Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2006 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

2006

# Does Agency Size Affect IS Security Compliance for e-Government?

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

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

Vincent Pang
*University of New South Wales*, vincentpang@acslink.net.au

# Does Agency Size Affect IS Security Compliance for e-Government?

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

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

Vincent Pang
Univ. of New South Wales
vincentpang@acslink.net.au

**Abstract**

*Security compliance has now become a major information systems management problem thanks to government regulations. Organizations are now developing methodologies and tools to assess compliance of Information Systems (IS) security. The research outlined in this paper is part of a longitudinal action research study which aims to help inform and improve security within Whole of Government (WoG). This paper examines the different effects of organisational size on IS security compliance within government organisations and how the adoption of security controls differed across small, medium and large government agencies. This paper identifies differences across government agencies rather than assuming that IS security compliance within e-government would be the same for different sized agencies. The approach utilised within this study may be extended to assess compliance with regulations in small, medium and large, multi-unit organizations in other sectors as well as government.*

**Keywords:** Compliance, Information System, Security, Risk, e-Business, e-Government

# Introduction

The transformation from traditional government practices to e-Government[14] may prove to be one of the most important policy decisions in the history of government. Research and popular press indicate that one of the major concerns of business and consumers is the security of on-line communications and financial transactions (eCommStrategies, 2000). Progress of e-Government will continue to grow if business and government are convinced that transactions are secure and reliable (The Audit Office of New South Wales, 2002).

An increasingly important aspect of government business is the development of e-Commerce systems commonly known as e-Government (Carter & Balanger, 2004). e-Government research is still immature as are e-Government business models and the benefits, which have not been fully realised. The current published literature focuses mainly on research areas such as business re-development of e-Government (driving government reform); connecting business to government connecting customers to government services; e-procurement or the payment of bills on-line; simplifying the processes of conducting business by on-line services; and grouping e-government into a one approach for all (Fingar, 1998). Current literature, however does not address a number of the main e-Government concerns surrounding risk and security issues.

The purpose of e-Government security systems is to safeguard the information being transmitted within the framework of electronic service delivery (Pivk, 2000). A New South Wales audit report

[14] "The use of information and communications technologies, and particularly the Internet, as a tool to achieve better government" *(OECD, 2003 p1*)

(2002, p.36) however stated, "*There appears to be limited knowledge at line agency level of the risks associated with increased use of the Internet and related technologies, and how best to manage them*". This paper outlines a research study which was an initiative of New South Wales Government to assist government agencies to improve the overall understanding of government's IS risks and security compliance. As the volume of electronic transactions is increasing, the extent of threats is also increasing from areas like hacking, virus infections and website defacement. It is crucial for government agencies to maintain trust with all participants and ensure associated risks are well managed (WA, 2003; Whitman, 2004). Most governments in Australia now adopt a risk management approach to security, based on risk identification, risk analysis and mitigation, combined with techniques to create awareness, deter, prevent, detect and recover from disasters.

## Information Systems Security

Information Systems Security (ISSec) is the effective implementation of policies to ensure that the confidentiality, availability and integrity of information and assets are protected from theft, tampering, manipulation or corruption. Heekes (2002), Hof (2002) and WA Government (2003) highlight the importance of IS security within e-Government systems. Electronic information is extremely portable and very easy to change. The administration, business and legal processes associated with security and protection of electronic government information have not been fully developed (Scott, 2003). Consequently, government projects are endeavouring to develop policies and procedures to improve security (Frank, 2003). From the public's perspective, government is seen as one entity; hence a security problem within one agency may be viewed as a failure of the government as an entity.

IS Security (ISS) has previously concentrated on protecting the confidentiality of documents stored electronically. In terms of the public perception of government organisations, security means the protection of records and data that are held for the purpose of administering the acts and policies of government agencies (Martin, 2005). This applies equally to paper documents as well as the data held in computer databases (Kiel, 2003). The rapid growth in the volume of information stored electronically and the uptake of e-Commerce within government has heightened the need for increased security to protect the privacy of this information and prevent fraudulent activities (Spinellis, 1999).

The process of improving security within the Whole of Government (WoG) therefore is viewed as essential. 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 increased use of electronic services, especially as the government is moving towards greater efficiency within the public service. The Office of Information and Communication Technology (OICT, 2004) in NSW outlines several benefit categories related to investment in information technology, as they relate to community expectations for:

- improved service;
- wider range of services;
- tailored services;
- geographic access to services;

- new legislation or regulations introduced;
- equity of access policies;
- reduced real operating budget;
- competition for resources;
- demand growing faster than resources; and
- changes in technology price/performance.

These driving factors can only be achieved where public confidence, and hence appropriate security, is established with the relevant information systems within the public service. These factors are a direct reference to the Critical Success Factors (CSF) of AS/NZS17799.2001/Amendent:1-2004, and underpin the successful implementation of the standard and the community expectations it reflects.

## Information Systems Security Standard

A number of frameworks AS/NZS4444:1999 have been developed and tested since the 1970s to quantify and manage the issue of information system security (Mitrou, et al, 2005). Australia's standard for Information Security Management, AS/NZS17799.1:2001 (Information technology - Code of practice for information security management), provides a framework and set of recommendations in a risk management context. Based on the British BS7799 Standard, AS/NZS17799.1:2001 has been revised for application to e-Commerce, and re-branded from its previous incarnation as AS/NZS4444.1:1999 Part 1 and AS/NZS4444.2:2000 Part 2. The Australian Standard AS/NZS17799.1:2001 and AS/NZS7799.2:2000 (revised as AS/NZS17799.2:2003) was selected as the framework for the project as it allowed agencies to be accredited to a nationally accepted and reliable approach methodology which also linked to the Australian Standard for risk management AS4360:1999 (revised in 2004). A more detailed chronology of the dates of introduction for IS Security standards in shown in figure 1 below.

The focus of AS/NZS17799.1:2001 is to protect security of information by providing a set of controls and best practices for situations that are applicable for e-Commerce. With the increasing volume of business being conducted between organisations over electronic networks, it is essential that a trusted relationship be established between the stakeholders trading together. One such scheme is for all parties to agree on an appropriate standard (AS/NZS17799.1:2001), adopt its principles, and move to certification. Accreditation and certification is possible for 7799 and recognised internationally (under ISO 17799) (Mitrou, et al, 2005), however, there are very few organisations that can offer this service and currently only two (2) organisations are offering the service of accrediting organisations and agencies in Australia. The adoption of standards is becoming increasingly important to establish benchmarks by which organisations and clients, conducting business on-line, can be assured. An additional benefit of this standard is its regular (6 monthly) review to ensure that certification to the standard is maintained, thus providing extra rigor to security compliance.

Risk management is also an integral part of AS/NZS17799.1:2001 security certification.

AS/NZS17799.1:2001 recommends a series of actions to define the scope/functions of the business project, and subsequently attempts to define the security risks associated within the scope of the project. Risks are then analysed, ordered and controls are proposed and actioned. To define the scope of the AS/NZS779.1:2001 accreditation project, the standard is broken into ten major control categories for information security, which are shown in Table 3.4. Within the framework of the ten major categories in the security standard, AS/NZS17799.1:2001 there are 127 security controls. These controls enable agencies to identify and develop safeguards to protect their information resources. Recently the standard AS/NZS17799.1:2001 has been superseded by an International Standard ISO/IEC27001:2005.

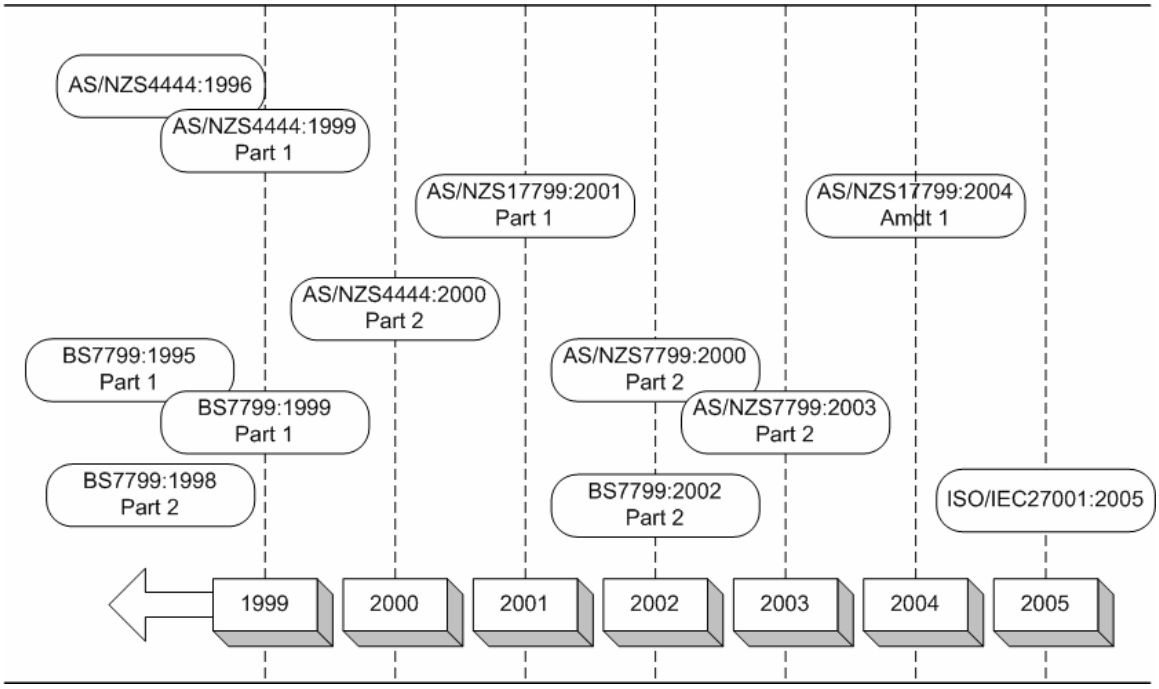


**Figure 1: Chronology of IS Security Standards**

Little is written on the risks, risk management and the level of security required to provide effective security for e-Government. Even less is written about recognising the differences between government agency categories where agencies are very diverse in size, function and funding. The vast majority of literature groups all agencies into one category type for research treatment (Cushing, 2005).

## Agency Categories

While the majority of literature groups agencies in one category governments themselves group agencies into many different categories for varying reasons. Firstly governments can categorise agencies into similar functions or portfolios (eg, health, justice, natural resources etc). Secondly agencies can be categorised by funding source either from government directly, a government trading organisation or a state owned corporation. For financial reasons (such as payroll), however, agencies are commonly grouped by size with full-time employee numbers (FTE) as the defining

criterion. Grouping by FTE is also used by other Australian governments, namely the Western Australian (WA, 2004) government, Australian the Federal government (ABS, 2005) the New Zealand government (New Zealand, 2004) and other international governments.

Another complication is that some small agencies host their IT systems with a central government agency bureau. This structure allows the creation of clusters groups and streamlines their IT operations. These clusters can be based either on shared arrangements by business type or portfolio affinity. This clustering reduces the time or resources expended on improving security for individual agencies. These clusters would create a bias towards the large agencies in terms of the management of shared services., because of there individual significance to the government

## Study Motivation

Although the state government takes the responsibility for information security, it is left to the government agency level to manage and develop strategies and polices to protect their own information. As individual agencies are the custodians of this information, they are in the best position to assess its value, and develop the appropriate security measures to protect and preserve it from threats (internal/external) and other risks.

Since individual agencies are responsible for their information this research seeks to determine an overall "rich picture" of the current status of IS security within these agencies. This philosophy is aligned to a 'whole-of-public sector' framework developed in 1977 (the Information Management & Technology Blueprint). This approach is necessary due to the increased connectivity between external agencies, businesses and individuals. Information transfers are becoming seamless and agencies need to review their security policies and practices to incorporate these connections (such as telecommunications, banking and many other services) and to review the inherent risks. In order to manage security effectively across government and other organisations, a benchmark needs to be established. National and International standards provide the level of consistency required to become a yardstick or measure as a consistent benchmark to security.

The NSW Government adopted the AS/NZS17799.1:2001 (Information technology - Code of practice for information security management) standard as the minimum level of IS security for agencies to achieve. Agencies were required to achieve compliance to this standard within three years starting in December 2001 to ensure a consistent approach to information security.

The focus of this study was to determine the factors or groups of factors that would assist agencies and organisations of different sizes improve the overall level of IS security based on AS/NZS17799.1:2001 (Information security management - Specification for information security management systems). The security control relating to this area of results and the Australian Standard are technological, physical, policy and personnel etc (Wood, 2001). These controls are the essence of an effective security framework. This framework has been validated in the Government of New South Wales (one of the six largest economies in the in Australia-Pacific region) in Australia. This research may also be useful in developing a methodology for the assessment of compliance in all organisational sectors and settings.

## Research Methods

This study concentrates on agency size as the method of agency categorisation. Categorising

Grouping agencies this way aligns them with other findings within the government domain.

This study adopts the small-medium-large grouping of government agencies based on full–time equivalent (FTE) staff numbers to analyse government responses to the survey. Although several category classifications may be applied, categorisation by government agency size in terms of FTE appears to be an accepted and established measure used already across NSW government. These categories are defined in Table 1 following:

| Category | Size | Count[15] |
|---|---|---|
| Large | > 1000 FTE. | ~ 11 |
| Medium | 350 – 1000 FTE; and | ~ 19 |
| Small | < 350 FTE[16]; | ~78 |

**Table 1 – Agencies Categories**

The Australian Standard AS/NZS17799.1:2001 (Information technology - Code of practice for information security management) contains ten major sections (see Table 2) of which nine deal with security issues and one with Business Continuity Planning.

Since agencies are required to achieve certification to the standard, the online survey questions developed for this study were grouped around the Security and Business Continuity Planning areas of the standard.

## Survey Instrument

An on-line survey (containing 85+ questions based on the Australian Standard AS/NZS17799.1:2001) was developed to measured agencies status using Likert-scale; yes/no radio button and short answer and comments. An analysis of the survey results was undertaken to determine the status of agencies in terms of security readiness and summarised to provide an overall measure. The survey was conducted between November 2001 and December 2004. Seven survey cycles were conducted across approximately 120 NSW government agencies. The number of survey questions increased during the study in three phases (also shown in table 2).

## Action Research Approach

The survey administration and development was part of a three-phase longitudinal research design that involved an initial exploratory strategy and an iterative development cycle of the survey which formed the basis of an action research study. An action research approach was used as a method to

[15] The count of agency numbers in categories varies due to agency splits and mergers dictated by central government discussions.

[16] Full Time Equivalent staff – (FTE)

directly intervene in the longitudinal survey cycles (Farbey et al., 1999). Action research is concerned with diagnosing *"a problem in a specific context and attempting to solve it in that content"* (Cohen & Manion, 1989 p2; Altrichter, 1990). Action research can also be described as *a "cyclic or spiral process, which alternates between action and critical reflection"* (Dick, 2002 p4). The flexible nature of action research is achieved by its cyclic process (see figure 2), allowed the iterations of the survey to develop a greater understanding of IS Security across the agency survey participants. These participants were the agencies nominated IS Security Manager.

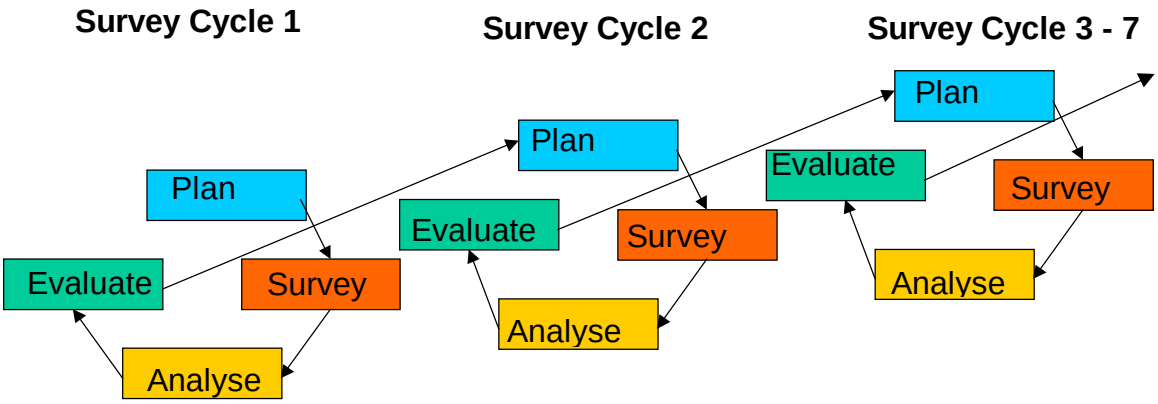


**Figure 2: Action Research Interacting Spiral**

| Key AS/NZS17799.1:2001 Control Categories for Information Security | Survey | | |
|---|---|---|---|
| | S1 | S2 | S3 |
| Security Policies | ▤ | ▤ | ▤ |
| Security Organisation | ▤ | ▤ | ▤ |
| Asset Classification & Control | | | ▤ |
| Personnel Security | | ▤ | ▤ |
| Physical / Environmental Security | | | ▤ |
| Computer & Network Mgt. | | | ▤ |
| Systems Development & Maintenance | | ▤ | ▤ |
| System Access Control | | ▤ | ▤ |
| Business Continuity Planning | | | ▤ |
| IS Policy Compliance | | | ▤ |

| Survey Cycle Questions | Survey | | |
|---|---|---|---|
| | S1 | S2 | S3 |
| Survey cycles 1 to 7 contains questions from S1 | ▤ | | |
| Survey cycles 3 to 7 contains questions from S1 and S2 | ▤ | ▤ | |
| Survey cycles 4 to 7 contained all questions | ▤ | ▤ | ▤ |

**Table 2 – Key Security Issues and Survey Distribution of Questions**

Agencies were directed by the "Head of State" to better manage the risks to their information systems and apply the necessary controls and security measures to improve their overall level of security and achieve the benchmark of certification to the standard within three years.

The survey was administered through an action research approach as many of the agencies had little or no experience with or awareness of the security standard and the full range of issues that could impact on them. The three project stages of a longitudinal seven survey cycle action research methodology saw the gradual administration of the survey questions S1, S2, S3 (see also Table 2) to an agency's IS security manager in order to gradually improve their knowledge of IS security measures at a manageable rate (considering the other demands the organisation places on their duties and time).

# Results

Agencies were asked if they had an IS security framework in place. The 10 categories of AS/NZS17799.1:2001 provided a universally recognisable description of a information security framework to the survey respondents. The requirements of the standard are an "*already accepted part of the IT Security landscape and will likely be so for the foreseeable future*" (Bindview, 2004 p4).

The three sub-category of agencies (large, medium and small) are discussed below:

Large agencies (over 1000 FTE staff) have sufficiently large corporate services structures to undertake a security program to achieve accreditation to the standard of AS/NZS17799:2001. They generally have enough resources to utilise technology wherever possible to achieve compliance to the standard.

However many large agencies are highly decentralised across long distances and many buildings which creates difficultly achieving accreditation across so many facilities. This problem is addressed in the risk analysis stage of accreditation where the highest risk business functions/processes are mitigated first and lower risk functions are subsequently dealt with.

For those agencies covering a wide geographic area, the regional or decentralised offices are usually similar in terms of organisational structures and duties performed. The process of accreditation can be scoped to permit a reduction of the number of regional offices needing accreditation for the entire organisation.

Medium-sized agencies (between 350 and 1000 FTE staff) have demonstrated the most commitment towards accreditation for their security program. In addition, they also participated in internal shared corporate services (mainly business process re-engineering) to consolidate services into fewer hardware platforms, which in turn allows more streamlined IT/IS systems.

Small agencies (under 350 FTE staff) present a more varied picture. Improving IS security across these agencies requires significant improvement due to the lack of resources and staff assigned to improving security.

| Security Policy | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Combined** | | | **Small** | | | **Medium** | | | **Large** | | |
| **Survey Date** | **No** | **Yes** | **% Yes** | **No** | **Yes** | **% Yes** | **No** | **Yes** | **% Yes** | **No** | **Yes** | **% Yes** |
| | | | | | | | | | | | | |
| **Nov_01** | 39 | 41 | 51 | 29 | 28 | 49 | 5 | 6 | 55 | 5 | 7 | 58 |
| **Jan_02** | 46 | 50 | 52 | 33 | 32 | 49 | 5 | 6 | 55 | 8 | 12 | 60 |
| **Apr_02** | 49 | 57 | 54 | 37 | 34 | 48 | 5 | 10 | 67 | 7 | 13 | 65 |
| **Aug_02** | 50 | 58 | 54 | 39 | 33 | 48 | 5 | 12 | 71 | 6 | 13 | 68 |
| **Nov_02** | 55 | 58 | 51 | 40 | 34 | 46 | 8 | 9 | 53 | 7 | 15 | 68 |
| **Nov_03** | 50 | 67 | 57 | 36 | 42 | 54 | 9 | 9 | 50 | 5 | 16 | 76 |
| A change of government after the 2003 election caused an agency re-shuffle | | | | | | | | | | | | |
| Nov_04 | 48 | 61 | 56 | 34 | 44 | 56 | 9 | 10 | 53 | 4 | 7 | 58 |

**Table 3 – Agencies with or without a Security Policy**

Table 3 highlights the percentage of agencies with a security policy, across small, medium and large categories.

Table 3 and Figure 3, demonstrate that the number of agencies with a security policy change over the period from November 2001 to November 2003 for the small (49% - 54%), medium (55% -

50%), large (58% - 76%) and combined groupings (51% - 57%). The November 2004 reflected the changes in government resulting from an agency re-shuffle. The recorded decrease in large agency security policies was possibly due to 'new' managers not being fully aware of their responsibilities in terms of the government's IS security initiative.

Overall there was an increasing trend in the number of agencies with a security policy and the decrease in the number of agencies without a security policy. Part of this improvement may be attributable to the action research approach of this study. However, there was scope for improvement with 46% of agencies still having no security policy. The remaining agencies without a security policy were more likely to have a more reactive approach to security. These agencies generally wait for security issues to emerge and then respond to the threat, in contrast to an agency having a consistent approach from having an actively documented IS security policy thus being pro-active before threats emerge.

Agencies were then asked if they had a dedicated IS security manager (see Table 4). The role of the IS security manager, was defined as having the responsibility for co-ordinating the implementation of IS security.

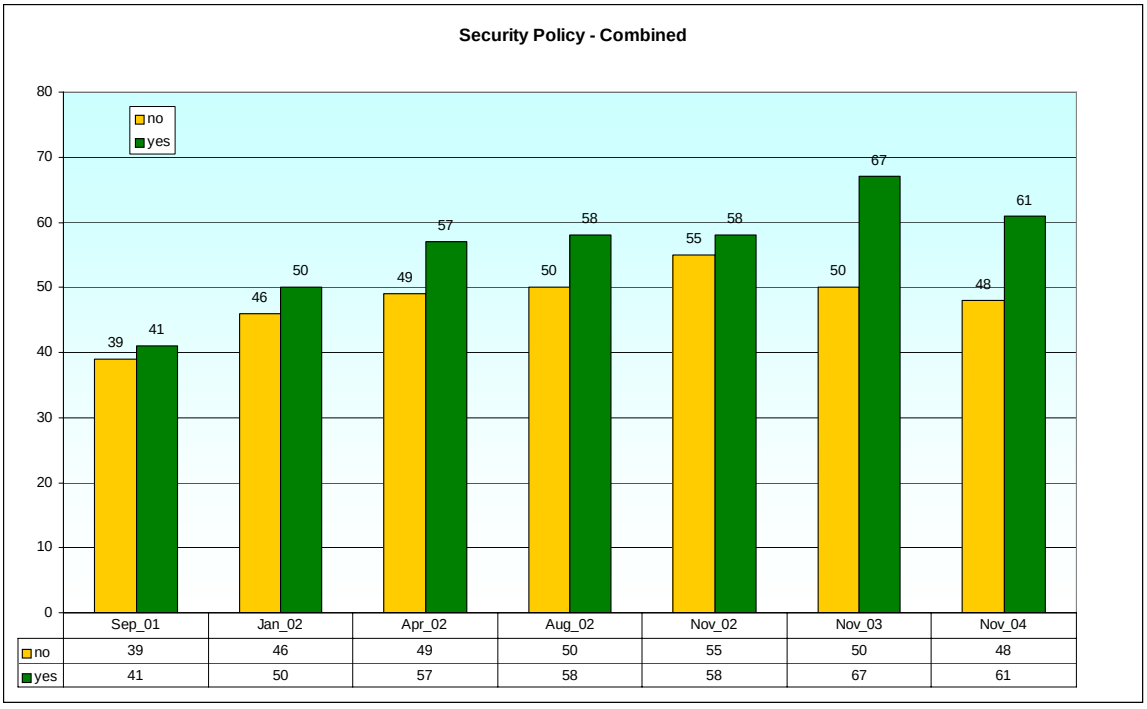


**Figure 3 - Agencies with an IS Security Manager (S-M-L Combined)**

The percentage increase in the number of IS security managers demonstrates a commitment to security within the agencies, indicating that management was becoming serious about the IS security problem. In terms of agency categories for the small agencies the percentage of IS security managers increased over the four years of the survey from 74% to 84%. For medium sized agencies the percentage of IS Security managers decreased from 100% to 70% over the survey but the number of IS Security managers did increase from 6 to 14 managers. The large agencies percentage of IS Security managers remained relatively constant (approximately 70%) however the number of IS Security managers increased from 5 managers to 14 over four years.

A detailed analysis of the on-line survey questionnaire has not been presented in this paper. However the results showed variable and significant differences between agency S/M/L categories across the seven cycles of the longitudinal survey study. The full survey results also demonstrated the impact of the action research approach to survey administration i.e. it raised awareness gradually (as well as giving incremental feedback to agencies while they learned about security compliance). Differences in resource allocation (namely IS Security Managers) between agencies of different sizes and the impact of security compliance to the standard AS/NZS17799.1:2001 were also highlighted.

In terms of completely complying with the standard only a relative few agencies managed full certification within the three-year project; however, the greater majority did make significant progress toward this goal and many other agencies subsequently did at well. The agencies that achieved full certification were in the category of medium sized agencies (in the range of 300-500 FTE staff), thus indicating IS staff and management within the agencies had the required knowledge, understanding and expertise to identify the need for effective security and begin the project immediately.

| **Do you have an IS Security Manager?** | | | | | |
|---|---|---|---|---|---|
| Survey Date | Agency Size | No | Yes | No of Survey[17] respondents | % of IS Sec Mgrs |
| Nov_01 | Small | 9 | 26 | | 74 |
| Nov_01 | Medium | 0 | 6 | | 100 |
| Nov_01 | Large | 2 | 5 | | 71 |
| Combined | | | 37 | 80 | 46.3% |
| Jan_02 | Small | 13 | 35 | | 73 |
| Jan_02 | Medium | 0 | 8 | | 100 |
| Jan_02 | Large | 6 | 9 | | 60 |
| Combined | | | 52 | 98 | 53.1% |
| Apr_02 | Small | 14 | 44 | | 76 |
| Apr_02 | Medium | 3 | 9 | | 75 |
| Apr_02 | Large | 6 | 11 | | 65 |
| Combined | | | 64 | 111 | 57.7% |
| Aug_02 | Small | 14 | 42 | | 75 |
| Aug_02 | Medium | 3 | 10 | | 77 |
| Aug_02 | Large | 4 | 11 | | 73 |
| Combined | | | 63 | 114 | 55.3% |
| Nov_02 | Small | 15 | 49 | | 77 |
| Nov_02 | Medium | 3 | 12 | | 80 |

[17] Total number of surveys received those who did not answer this questions were assumed to have no IS Security Manager.

| | | | | | |
|---|---|---|---|---|---|
| Nov_02 | Large | 5 | 15 | | 75 |
| Combined | | | 76 | 114 | 66.7% |
| Nov_03 | Small | 10 | 62 | | 86 |
| Nov_03 | Medium | 3 | 14 | | 82 |
| Nov_03 | Large | 6 | 13 | | 68 |
| Combined | | | 89 | 118 | 75.4% |
| Nov_04 | Small | 12 | 61 | | 84 |
| Nov_04 | Medium | 4 | 14 | | 78 |
| Nov_04 | Large | 6 | 14 | | 70 |
| Combined | | | 89 | 112 | 79.5% |

**Table 4 – Agencies with an IS Security Manager**

The small agencies generally had difficulty with their security projects although the percentage of agencies with IS Security Managers was high as they were mainly part-time positions however 50% of them had IS security policies. Conversely, the large agencies generally had too many core information systems to attempt to make them security compliant with all their systems. They had the lowest number of IS Security Managers at approximately 60% but further analysis suggested that they used specialist consultants to develop security policies. This explains why 58% - 76% of agencies have security policies, which for some very large agencies was an enormous task. Agencies in both these categories (small and large) would have benefited by adopting, a risk management approach that would allow them to identify those systems that were crucial to the agency and concentrate on making them compliant to the standard AS/NZS17799.1:2001. This would provide the greatest security protection to that agency's most critical system(s).

Both small and large agencies had this problem because they generally lacked a risk management strategy. A well developed business impact analysis would have allowed the available resources to be better used and permit the agency to learn the process of becoming certified to the major business system (and then subsequently roll out other less crucial systems).

Large agencies have the benefit of more resources being available for projects, however large agencies also have substantial IS/IT system investments. Any changes, updates or upgrades are expensive in terms of resources and budget. The organisation culture usually places equal importance on all systems whereas a risk management approach would identify systems that are more critical thus, creating a list of systems/projects in order of importance to the government agency. In addition, the culture within the large organisation dictated that the IS staff should be responsible for and manage the issues of achieving accreditation to the standard by themselves. This compounded the problem because newer systems are generally more complex (including security settings), thus requiring greater effort from IS staff to commission and maintain them.

In small agencies, the organisational culture had a greater influence on the lack of progress with achieving compliance. Small agencies generally have limited resources available in the IS/IT branch and additional projects, such as security compliance, must compete for limited resources. Mandating improved security across agencies placed an increased workload on the staff. Small agencies were already coping with other IS/IT issues of more complex systems, updates, software patches, equipment replacement etc, and had limited access to training courses and forums.

## Conclusions, Limitations and Further Research

Based on the discussion above, practitioners should conduct a risk analysis of their agency systems and determine the agency's most critical system and thus complete certification firstly for this system. Also, a comprehensive business impact analysis would allow senior management to assign resources to the certification of the most critical agency systems.

A strategy for large agencies trying to achieve certification to the security standard and full risk analysis of all business systems, must be undertaken to identify an agency's most vital business system. Certification of less critical systems should then be subsequently undertaken. Where large agencies have multiple critical systems a business impact analysis would allow management to determine the effect each system would have on an agency if it failed. For small agencies that usually only have one or two critical systems (one being the finance or human resource system), usually these systems are outsourced to security compliant central agencies or processing bureaux thus, allowing the larger central agency (or organisation) to incorporate the smaller systems into their security certification strategy an this improves IS security for both the central and small agencies.

This study has recognised the differences across agencies rather than assuming that security compliance within e-government would be the same for small, medium and large agencies. This study highlights the deficiency of having a single viewpoint for an e-government study of this type.

Further analysis might compare data such as this, across various government portfolios as well as across and between different organisation sectors. This study may also be highly relevant to other national governments or multi-organisational corporations.

## References

Altrichter, H (1990) "Do We Need an Alternative Methodology for Doing Alternative Research?", Zuber-Skerritt (Ed.) "Action Research for Change and Development", Brisbane: Centre for the Advancement of Learning and Teaching (CALT) Routledge, London (UK).

Australian Bureau of Statistics (2004) "Schools, Australia, 2005" http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4221.02005?OpenDocument (Accessed 2-11-2004)

Bindview., (2004) "Implementing ISO17799: A Practical Guide", *whitepaper*, 1256WP0009 04.04 Sunnyvale, CA

Spinellis ; S. Kokolakis ; S. Gritzalis., (1999) "Security requirements, risks and recommendations for small enterprise and home-office environments", *Information Management & Computer Security* 1999, Bradford.

Carter, L., and Belanger, F., "The Influence of Perceived Characteristics of Innovating on e-Government Adoption", *Virginia Polytechnic Institute & State University*, Blacksburg, USA http://www.ejeg.com/volume-2/volume2-issue-1/v2-i1-art2.htm (Accessed 12-9-2002)

Cohen, L., Manion, L., (1989) "Research Methods in Education", (3rd ed.) London: Routledge.

Cushing, J., Pardo, .T, (2005) "Research in the Digital Government Realm", *IEEE – Innovative Technology for Computer Professionals – Computer*, December 2005

Dick, B., (2002) "What is Action Research",

http://www.scu.edu.au/schools/gcm/ar/whatisar.html. (Accessed 25-8-2003)

eCommStrategiesInc., (2000) "Focus on B2B Expectations: B2B Web Site Earning to grow 500 Percent by 2002", eComm Strategies Inc http://www.ecommstrategies.com/insights/knowledge/2000-11/expectations_of_B2B.html. (Accessed 15-6-2001)

Farbery, B., Land, F., Targett, D., (1999) "Reflections on a Qualitative Study", (on-line), Available at http://www.is.lse.ac.uk/wp/pdf/WP84.pdf. (Accessed 25-4-2004)

Fingar, P., (1998) "A CEO's Guide to eCommerce Using Intergalactic Object-Oriented Intelligent Agents", July 1998. http://home1.get.net/pfingar/eba.htm. (Accessed 17-12-2002)

Frank, D., (2003) "Policy would secure users, transactions", *Federal Computer Week*, Falls Church, Jan 27, (17:2), 2003, p. 10. (Accessed 25-4-2004)

Heeks, R., (2003) "eGovernment for Development Basic Definitions Page", IDPM, University of Manchester, UK, 2002, http://www.egov4dev.org/egovdefn.

Hof, S., (2002) "Security Concepts and Requirements of e-Government Sites and other Public Electronic Processes", http://falcon.ifs.uni-linz.ac.at/research/phd_hof/ .(Accessed 25-3-2003)

Kiel, A., (2003) "Paper and pixels", *Document Processing Technology*, Madison, Feb 2003, Vol. 11, Iss. 1, pg2.

Martin, N (2005) "Protecting Government Information Post 9/11: An Evolving Role for Security Architectures", *(ACIS) 16th Australasian Conference on Information Systems Protecting Government Information*, 29 Nov – 2 Dec 2005, Sydney.

Mitrou, L. and Karyda, M., (2005) "Employees' privacy vs. employers' security: Can they be balanced?", *Telematics and Informatics*, In Press, Corrected Proof, (Accessed 6-10-2005).

NZ Local Government FAQ (2004) "Full-time Equivalent Staff Employed by Local Authorities", http://www.lgnz.co.nz/faq/staff.html (Accessed 18-10-2004)

OECD, (2003) "The e-government imperative: main findings" http://www.oecd.org/dataoecd/60/60/2502539.pdf. (Accessed 15-4-2004).

OICT, (2004) "Office of Information and Communications Technology, 'Benefits Realisation Register Guideline'", http://www.oict.nsw.gov.au/guidelines/4.3.3.b-benefits.asp. (Accessed 15-5-2004)

Pivk, A., Gams, M., (2000) "Intelligent Agents in E-commerce", *Elektrotehniški vestnik Electrotechnical Review*, Ljubljana, Slovenija http:// ai.ijs.si/Sandi/publications/IAinEC.pdf

Scott, J (2002) "PricewaterhouseCoopers – Risk management survey" inhouse NSW Government Report.

Standards, Australia (1999), AS/NZS 4444.1:1999 "Information Security Management", Standards Australia, 1999.

Standards, Australia (2000), AS/NZS 4444.2:2000 "Information Security Management", Standards Australia, 2000.

Standards, Australia (2001), AS/NZS ISO/EC 17799:2001 "Information Technology – Code of Practice for Information Security Management", Standards Australia, 2001.

Standards, Australia (2001), AS/NZS ISO/EC 17799:2001/Amdt 1-2004 "Information Technology – Code of Practice for Information Security Management", Standards Australia, 2004.

Standards, Australia (2000), AS/NZS7799.2:2000 Information Security Management -- Part 2: Specification for Information Security Management Systems", Standards Australia, 2000.

Standards, Australia (2003), AS/NZS7799.2:2003 Information Security Management -- Part 2: Specification for Information Security Management Systems", Standards Australia, 2003.

Standards, Australia (1999), AS/NZS4360:1999 "Risk Management", Standards Australia, 1999.

Standards, Australia (2004), AS/NZS4360:2004 "Risk Management", Standards Australia, 2004.

The Audit Office of New South Wales, (2002) "Performance audit report: e-government: use of the Internet and related technologies to improve public sector performance", http://www.audit.nsw.gov.au. (Accessed 23-8-2004)

WA Government, 2003 "Definition of e-Government", http://www.egov.dpc.wa.gov.au/index.cfm?fuseaction=guidelines.security". (Accessed 25-4-2004)

WA Government (2004) "Employment in WA State Government Bodies", http://www.wagiv.wa.gov.au/documents/emp_200506.pdf (Accessed 25-3-2003)

Whitman, M.E., (2004) "In defense of the realm: understanding the threats to information security", *International Journal of Information Management*, (24:1), pp. 43-57.

Wood, M., (2001) "Overview of Biometric Encryption", http://www.sans.org/rr/paper.php?id=1144. (Accessed 23-1-2002)