December 2003

Compliance with an Information Security Management Standard: A New Approach

Malcolm Pattinson
University of South Australia

COMPLIANCE WITH AN INFORMATION SECURITY MANAGEMENT STANDARD: A NEW APPROACH

Malcolm R. Pattinson
School of Accounting & Information Systems
University of South Australia
m.pattinson@unisa.edu.au

Abstract

The principal aim of this paper is to examine an innovative approach to determine the extent that an organisation complies with a generally-accepted information security management standard. This new approach is modelled on the Goal Attainment Scaling (GAS) methodology and is combined with a set of baseline security controls extracted from the International Standard AS/NZS ISO/IEC 17799: 2001. This new approach requires that a tailor-made measurement device is developed and then used to conduct multiple assessments of the state and condition of information system (IS) security controls within the same organisation. Metrics are generated for the various security areas, which provide an indication of the degree of compliance with the standard. The paper reports on the application of this approach within an agency of a South Australian (SA) government department.

Keywords: Information System (IS); Information Technology (IT); Information Security Management; Goal Attainment Scaling (GAS); AS/NZS ISO/IEC 17799: 2001 (AS/NZS 17799)

Introduction

The need for adequate information system security has never been greater. Factors that have contributed to this need include:

- the increased use of, and dependence on, the internet for commercial transactions within public and private sectors
- the realisation by IS managers, CIOs and Boards of Directors that they have a duty of care responsibility and are accountable for their actions
- the emergence and increased use of new technologies such as wireless, bluetooth and mobile commerce
- the expectation by customers and trading partners that the security status of an organisation's information systems are satisfactory.

This increased need has triggered the realisation of IS managers and CIOs that the security of their information systems is maintained at a satisfactory level and that this level is able to be communicated to various stakeholders. This implies that management need a generally-accepted benchmark against which they can measure the status of their organisation's IS security.

Such benchmarks, in the form of IS security standards, have emerged in the last 10 years. The most prominent of these being the British Standard BS7799 (BSI, 1999), which was first developed in 1995. Other significant information security standards include BSI, COBIT, GASSP, GMITS, ISF, NIST and the AS/NZS ISO/IEC 17799: 2001 (Standards Australia/Standards New Zealand, 2001) (hereafter referred to as AS/NZS 17799).

Armed with these standards, how do managers use such standards to measure the level of IS security within their organisations? How do they measure the adequacy of their IS controls? How do they establish whether or not they are compliant with a mandated standard? What is needed is a means of generating a metric to indicate the state of IS security within organisations and the degree of compliance with an internationally accepted standard.

The research outlined in this paper investigates an approach which will enable management to measure the adequacy of their IS controls and to compare these findings with a recognised standard. The principal aim of this paper is to examine the appropriateness of a goal attainment scaling (GAS) methodology to assess and quantify the state and condition of IS controls for the purpose of determining the degree of compliance that an organisation has with the International Standard AS/NZS 17799.

The remainder of the paper is consists of:

- A discussion of why the research is considered worthwhile and how it contributes to the field of study.
- An overview of the structure and content of the AS/NZS 17799 standard followed by an explanation of the GAS methodology.
- A brief description of how the GAS-based methodology was used in a South Australian government agency and a discussion of the major issues and findings, followed by a summary.

Justification for Research

A number of authors have reported that there is a need for management to continuously assess the state of IS security within their organisations. For example, Kisin, (1996), claims that if continuous measurement, in accordance with policies or standards, is not done, employees and end-users will become blasé. Similarly, Eloff and von Solms, (2000) emphasise the need for line managers to continually confirm their compliance with their own security policies and also with mandated codes of best practice.

Continuous measurement of this nature achieves a number of benefits. For instance, it communicates to employees that management are serious and that the information security policy is actually being enforced. Also, it ensures that controls are updated as new technology is introduced to the organisation.

The need for management to know the level of their IS security and the extent of compliance with mandated policies and standards has increased in recent years because:

- Subsidiaries of large organisations need to be sure they are compliant with such standards
- Governments are made up of separate operating entities and it would be useful to compare security levels
- Managers may need some form of confirmation that their trading partners are adequately secured
- Shareholders may demand a particular level of compliance with standards
- Directors have a 'duty of care' responsibility to comply with standards

The above points indicate that there is a need for a simple and inexpensive self-assessment methodology that will enable management to assess the level of IS security and the extent of compliance with an adopted standard. This paper investigates such an approach used in conjunction with the following International Standard.

The AS/NZS ISO/IEC 17799:2001 (AS/NZS 17799)

This Standard, titled *Information technology - Code of practice for information security management* was developed in 2001 by a joint technical committee made up of members from various Australian and New Zealand organisations and published in June 2001. Although it supersedes the Standard, AS/NZS 4444.1:1999, *Information Security Management, Part 1: Code of practice for information security management*, only small editorial changes were made. It is identical to the international Standard ISO/IEC 17799:2000, *Information technology – Code of practice for information security management.* All of these standards are based on Part 1 of the United Kingdom's Department of Trade & Industry's Standard BS7799, which was first published as a British Standard in 1995. (Ccure, 1999).

It is stated in the preface of the AS/NZS 17799, that the objective of the document is to provide management with a basis for developing their own organisational information security framework. Essentially it provides a set of baseline security controls covering the complete spectrum of IS security. It is written in such a way as to be technology independent and therefore has the potential to provide benefits to all types of organisations operating on various hardware & software platforms. However, compliance with this Standard does not imply that an organisation is internationally certified.

The Standard comprises ten categories of information security management divided into 36 sub-categories. These are further itemised into 127 controls. Figure 1 below is an extract of this Standard showing all ten categories of information security management and an expanded view of the sub-category *Physical and Environmental Security*.

3. SECURITY POLICY
4. ORGANIZATIONAL SECURITY
5. ASSET CLASSIFICATION AND CONTROL
6. PERSONNEL SECURITY
7. PHYSICAL AND ENVIRONMENTAL SECURITY
7.1 SECURE AREAS
7.1.1 Physical security perimeter
7.1.2 Physical entry controls
7.1.3 Securing offices, rooms and facilities
7.1.4 Working in secure areas
7.1.5 Isolated delivery and loading areas
7.2 EQUIPMENT SECURITY
7.2.1 Equipment siting and protection
7.2.2 Power supplies
7.2.3 Cabling security
7.2.4 Equipment maintenance
7.2.5 Security of equipment off-premises
7.2.6 Secure disposal or re-use of equipment
7.3 GENERAL CONTROLS
7.3.1 Clear desk and clear screen policy
7.3.2 Removal of property
8. COMMUNICATIONS AND OPERATIONS MANAGEMENT
9. ACCESS CONTROL
10. SYSTEMS DEVELOPMENT AND MAINTENANCE
11. BUSINESS CONTINUITY MANAGEMENT
12. COMPLIANCE

Figure 1. Extract of AS/NZS ISO/IEC 17799:2001

This standard is one of a number of internationally accepted standards that is suitable as a basis for certification of an organisation's IS security. There are a few reputable certification schemes that provide management with assurance that they comply with best practices. Two such schemes, C:Cure and ISIZA offer AS/NZS 17799 (in fact BS 7799) accreditation. With this background and demonstrated level of acceptance, the AS/NZS 17799 is the obvious choice of standard to be incorporated into a potential measurement device. Notwithstanding this point, the proposed methodology in this current research could have used any standard, although some are more suitable than others because of the way they are structured and written.

The Goal Attainment Scaling (Gas) Methodology

GAS is a program evaluation methodology used to evaluate the effectiveness of a program or intervention. It attempts to measure how well a particular program is achieving or has achieved its objectives. Kiresuk and Lund (1982) state that program evaluation is a process of establishing "...the degree to which an organisation is doing what it is supposed to do and achieving what it is supposed to achieve." (p. 227). The GAS approach to program evaluation originally concentrated on the implementation and administration of social programs, in particular, mental health programs. More recently, it has been successfully adopted in other human service delivery programs as diverse as education, rehabilitation, medicine, corrections, nursing, chaplain training, social work, chemical dependency, and program administration (Kiresuk et al, 1994). In the implementation and evaluation of programs involving human endeavour, managers are concerned about the effectiveness of departments or projects in achieving the objective(s). The use of the GAS methodology for this purpose can aid in organising and focusing methods, communicating the objectives of the system, and facilitating the help of others in reaching those objectives. At the same time it provides management

with a measurement tool that will provide simple answers to the questions 'how close to the objective(s) are we?' and/or 'what improvement have we made?'

In regard to the evaluation of IS security, the GAS methodology provides more information than simply establishing whether or not a control has been implemented. It purports to establish the extent to which a control has been implemented. Typical compliance testing methods may in fact be extended by the assignment of either a score or a few words for each reference point on a scale. Scales of this type are commonly referred to as Likert scales and may have points labelled zero to five or brief descriptions such as 'not implemented', 'minimal implementation', 'half implemented', 'almost fully implemented' and 'fully implemented'. The GAS method takes these descriptions a step further by having a few sentences for each reference point as shown in Figure 2 below. This feature of GAS reduces subjectivity substantially because the evaluator is able to compare the actual situation with each of the described situations and select the description of 'best fit'. However, the main advantage that GAS has over the typical Likert scales is the fact that stakeholders are involved in developing comprehensive descriptions for each GAS level. This not only provides more information to evaluators than do typical Likert scales, but this 'transparency' could reduce confusion and promotes more accurate self-assessment.

One of the essential components of the GAS methodology is the evaluation instrument. This is primarily a table or matrix whereby the columns represent goals to be assessed and the rows represent levels of attainment of those goals. More specifically, the rows represent five contiguous descriptions of the different levels of 'attainment' of each goal ranging from the best-case scenario at the top to the worst-case scenario at the bottom. When applied to the evaluation of IS security, the goals become IS controls with levels of attainment as shown in Figure 2 below.

7.1 SECURE AREAS
Objective: To prevent unauthorised access, damage and interference to business premises and information.

LEVEL OF ATTAINMENT OF IS CONTROL	7.1.1 Physical Security Perimeter	7.1.2 Physical Entry Controls	7.1.3 Securing Offices, Rooms & Facilities	7.1.4 Working in Secure Areas	7.1.5 Isolated Delivery & Loading Areas
Much more than Acceptable level + 2	All IT facilities are housed in a physically sound building and all doors and windows are lockable. Reception areas are manned. All fire doors are alarmed and slam shut.	Physical access to areas where there are IT facilities require users to authenticate themselves using a swipe card. Users wear ID badge and visitors are recorded and always accompanied. Access rights are reviewed regularly.	All IT equipment is locked down. All doors & windows locked when unattended. All offices and cabinets are lockable.	All third party people are authorised and supervised and always accompanied. Access is monitored continuously.	Delivery & loading areas are isolated from IT areas. Holding area for goods is secure and requires authentication prior to entry. Incoming material is inspected & registered
Somewhat more than Acceptable level + 1	All IT facilities are housed in a physically sound building and all doors and windows are lockable. Reception areas are manned.	Physical access to areas where there are IT facilities require users to authenticate themselves using a swipe card. Users wear ID badge and visitors are recorded.	All IT equipment is locked down. Most doors & windows locked when unattended. Most offices and cabinets are lockable.	All third party people are authorised and supervised. Access is monitored in ad hoc manner.	Delivery & loading areas are isolated from IT areas. Holding area for goods is restricted.
Acceptable level 0	All IT facilities are housed in a physically sound building and all doors and windows are lockable.	Physical access to areas where there are IT facilities require users to authenticate themselves using a swipe card.	Most IT equipment is locked down. Generally, doors & windows locked when unattended. Most offices and cabinets are lockable.	All third party people are authorised and supervised.	Delivery & loading areas are isolated from IT areas.
Somewhat less than Acceptable level - 1	Most IT facilities are housed in a physically sound building and most doors and windows are lockable.	Physical access to areas where there are IT facilities require users to key in a code.	Approx. half of IT equipment is locked down. Half of the time doors & windows locked when unattended. Approx. half of offices and cabinets are lockable.	Some third party people are authorised and supervised.	Sometimes goods are delivered to IT areas. Goods are recorded and delivery personnel are supervised or monitored.
Much less than Acceptable level - 2	Very few IT facilities are housed in a physically sound building and most doors and windows are lockable.	Physical access to areas where there are IT facilities is unrestricted.	Very little IT equipment is locked down. Rarely are doors & windows locked when unattended. Very few offices and cabinets are lockable.	Very few third party people are authorised and supervised.	Sometimes goods are delivered to IT areas without being recorded or delivery personnel have unrestricted access to IT areas.

Figure 2. GAS Follow-up Guide for 'Secure Areas'
(Adapted from the GAS methodology (Kiresuk *et al*, 1994))

This current research uses a methodology based on the GAS methodology. There were changes made to the original GAS evaluation tool to accommodate the nature of IS security and to make the instrument more user-friendly.

Application Of The Gas-Based Methodology

Objectives

This research project had two objectives – one management the other research. The management objective was to evaluate the existing IS controls and to report the extent of compliance with the AS/NZS 17799. The research objective was to investigate the appropriateness of the GAS-based methodology in assessing the state and condition of IS controls for the purposes of determining the extent of compliance with the AS/NZS 17799.

The Case Study Organisation

The case study organisation is an agency of the Department of Human Services (DHS) within the South Australian government. The DHS employs 23,000 staff and is responsible for the policy administration and operation of public health, hospitals, family and community services, disability services, ageing and housing. The case study agency is one of many under the umbrella of public health and consists of a central hospital, two large suburban clinics, a warehouse and approximately 100 small clinics across the state of South Australia. It employs approximately 800 staff. The case study agency's information systems consist of multiple servers and networks which are predominantly Windows NT operations running office applications, an engineering maintenance system and various patient management systems. These systems are internally supported by a small contingent of IT staff and by the outsource organisation, EDS.

The Research Design

The research design consisted of three phases. In the first phase, the GAS-based instrument was developed for the complete spectrum of information security management. In the second phase, this instrument was used to conduct the assessment and in the third phase, the results were calculated, analysed and reported to management.

Phase 1: Develop the GAS-Based instrument

The GAS evaluation instrument developed in this phase of the study represented all aspects of IS security for an organisation. Consequently, the instrument needed to comprise multiple follow-up guides which spanned the whole spectrum of IS security. The number of follow-up guides depends on how the participants wish to group the 36 sub-categories of IS security. They could simply adopt the 10 categories as per the standard or they could specify their own groups, as in this study. The resulting GAS evaluation instrument, comprised 16 follow-up guides, each of which was developed in accordance with the Kiresuk *et al* (1994, pp. 7-9) nine-step process as described below.

> Step 1: *Identify the security areas to be focused on*
> For the purpose of this research, the areas to be focused on included all aspects of IS security within an organisation. The Standard AS/NZS 17799 was used to select 16 areas (hereinafter called groups) across the Standard's 10 IS security categories, 36 sub-categories and 127 controls.
>
> *Step 2: Translate the selected security areas into several controls*
> The individual IS security aspects or categories identified in the previous step will each warrant a separate GAS follow-up guide for which at least three objectives should be identified. In the context of IS security, these objectives can be operational objectives or outcome objectives, depending on how IS security is to be evaluated. Operational objectives translate into IS controls. The selection of a set of IS controls which address the area being evaluated is an extremely critical task in the methodology in terms of the validity of the results. Selected controls must be those considered most important and should be broad in nature such that a set of controls is representative of all possible controls which pertain to the particular area being evaluated.

Step 3: Choose a brief title for each control
An abbreviated title was developed for each IS control selected in the previous step so that the eventual user of the GAS follow-up guides would easily recognise the control being evaluated.

Step 4: Select an indicator for each control
This step relates to the criteria used to measure an IS control. The indicator is an element of measurement chosen to indicate the level of attainment of the IS control.

Step 5: Specify the minimal acceptable level of attainment for each control
This step required the development of narrative for the 'zero' or middle cell for each control within each follow-up guide. This description represents the minimum level of acceptance of an IS control.

Step 6: Review the acceptable levels of attainment
The objective of this step is to confirm the relevance and understandability of the descriptions by potential users. It is also important that these descriptions represented minimal acceptable levels of attainment of IS controls.

Step 7: Specify the 'somewhat more' and 'somewhat less' than acceptable levels of attainment
This step required that narrative be developed which described the 'somewhat more' and 'somewhat less' than the minimum level of acceptance scenarios for each IS control.

Step 8: Specify the 'much more' and 'much less' than acceptable levels of attainment
This step required that narrative be developed, as in Step 7, but which described the 'much more' and 'much less' than the minimum level of acceptance scenarios for each IS control.

Step 9: Repeat these scaling steps for each of the controls in each follow-up guide
This step is simply a repeat of Steps 1 to 8 above.

Additional Step: Assign Control Weightings
This Step is not an essential step because T-scores can be generated whether controls are weighted or are of equal weight (i.e. non-weighted). For this project, it was decided to assign a weight between 1 and 5 to each of the 127 controls whereby 1 is 'not important' and 5 is 'extremely important'. All controls are obviously important but relative to each other, some controls are more important than others. This 'importance weight' was based on the perceived criticality of the control in question. A control was considered critical, and therefore important, if it was perceived to help minimise the frequency of occurrence of threats that were considered most damaging to the organisation.

Phase 2: Use Instrument to Conduct Assessment

This phase of the research project required the selected evaluators to fill-in each of the follow-up guides by placing a tick in one of the 5 cells of each column of each follow-up guide. The ticked cell within each column should be the one with a descriptive narrative that best matches the actual situation within the organisation. This was completed for each of the 127 controls in the evaluation instrument.

In comparison to the first phase of this project where the instrument was developed, this phase was relatively quick and easy. Timings were conducted on various evaluators with no prior experience or training and in all cases a single A4 sheet of 5 columns (i.e. controls) took less than 3 minutes for evaluators to read, and then to tick the most suitable cell.

Phase 3: Analysis of Results and Report to Management

On completion of the multiple evaluations, each set consisted of 127 scores, one for each control, with values of -2, -1, 0, +1 or +2 as per the GAS methodology. These raw scores were then converted into two T-scores for each of the 16 follow-up guides, one that used control weights and one that did not (refer Figure 3 below).

It should be noted that the raw scores for each of the follow-up guides could have been converted to a summary T-score in a number of ways with equally relevant results. For example one could have summed the scores or taken the average of the scores

and then applied some form of linear transformation to normalise each matrix. This project adopted the GAS calculation for T-scores as the form of linear transformation because it has been widely used, albeit in the health discipline (Kiresuk *et al*, 1994).

A GAS T-score is a linear transformation of the average of the raw scores in each follow-up guide using the formula documented by Kiresuk *et al* (1994) and presented below:

$$T - score = 50 + \frac{10\sum w_i x_i}{\sqrt{(1-p)\sum w_i^{\,2} + p(\sum w_i)^2}}$$

where x_i is the outcome score for the ith scale with a weight of w_i, and p is the weighted average inter-correlation of the scale scores and commonly set at 0.3. Scores on the individual scales between -2 and +2 each are assumed to have a theoretical distribution with a mean of zero and a standard deviation of 1. This formula then produces T-scores with a mean of 50 and a standard deviation of 10 when each scaled control is scored using the -2 to +2 scale.

Figure 3 below shows a comparison of the generated T-scores for both non-weighted and weighted calculations for each of the 16 information security groups.

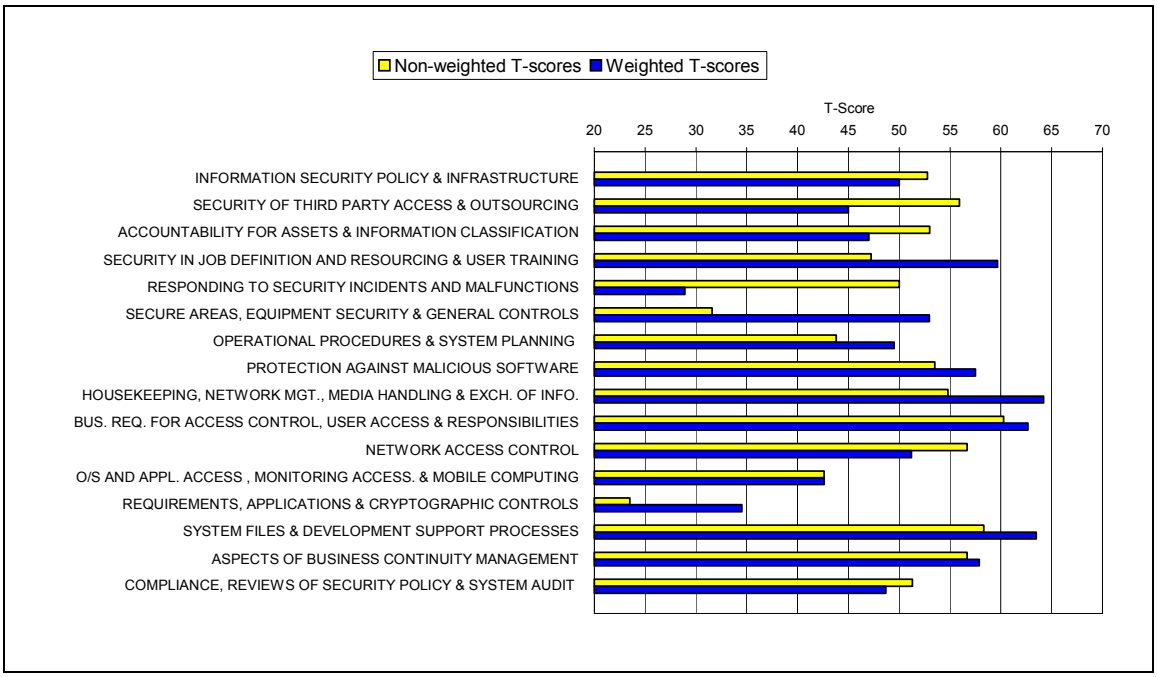

Figure 3. T-Scores for the Information Security Groups

A T-score of 50 or more for a particular information security group indicates that, on average, the controls specified within are considered acceptable. Assuming that these controls are representative of all controls specified for this set of security areas within the International Standard AS/NZS 17799 then it is probable that the controls in place for this information security group are generally compliant with the Standard. The extent of compliance is reflected in the amount that the score is greater than 50.

A T-score of less than 50 for a particular information security group indicates that, in general, the controls in place are not acceptable and therefore are not totally compliant with the Standard. To find out exactly which controls were considered less than acceptable, refer back to the follow-up guides for the particular information security group to see which individual controls were marked as 'somewhat less' or 'much less' than acceptable (i.e. with a score of -1 or -2).

In Figure 3 above, using the weighted T-scores (shown in dark shade), at least 6 of the 16 IS security groups are below the acceptable score of 50. The worst group appears to be "Responding to Security Incidents and Malfunctions" with a score of

approximately 29. In terms of the extent of compliance with the AS/NZS 17799, all 16 information security groups must achieve a T-score of 50 or more to achieve basic compliance. If basic compliance is achieved, then an aggregate T-score across all information security groups will be calculated. This single number could be used to indicate the extent of compliance with the standard.

Research Issues

Development of a Tailor-Made Measuring Instrument

The proposed methodology requires that the GAS-based measuring instrument be developed specifically for each organisation. This task proved to be quite difficult and time consuming, particularly the scaling of IS controls into five levels of acceptability ranging from best-case scenarios to worst-case scenarios. The skill, expertise, time and effort required to develop a GAS-based instrument unique to each organisation suggests that either a GAS expert be used or training is conducted.

The Need for Training

It became evident during this research project that training of potential GAS goal setters is a critical component of the GAS methodology if a meaningful result is to be achieved. The GAS methodology is reported to have been used in hundreds of organisations and for many different purposes (Kiresuk et al, 1994). From these, Kiresuk *et al* (1994) have concluded, "Effective training must be provided to staff who will be employing the technique, time must be allowed for the staff to use the technique properly, and administrative support must be available to sustain the implementation." (p. 6). In fact, proper training is considered such an important issue that Kiresuk et al (1994) devoted a whole chapter to topics such as curriculum design, skills to be developed, GAS goal setting, GAS goal scoring and the costs of training.

Evaluating A Non-Human Service

An important question is whether the same arguments for GAS's success in evaluating human service programs can be extended to a study where the program being evaluated is a management 'program' (or plan) where the subjects are not individuals but procedures or activities. In the evaluation of a health or education program, the GAS methodology measures the outcomes of a program by assessing the impact that the program has on individuals, that is, the 'condition' of the individuals. In contrast, this research uses a GAS-based methodology to measure the process of implementing and maintaining a set of IS controls, by assessing the state of these controls. The most significant difference between an evaluation of a human service compared to a non-human service appears to be that the recipient of human service may also be involved in the goal setting process. In the case of a non-human service, this does not happen because the recipient is the organisation, not a human being. However, stakeholders or representatives of the organisation should be involved in the goal setting process. Notwithstanding the limited number of non-human service test cases in which GAS has been applied, the author believes that the methodology warrants further investigation in these situations to ascertain its usefulness and relevance. At this stage it would be incorrect to assume that the success of GAS in the evaluation of human service delivery programs automatically applies to non-human service programs.

The Design & Content of the AS/NZS 17799

The AS/NZS 17799 was not designed as a document that enabled line managers to easily determine their level of compliance. It does not provide management with guidelines of how to assess IS controls and to then establish whether or not they are compliant with the standard. This point is clearly stated in the document introduction. Its purpose is to provide management with a set of baseline IS controls from which they can develop a 'framework' document in accordance with their IS policy document and their unique risk objectives. The content and structure of this IS security framework document will determine whether it can be used to easily conduct a compliance audit. In the case of the organisation in this research project, the framework document was not in appropriate form and hence the reason why a compliance audit was not conducted. It should be noted that in February 2003, part 2 of the AS/NZS 17799 was published. This document is identical to BS 7799.2:2002 (BSI, 1999) and is meant to explain how to apply the code of practice described in part 1 of the AS/NZS 17799. However, it does not generate a metric that can be used for certification purposes.

Not an Audit

It is important to appreciate that the methodology applied within the case study organisation was NOT an audit of the organisation's IS controls. That is, the actual application of the methodology did not use independent persons to test and observe IS controls in order for them to ascertain their state or condition. In fact, internal people were used to conduct individual assessments based on their knowledge and perception of the state of each IS control. However, there is no reason why the same assessment device could not be used by an independent IS auditor during the course of testing and observation.

Summary

This paper proposes a new approach for IS managers and internal auditors to establish the extent to which their organisation complies with the international standard AS/NZS 17799. This approach incorporates a set of baseline IS controls, extracted from the standard, with a GAS-based evaluation methodology. A research project, conducted within a case study organisation, examined the merit of this approach and demonstrated that the proposed methodology has considerable merit in determining the level of compliance with the AS/NZS 17799. The major reasons for reaching this conclusion are:

- Once the measurement device is developed, an assessment can be conducted quickly and easily.
- The use of relevant employees to develop the measurement instrument increased awareness of the issues and encouraged better communication.
- Although the instrument is developed as a tailor-made device in accordance with the organisation's IT infrastructure and IS risk objectives, it is based on the IS controls contained in the AS/NZS 17799. This 'common denominator' provides the opportunity to compare the results of different organisations. The author aims to conduct further research in this area in an attempt to establish the validity of comparing results.
- The methodology provides management with a set of numbers, which indicate the areas of security that are most in need of action.
- There are a number of positive characteristics of the original GAS methodology that are inherent in the hybrid approach that is proposed in this paper. Firstly, the instrument provides a system of scoring each control, much like a Likert scale, and these scores are aggregated and averaged using a linear transformation formula to generate a rating for a particular group of IS security being assessed. These metrics, when combined with the AS/NZS 17799, have the potential to become the basis of a certification scheme. The author is also conducting research in this area.

References

British Standards Institute (BSI), (1999), BS7799, *Code of Practice for Information Security Management*.

Ccure, (1999), **http://www.c-cure.org/7799history.htm**, Copyright BSI-DISC 1998-2002 (accessed on 07/03/2003)

Eloff, M. M. & von Solms, S. H., (2000), "Information Security Management: An Approach to Combine Process Certification And Product Evaluation", *Computers & Security*, Vol. 19, No. 8, pp. 698-709.

Kiresuk, T. J. & Lund S. H., (1982), "Goal Attainment Scaling: A Medical-Correctional Application", *Medicine and Law*, Vol. 1, pp. 227-251.

Kiresuk, T. J., Smith, A., & Cardillo, J. E., (Eds), (1994), *Goal Attainment Scaling: Applications, Theory and Measurement*, Erlbaum Inc, N.J., U.S.A.

Kisin, R., (1996), "IT Security – Implementing 'best practices'", *Computer Audit Update*, January, Elsevier Science Ltd.

Standards Australia/Standards New Zealand, (2001), AS/NZS ISO/IEC 17799:2001, *Information Technology - Code of practice for information security management*.