2008

Moving Towards Information System Security Accreditation within Australian State Government Agencies

Stephen Smith  
University of New South Wales, stephen.smith@unsw.edu.au

Rodger Jamieson  
University of New South Wales, r.jamieson@unsw.edu.au

Deborah Bunker  
University of New South Wales, d.bunker@unsw.edu.au

Donald Winchester  
University of New South Wales, d.winchester@unsw.edu.au

Follow this and additional works at: http://aisel.aisnet.org/amcis2008

Recommended Citation
http://aisel.aisnet.org/amcis2008/46

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Moving Towards Information System Security Accreditation within Australian State Government Agencies

Stephen Smith  
School of Information Systems  
University of NSW  
Australia  
stephen.smith@unsw.edu.au

Rodger Jamieson  
School of Information Systems  
University of NSW  
Australia  
r.jamieson@unsw.edu.au

Deborah Bunker  
School of Information Systems  
University of NSW  
Australia  
d.bunker@unsw.edu.au

Donald Winchester  
School of Information Systems  
University of NSW  
Australia  
d.winchester@unsw.edu.au

ABSTRACT
This paper investigates the current status of Information System Security (ISS) within New South Wales State government agencies in Australia. A 3-year longitudinal survey was used to increase awareness and motivate ISS managers. In addition, the survey was used as a management tool to monitor compliance with ISS standard’s controls (AS/NZS17799:2001). In 2004 an amendment to the standard added critical success factors (CSFs) as being necessary for an agency’s movement to accreditation. An analysis of the CSFs results was undertaken to determine the status of an independently acting agency’s security readiness and they were summarized to then provide an overall measure. This measure provided a ‘benchmark’ for an agency’s security readiness to the standard’s CSFs (AS/NZS17799:2004.AMDT). While the process for improving security based on CSFs is adequate, actual improvement in ISS across government requires further effort. This research contributes to the level of understanding of ISS compliance within e-Government.

Keywords

INTRODUCTION
For business and government, the Internet has provided a seamless communication channel between organizations and customers, which is independent of time and geographic boundaries (Greenfield and Campbell, 2004; Quelch and Klein, 1996). However, in recent times growth of electronic data interchange (EDI) in Australia has been slower than expected (C&L, 1994; Cullen, 1995), partly due to a number of risks and barriers, incorporating technological, security, control, legal and organizational issues (Cullen, 1995). E-Government has been defined as “the use of information and communication technologies (ICT) to improve the activities of public sector organizations” (Heeks, 2002, p3).

Government information repositories are an important resource that should be secure. Information should be protected at the whole-of-government (WoG) and individual agency level. It is clear that where the public is involved in transacting electronically with government, public confidence is essential to ensure the future viability of these services. Cost savings are a major driving factor towards an increasing amount of electronic services, especially as the government is moving towards greater efficiency within the public service (and scrutiny via 4-year election cycle).

Information Systems Security (ISS) is an essential part of ensuring public confidence in government and refers to: [The] protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats (http://www.its.bldrdoc.gov/projects/dev glossary/_information_systems_security.html).
The aim of this research is to understand IS Security compliance across New South Wales (NSW) state government agencies and also to measure this compliance. The NSW government is the largest state government in Australia by population, government agency full-time employees (FTEs) and revenue. Based on government agency FTEs, the NSW state government is also one of largest (non-national or non-Federal) governments in the Asia-Pacific region, similar in size to Washington or Arizona State in the United States (US) or Ontario and Quebec provinces in Canada. It is larger than most governed counties in the United Kingdom (UK), government metropolitan regions in France, states in Germany, or prefectures in Japan. Due to its size and relationship to NSW citizens ISS compliance is an important factor in its operations.

The plan of our paper is as follows. The next section reviews the literature. The third section introduces the background to the study. The fourth section explains the methodology and the fifth section discusses the results. The sixth section concludes and gives suggestions for further research. The final section looks at implications and limitations.

LITERATURE REVIEW

Current ISS management literature is well documented, with many ISS management strategies, technologies, frameworks and methodologies having been developed. Kadam (2007, p. 246) posits that “the development of the information security policy is a critical activity”. An information security policy should be selected on appropriate control objectives that need to be achieved based on the requirements of the organization (Kadam, 2007). The objectives can be taken from a standard such as International Standards Organization, ISO 27001, a framework or code such as ISO 17799, Control Objectives for Information and related Technology (COBIT), legislation such as the US Health Insurance Portability and Accountability Act of 1996 (HIPAA), the European Union Data Protection Act (1998) or recommendations based on an accord like Basel II (Kadam, 2007). Most of this research, however, focuses on e-Commerce implementation or on the technical issues of information system security (Backhouse and Dhillon, 2001). There is very little research in the e-Government domain and research into ISS as a whole is still in its infancy (Sharman, Rao and Upadhyay, 2004). While the literature indicates a predominately ‘positivist’ viewpoint, there is a trend to move away from a technical context to a wider scope for information security management (refer Backhouse and Dhillon, 2001; Siponen and Willison, 2007). This move has assisted in providing a more diverse understanding of information security management and guides research to develop better methods for the management of information security (see, for example, Siponen, 2005a, 2005b; Siponen and Iivari, 2006).

“Standards (de jure) are fundamental compatibility specifications that shape the configuration of information systems” (Backhouse, Hsu and Silva, 2006, p.413). Von Solms (1999) examines information security management in the context of businesses having to comply with a standard (British Standard, BS 7799) before other organizations allow them to supply goods to their network. Smith (2005), Smith, Bunker and Pang (2006), Smith and Jamieson (2006), and Smith, Jamieson and Winchester (2007) examine ISS standards in an e-Government context using action research methodology. De jure standards are often updated periodically to reflect the changing nature of the underlying environment and ISS standards have had updates to keep up with ISS innovations (for an illustration of ISS standard development over time (and regions), see Backhouse et al., 2006; Smith et al., 2006). This review clearly indicates the two major gaps in the literature, namely the lack of research into Information Security Management and into e-Government, especially in the intersection of the two domains.

BACKGROUND TO STUDY

The NSW government endorsed a strategy called the ‘Shared Corporate Services Strategy’ (SCS) to improve the delivery of corporate services, realize the full potential and benefits IS/IT technologies and to reduce costs. The purpose of this strategy was to provide a consistent standard approach to government services. The Office of Information and Communication Technology (OICT, 2001) recognize two security standards (and their updated standards) in the ICT area:

- ‘Common Core Criteria’ (ISO 15048) – this standard outlines engineering processes for developing software or hardware related to ICT security products; and
- ‘Information security management’ (Australia Standard/New Zealand Standard, AS/NZS4444:1999) – specification for information security management systems. It should be noted that this standard has been superseded by AS/NZS17799.1:2001, which was amended in AS/NZS17799.1:2004 AMDT (amendment).

The NSW Government adopted the AS/NZS17799.1:2001 (and amendment) standard as the minimum level for their agencies to achieve. Agencies were required to achieve compliance to this standard within three years to ensure a consistent approach to information security. The number of NSW government agencies varied from the first survey in 2002 to the 2004 survey because of changes in the structure of government, e.g., agencies can merge together (2 into 1), and new agencies can be created. The number of fully funded agencies classified as budget dependent in 2002 was 71. We group the agencies by size using full-time equivalent employees (FTEs) where the cutoffs for the groups are shown in Table 1, for large (>1,000 FTEs), medium (350-1,000 FTEs) and small (<350 FTEs) groups.
Table 1. The Distribution of Budget Dependent Agencies by Staff Numbers (FTEs).

Previous research investigated ISS in Australia, through the analysis of the ten (10) categories outlined in Table 2 of Security Standard AS/NZS17799.1:2001 (refer, Smith et al., 2007).

<table>
<thead>
<tr>
<th>Agency Group</th>
<th>Size Cut-offs – (Full-time Equivalent, FTE, staff per agency)</th>
<th>Range (minimum to maximum) and Mean (FTE) within Size Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large</td>
<td>&gt;1,000 FTE = 18 agencies in the large group</td>
<td>Range: 1,285 to 86,541 FTEs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mean agency size = 14,295 FTEs</td>
</tr>
<tr>
<td>Medium</td>
<td>350 - 1,000 FTE = 12 agencies</td>
<td>Range: 385 to 933</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mean agency size = 627</td>
</tr>
<tr>
<td>Small</td>
<td>Small: &lt; 350 FTE = 41 agencies</td>
<td>Range: 11 to 346</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mean agency size = 124</td>
</tr>
</tbody>
</table>

Table 2. Ten Control Categories from the Security Standard

This paper diverges from Smith, Jamieson and Winchester (2007) and investigates ISS from the perspective of critical success factors (CSFs) within the amended standard AS/NZS17799.1:2004/AMDT which are shown in Table 3.

<table>
<thead>
<tr>
<th>Critical Success Factors (AS/NZS17799.1:2004/AMDT p.5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security policy, objectives and activities that reflect business objectives</td>
</tr>
<tr>
<td>2. An approach to implementing security that is consistent with the organizational culture</td>
</tr>
<tr>
<td>3. Visible support and commitment from management</td>
</tr>
<tr>
<td>4. A good understanding of the security requirements, risk assessment and risk management</td>
</tr>
<tr>
<td>5. Effective marketing of security to all managers and employees</td>
</tr>
<tr>
<td>6. Distribution of guidance on information security policy and standards to all employees and contractors</td>
</tr>
<tr>
<td>7. Providing appropriate training and education</td>
</tr>
<tr>
<td>8. A comprehensive and balanced system of measurement, which is used to evaluate performance in information security management and feedback suggestions for improvement.</td>
</tr>
</tbody>
</table>

Table 3. Critical Success Factors from AS/NZS17799.1:2004/AMDT
As a result the research question we seek to answer is as follows:

“What is the current status of information system security based on Australian standard AS/NZS17799.1:2004.AMDT (now International Standard Organization, ISO 27001) critical success factors within New South Wales state government agencies”?

**METHODOLOGY**

The research question seeks to identify factors that can help provide common system’s procedures and controls to improve the level of ISS across agencies. The issues identified in the research question and survey questionnaire are based on principles and structures of the NSW state government. The objective of ISS is to preserve and secure an agency’s information repository and the business systems and processes that support them in terms of confidentiality, integrity, and availability.

From a review of the published literature, it was expected that security methodologies and frameworks like the Australian standard AS/NZS17799.1:2004.AMDT would be well established within organizations, however, this does not appear to be the case. This study seeks to fill this gap. The study as presented here involved the development of a survey instrument (Newsted, Huff and Munro, 1998), grounded in the established security body of knowledge. This instrument was then applied to a test group and resulting data was reduced using descriptive statistical analysis.

Information systems (IS) researchers have previously used interviews to gain insight (Fontana and Frey, 1994) and surveys as a tool to acquire ISS data for management ISS investment decisions (Straub, 1990), and to analyze various types of computer and internet attacks (Bagchi and Udo, 2003; Hinde, 2002; Thompson, 1998) and abuse (Baskerville, 1993). For IS researchers who carry out their own surveys (as opposed to using secondary survey data) the IS literature sets out methods that should be followed to validate instruments (e.g., Straub, 1989) and to maintain research rigor. Other IS researchers have based their survey questions on specific areas within the policy documentation of government, and/or from within ISO standards (Smith, 2005; Smith, Bunker and Pang, 2006; Smith and Jamieson, 2006; Smith, Jamieson and Winchester, 2007).

To monitor this process of an agency achieving compliance to the AS/NZS17799.1:2004.AMDT standard, the survey was placed online and agencies were requested to complete it at regular intervals to measure their progress. The first online security survey was in November 2001. Seven surveys in all were completed (see Table 4, for survey dates) only six looking at CSFs with the first survey being a pilot study. The survey contained 85 questions, taking over 30 minutes to complete plus the time it would take to collect and consolidate the agency data for the survey questions. Between surveys, interviews and forums also took place to gain feedback from ISS managers. Relevant survey feedback from both interviews and a forum added data comprehensiveness to the survey cycle. The main focus of this study is the online security surveys analysis. Additional government agency information (e.g., FTEs) was obtained from annual reports, reports, publication, and their website(s).

**DISCUSSION OF RESULTS (SECURITY STANDARD AS/NZS17799.1:2004.AMDT)**

The survey data was analyzed against each of the ISS CSFs.

**Security policy, objectives and activities that reflect business objectives**

This factor was directed at the government agency level. The achievement of this factor was demonstrated by 41 agencies in 2004 having a security policy, which equates to 36% compliance. The security policy states the objectives of security compliance within the business environment, and the security plan spells out the activities, which need to be undertaken. The number of agencies with a security plan in 2004 was 24, which represent 21% of agencies (based on the 113 responses to this question).

**An approach to implementing security that is consistent with the organizational culture**

This factor was directed at the Whole of Government (WoG) level. The entire project represents a consistent approach to security across government. It began with the first Premier’s Circular PC2001-46 in April 2001 and is still ongoing. The Premier’s Circular is an instruction issued by the head of state government agencies CEO’s requiring them to implement specific policy and procedures within their administration. The WoG strategy was mandated for all agencies to achieve certification by December 2004 although the deadline was moved to December 2006.
Visible support and commitment from management

This factor was directed at the government agency level. The compliance to this success factor was demonstrated by 131 agencies attempting the on-line security survey and only eight (8) agencies made no attempt to complete in 2004. This meant that the majority of agencies have some form of management commitment to improving security within their agency.

This CSF of ‘management support and commitment’ is addressed in two previously discussed issues namely:

- Category 1 - Security Policies - The achievement of this factor is measured by 39 chief executive officer’s (CEO’s) signing off the 73 agency security policies in 2004, which equates to 53% (i.e., 39/73) support and commitment by senior management.

- Category 2 - Security Organization - Allocation of an ISS Managers - the achievement of this factor is measured by the increasing support of CEO’s from 46.3% (i.e., 37 ‘yes’ responses from 80 agencies which answered the question) of agencies in 2001 with an ISS manager to 79.5% (i.e., 89 ‘yes’ responses from 112 agencies which answered the question) in 2004 which means considerable support and commitment from senior management.

A good understanding of the security requirements, risk assessment and risk management

This factor was directed at the government agency level. The achievement of this factor is demonstrated by the majority of agencies identifying risks within their agencies (for business continuity planning, BCP and e-Commerce) and rating the assessment level in 2004 as demonstrated on the graph in Figure 1. The results in Figure 1 show an even distribution of risk with the exception of the majority of agencies having a low assessment for their e-Commerce systems and medium risk for their risk assessment of BCP within the agency.

![Figure 1. Agency Risk Assessment](image-url)
Figure 2: Agency Risk Assessment for e-Commerce systems

<table>
<thead>
<tr>
<th></th>
<th>Apr_02</th>
<th>Aug_02</th>
<th>Nov_02</th>
<th>Nov_03</th>
<th>Nov_04</th>
</tr>
</thead>
<tbody>
<tr>
<td>combined</td>
<td>2.35</td>
<td>2.33</td>
<td>2.39</td>
<td>2.46</td>
<td>2.35</td>
</tr>
<tr>
<td>small</td>
<td>2.58</td>
<td>2.33</td>
<td>2.28</td>
<td>2.28</td>
<td>2.17</td>
</tr>
<tr>
<td>medium</td>
<td>2.18</td>
<td>2.46</td>
<td>2.38</td>
<td>2.63</td>
<td>2.33</td>
</tr>
<tr>
<td>large</td>
<td>2.67</td>
<td>2.20</td>
<td>2.76</td>
<td>2.94</td>
<td>3.00</td>
</tr>
</tbody>
</table>

Figure 3: Rating of the level of security for e-Commerce systems

<table>
<thead>
<tr>
<th></th>
<th>Apr_02</th>
<th>Aug_02</th>
<th>Nov_02</th>
<th>Nov_03</th>
<th>Nov_04</th>
</tr>
</thead>
<tbody>
<tr>
<td>combined</td>
<td>3.18</td>
<td>2.92</td>
<td>2.78</td>
<td>2.88</td>
<td>2.78</td>
</tr>
<tr>
<td>small</td>
<td>2.81</td>
<td>2.76</td>
<td>2.52</td>
<td>2.61</td>
<td>2.56</td>
</tr>
<tr>
<td>medium</td>
<td>3.18</td>
<td>3.69</td>
<td>3.29</td>
<td>3.47</td>
<td>3.00</td>
</tr>
<tr>
<td>large</td>
<td>3.00</td>
<td>2.70</td>
<td>3.24</td>
<td>3.33</td>
<td>3.37</td>
</tr>
</tbody>
</table>

Figures 2 and 3 plot the mean of these measures. Briefly, the analysis of the means suggests for both figures that the medium sized agencies show a slightly higher risk to e-Commerce systems and a slightly higher security level than small and large agencies. The level of risk is measured using a Likert scale from 1 (low) to 7 (high). A full analysis of Figures 2 and 3 and the interaction between the measures is beyond the scope of this research paper but should be followed-up in any future research. Table 4 shows the level of risk e-Commerce systems and the level of security for those systems across the six (6) cycles that this data was collected.
Table 4. Agency Risk and Security Assessments

<table>
<thead>
<tr>
<th>How would you rate the level of security across your E-commerce systems?</th>
<th>Low</th>
<th>2</th>
<th>3</th>
<th>Medium</th>
<th>5</th>
<th>6</th>
<th>High</th>
<th>Total Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 01</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jan 02</td>
<td>16</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>36</td>
</tr>
<tr>
<td>Feb 02</td>
<td>6</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>36</td>
<td>204</td>
</tr>
<tr>
<td>Mar 02</td>
<td>32</td>
<td>8</td>
<td>14</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>36</td>
<td>204</td>
</tr>
<tr>
<td>Apr 02</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td>204</td>
</tr>
<tr>
<td>May 02</td>
<td>8</td>
<td>1</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td>204</td>
</tr>
<tr>
<td>Jun 02</td>
<td>22</td>
<td>6</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>33</td>
<td>204</td>
</tr>
<tr>
<td>Jul 02</td>
<td>15</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>33</td>
<td>204</td>
</tr>
<tr>
<td>Aug 02</td>
<td>43</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>33</td>
<td>204</td>
</tr>
<tr>
<td>Sep 02</td>
<td>33</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>33</td>
<td>204</td>
</tr>
<tr>
<td>Oct 02</td>
<td>57</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>33</td>
<td>204</td>
</tr>
<tr>
<td>Nov 02</td>
<td>38</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>1</td>
<td>2</td>
<td>13</td>
<td>204</td>
</tr>
<tr>
<td>Dec 02</td>
<td>6</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>15</td>
<td>204</td>
</tr>
</tbody>
</table>

Agencies: Small, Medium, Large

Combined

Table 4. Agency Risk and Security Assessments
<table>
<thead>
<tr>
<th>Agency Group</th>
<th>Agency Risk Assessment for e-Commerce systems</th>
<th>Rating of the level of security for e-Commerce systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>lowest risk</td>
<td>lowest risk</td>
</tr>
<tr>
<td>Medium</td>
<td>slightly higher risk</td>
<td>highest risk</td>
</tr>
<tr>
<td>Large</td>
<td>highest risk</td>
<td>highest risk at the end of 2004</td>
</tr>
</tbody>
</table>

Table 5. Rating of the Level of Risk and Security for e-Commerce Systems

Table 5 shows that all of the ratings of overall security for e-Commerce systems for each size grouping (see Table 1) are less than moderate, indicating that this could be improved.

Effective marketing of security to all managers and employees

This factor is directed at the WoG level. The entire project represents a consistent approach to security across government including:

- a top down approach (commitment at senior level);
- appointing a central government agency to monitor the level of accreditation;
- a web based information resource (central government agency website) allowing information (including links to other resources) to be disseminated to all managers and employees;
- additional premier’s circulars;
- access to relevant standards;
- regular contact with agencies; via surveys, one-on-one interviews, emails; and
- forums (refer Smith and Jamieson, 2006).

Distribution of guidance on information security policy and standards to all employees and contractors

This factor was directed at the WoG and agency level. This factor included the previous success factor and the appointment of individual certification organizations to be engaged as consultants to assist the non-accredited agencies move towards accreditation, without the need for onerous documentation to appoint them.

Providing appropriate training and education;

This factor is directed at the WoG and agency level. This was achieved by the production of a video (title ‘I wish it wasn’t me !!’) specifically targeted at government agencies. In addition in-house information sessions, induction training (including security policies), pamphlets, banners and other multimedia aids for security awareness, were produced and disseminated to agencies.

A comprehensive and balanced system of measurement, which is used to evaluate performance in information security management and feedback suggestions for improvement.

This factor was directed at the WoG and agency level. This factor includes the previous success factor ‘(f)’ and includes the WoG on-line security survey, forums, focus groups, interviews (both individual and group) and finally reporting to agencies and government on the progress of agencies security projects. This success factor is the accreditation of agencies to the security standard AS/NZS17799.1:2001.

CONCLUSION

The critical success factors for the security standard highlight a set of measures, which support the 10 control categories of Part 1 of the 2001 security standard (see Table 2). The CSF’s really define the factors that would assist this research and it has shown the factors that would assist agencies achieve certification.

From a government agency perspective, the most important factor, which was mentioned at almost every government agency interview and frequently in the forum and focus group, was ‘senior management support’. Other issues include the development of security policies, plans and informed staff to understand the security requirements, risk assessment and management of their government agency.
From a WoG perspective there were four main factors influencing the drive to improve security. The first was the Premier’s Circular PC2001-46, which established a government wide consistent approach to ISS management. The second was the use of Office of Information Communications and Technology (OICT) staff to effectively market the strategy to agencies and staff combined with providing guidance on information security policies. Thirdly, appropriate training and education was given via the video and group forums to provide an environment for government agency staff to be informed and raise concerns. Finally the development of a ‘system of measurement’ to evaluate the performance of security has been reflected in this research - the on-line security survey in conjunction with our analysis gives a measure of the performance of information security management within agencies.

The conclusion from the current survey and government agency contacts indicates that only four agencies have achieved the goal of AS/NZS17799.1:2001 (with 2004 amendment) compliance within the original target date of December 2004 and seven by December 2005 (note the due date for target compliance was extended until December 2006. Agency compliance at December 2006 is confidential).

The results were further validated externally by another government agency’s ISS survey. This research contributes to the level of understanding of ISS within the domain of e-Commerce within Government (e-Government).

Further research could develop models, theories and undertake empirical research at the intersection of ISS and e-Government to improve ISS management in government ICT practice.

**IMPLICATIONS AND LIMITATIONS**

The purpose of this study was to demonstrate an increase in compliance to security issues and the Australian Standard. This research has implications for governments who intend to progress towards ISS de jure standard accreditation. A limitation of ‘question only’ survey analysis is the possibility of bias in answering the research question. Over time participants can get better at answering the questions giving the perception of a better security. To minimize this effect additional techniques were employed. First, by providing a benchmark of responses (for the feedback of the results of their agency survey when compared to other agencies), across agencies, this motivated participants to include the major areas (for example confidentiality, integrity and availability), within their organizations security policy and plans. Second, a series of one-on-one follow-up interviews conducted to verify the survey responses and finally the certification process was independent and covered all aspects of agencies ISS project.

**REFERENCES**