclusion

In an environment that is embracing e-health, the importance of information security governance is emerging as a key factor in the assurance and protection of healthcare information. To complement and build on developments in information security practices, investigation into the effective governance processes that can be aligned with, and fed into by, information security practice has been undertaken. The aim of this cycle of the research was to develop and validate an information security governance framework within the general practice environment.

As such, a flexible qualitative research approach was identified in action research, which would enable iterative changes to the framework to be made throughout the research process. Consistent with other frameworks and practices in security, CMMI was selected as a suitable measurement against which to model a new information security governance process. The formulation of an initial information security governance framework was

Framework Updates	
CMMI was retained, and the five CMMI levels were maintained	Framework was updated to measure the policies and process of the RACGP CISS standard. Previously not included in the framework
Levels 2 - Defined and Level 3 - Managed, were swapped	An audit policy was included
Level 4, name was changed to Established	The word governance was replaced with management, as in information security management
Level 5, name change to Optimised in line with the other 'ed' endings	A Disclaimer statement was added in preparation for applying the framework in general practices
Framework name change the Mahncke-Williams Capability Framework (Mahncke & Williams, 2012), also known as the capability framework.	Risk management was not removed from the framework, and the order of the 10 areas were rearranged so that risk could be addressed first in line with best practice
An information security awareness survey was added for staff	The visual look of the framework was improved, in part to address the issue of complexity
Measuring human risk was added	A Glossary was added

Table 4: Framework Updates

based upon the literature, and review through action research methodology sought to validate this framework.

The first three focus groups failed to validate the preliminary framework. However, as has been evident during this research, the information security literature is continually being updated in response to the current environment. During this research a new ISO standard was released, ISO/IEC 2701:2013, and further the RACGP released a new version of their CISS (2013) standard. Therefore, the framework required amending and validation during a second research cycle. The governance framework will be further adapted to include measuring adherence to the policies and processes within the new CISS (2013) standard.

In subsequent research the modified framework will be tested in General Practice to determine if information security governance can be implemented into a healthcare environment. Further, it will be determined if implementation of the framework could improve security performance within General Practice. The significance of this work to date therefore, is the application of information security governance within General Practice. Securing healthcare information is vitally important in the developing electronic healthcare environment.

Acknowledgements

Rachel J Mahncke is the PhD candidate (the researcher), and Associate Professor Patricia A H Williams is the Principal Supervisor.

Conflict of Interests

None declared.

References

1. Mahncke RJ, Williams PAH. Australian primary care health check: Who is accountable for information security? Proceedings of the 9th Australian Information Security Management Conference. SECAU Security Research Institute, Edith Cowan University, Perth, WA; 2011:48-54.

2. Ponemon Institute. Electronic Health Information at Risk. 2009 [cited 2012 Jul 24]. Available from: http://www.ponemon.org/data-security.

3. Allen C. In Healthcare industry CIOs, CSOs must improve security. 2012 [cited 2012 Mar 8]. Available from: http://ithealthcare.computerworld.com/health-care/42988/healthcare-industry-cios-csos-must-improve-security.

4. Privacy Rights Clearinghouse. Data Breaches: A Year in Review. 2011 [cited 2012 Aug 21]. Available from: https://www.privacyrights.org/data-breach-year-review-2011.

5. The Royal Australian College of General Practitioners (RACGP). Practice Standards. Computer and information security standards. 2013 [cited 2013 Jun 30]. Available from: http://www.racgp.org.au/your-practice/standards/ciss.

6. International Organization for Standardization. ISO/IEC 27002:2005 International standard - Information technology - Security techniques - Code of practice for information security management. 2005 [cited 2009 May 15].Available from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103uis.georgetown.edu/departments/eets/dw/GLOSSARY0816.html.

7. General Practice Computing Group (GPCG). Security guidelines for general practitioners. 2004 [cited 2009 Jun 22]. Available from: http://www.gpcg.org.au/index.php?option=com_content&task=view&id=128&Itemid=38.

8. Department of Health and Ageing. Government of Western Australia. Clinical Governance Standards for Western Australian Health Services. 2005 [cited 2012 Apr 10]. Available from: http://www.safetyandquality.health.wa.gov.au/docs/clinical_gov/1.4%20Clinical%20Governance%20Standards.pdf.

9. National E-Health Transition Authority (NEHTA). NEHTA releases eHealth information security and access framework to strengthen patient records protection. 2013 [cited 2013 Feb12]. Available from: http://www.nehta.gov.au/media-centre/nehta-news/942-nehta-releases-ehealth-information-security-and-access-framework-to-strengthen-patient-records-protection

10. ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. 2013 [cited 2013 Feb 12]. Available from: http://www.isaca.org/COBIT/Pages/default.aspx.

11. IT Governance Institute. COBIT 4.1 Excerpt. 2007 [cited 2009 Mar 20]. Available from: http://www.itgi.org/Template_ITGI.cfm?Section=Recent_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=45948.

12. National Institute of Science and Technology (NIST). Security Metrics Guide for Information Technology Systems. Special Publication 800-55. 2003 [cited 2012 Apr 10]. Available from: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

13. Committee of Sponsoring Organisations of the Treadway Commission (COSO). Putting COSO theory into practice. 2005 [cited 2009 Jun 2]. Available from: http://www.coso.org/resources.htm.

14. Hertzog P. Open Source Security Testing Methodology Manual (OSSTMM3). 2010 [cited 2012 Apr 20]. Available from: http://www.isecom.org/research/osstmm.html.

15. Williams PAH. 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; 2007.

16. Harris S. Information Security Governance Guide. 2006 [cited 2012 Apr 25]. http://searchsecurity.techtarget.com/tutorial/Information-Security-Governance-Guide.

17. Schensul JJ. Methods. The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. [cited 2009 May 20]. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n268.html.

18. Williams PAH. Making research real: Is Action Research a suitable methodology for medical information security investigations?. In C. Valli and A. Woodward (Eds), Proceedings of the 4th Australian Information Security Management Conference, School of Computer and Information Science, Edith Cowan University, Perth, WA. 2006: 184-195.

19. Hampshire A, Blair M, Crown N, Avery A, Williams I. Action research: a useful method of promoting change in primary care? Family Practice. 1999; 16(3): 305.

20. Myers MD. Qualitative research in business & management. Los Angeles: SAGE Publications Ltd; 2009.

21. Cullen J. The needle and the damage done: Research, action research , and the organizational and social construction of health in the "information society", Human Relations. 1998; 51(12): 1543-1564.

22. Baskerville R, Wood-Harper AT. A critical perspective on action research as a method for information systems research, Journal of Information Technology, 1996;11(3):235-246.

23. McIntyre A. Participatory action research. Los Angeles : Sage Publications; 2008.

24. Somekh B. Action Research. The Sage Encyclopedia of Qualitative Research Methods. SAGE

Publications. 2008 [cited 2009 May 20]. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n4.html.

25. McDermid DC. The Development of the Business Rules Diagram. PhD Thesis. 1998 [cited 2009 Jun 22]. Available from: http://espace.library.curtin.edu.au:80/R/?func=dbin-jumpfull&object_id=9382&local_base=GEN01.

26. Krueger RA , Casey MA. Focus Groups. The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. 2009 [cited 2009 May 20]. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n.html.

27. McKechnie E. Observational Research. The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. 2008 [cited 2009 May 20]. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n295.html.

28. The National Institute of Standards and Technology (NIST). NIST SP 800-100 Information Security Handbook: A Guide for Managers. 2006 [cited 2013 Feb 12]. Available from: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

29. International Organization for Standardization (ISO). ISO 27799-2008 Health informatics — Information security management in health using ISO/IEC 27002. 2008 [cited 2009 Jun 15]. Available from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41298.

30. International Organization for Standardization (ISO). ISO/IEC 27014 Information 53. technology – Security techniques-Governance of information security (DIS). 2012 [cited 2012 Jul 31]. Available from: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43754.

31. IsecT Ltd. ISO/IEC 27014 Information technology – Security techniques- Governance of information security (DIS). 2012 [cited 2012 Jul 31]. Available from: http://www.iso27001security.com/html/27014.html.

32. ISM3 Consortium. Information security management maturity model. 2007 [cited 2013 Feb 12]. Available from: http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00.pdf

33. Department of Health. Clinical Governance Standards for Western Australian Health Services. 2005 [cited 2012 Jul 31]. Available from: http://www.safetyandquality.health.wa.gov.au/initiatives/clinical_governance.cfm.

34. U.S. Department of Health & Human Services. OCR HIPAA Audit Protocol. 2012 [cited 2012 Aug 7]. Available from: http://ocrnotifications.hhs.gov/hipaa.html

35. Williams PAH. 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; 2007.

36. Xenos . Technical issues related to IT governance tactics: Product metrics, measurements and process control. In Van Grembergen, W. Ed. Strategies for information technology governance. Idea Group Publishing: Hershey, PA, USA; 2004.

37. Mahncke RJ, McDermid DC, Williams PAH. Measuring Information Security Governance Within General Medical Practice. Proceedings of the Australian Information Security Management Conference. SECAU Security Research Centre, Edith Cowan University, Perth, WA. 2009 [cited Mar 12]. Available from: http://ro.ecu.edu.au/ism/9/.

38. Williams PAH. Information governance: A model for security in medical practice. Journals of Digital Forensics, Security and Law. 2007; 2(1): 57-72.

39. ISACA. CobiT 4. 2004 [cited 2012 Jul 31]. Available from: http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx.

40. Carnegie Mellon Institute. CMMI® for Services, Version 1.3. 2010 [cited 2013 Mar 12]. Available from: http://cmmiinstitute.com/cmmi-getting-started/.

41. Software Engineering Institute. Capability Maturity Model for Software (CMM). 2009 [cited 2009 Mar 12]. Available from: http://www.sei.cmu.edu/cmm.

42. PooleV. Why information security governance is critical to wider corporate governance demands – a European perspective. 2006 [cited 2009 Feb 22]. Available from:

http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=30681&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

43. Williams PAH. The application of CMM to practical medical security capability. Journal: Information Management & Computer Security. 2008;16(1):58 - 73. doi: 10.1108/09685220810862751.

44. Beveridge C. Information governance. Measures for preserving stakeholder confidence. 2008 [cited 2009 Feb 22]. Available from: http://www.colinbeveridge.com/index.php/downloads.

45. Mahncke RJ, Williams PAH. Developing governance capability to improve information security resilience in healthcare. Proceedings of the 1st Australian eHealth Informatics and Security Conference, SECAU Security Research Centre, Edith Cowan University, Perth, WA; 2012.

46. Williams PAH. The application of CMM to practical medical security capability. Information Management & Computer Security. 2008;16(1):58 - 73. doi: 10.1108/09685220810862751.

47. BECTA. Developing an elearning strategy: BECTRA Matrix. 2006 [cited 2013 Feb 12]. Available from: http://designing.flexiblelearning.net.au/tours/documents/becta_matrix.pdf.

48. de Haes S, Van Grembergen W. IT governance and its mechanisms. Information Systems Control Journal 1. 2004 [cited 2009 Feb 22]. Available from: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16700&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

49. Guldentops E. Governing information technology through CobiT. In Van Grembergen, W. Ed. Strategies for information technology governance. Idea Group Publishing: Hershey, PA, USA; 2004.

50. National E-Health Authority (NEHTA). What is PCEHR?. 2013 [cited 2013 Feb 12]. Available from: http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcehr.

51. Standards Australia. HB 174:2003 Information security management - Implementation guide for the health sector. 2003 [cited 2013 Feb 12]. Available from: http://infostore.saiglobal.com/store/details.aspx?ProductID=568742.

52. International Organization for Standardization (ISO). ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements. 2005. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=42103.

53. International Organization for Standardization (ISO). ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management. 2005. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=50297.

Correspondence

Rachel J Mahncke
Edith Cowan University
School of Computer and Security Science
Building 13, Room 13.107C
Edith Cowan University
2 Bradford Street
Mount Lawley WA 6050
rmahncke@our.ecu.edu.au