The Role of Auditing in Promoting Security Awareness and Best Practice

2 November 1995

Pat Barrett
Auditor-General for Australia
INTRODUCTORY REMARKS

The focus of my address today will be on how auditors, particularly external auditors such as the Australian National Audit Office, can play an effective role in enhancing the security regime in agencies to improve the overall performance of public administration. My comments will be in the following four contexts:

- the vast amount of information held by public sector agencies which is extremely varied in nature and confidentiality status, and, as such, represents an extremely valuable public asset for which we are all accountable, within a changing public management environment;

- the role of auditing and other review activities and their contribution to the overall accountability (results) framework;

- ANAO's experience and developments in auditing matters of information security and related topics; and

- a brief look at how the ANAO is addressing its responsibilities to protect its own information base.

The Australian Society of Certified Practising Accountants (ASCPA) Audit Centre of Excellence has noted that:

*Security, a prime function of management, is as important as the other core functions of operations and finance.* Information Technology Risks and Responses - A Brief Guide for Practitioners and Management

Audit Centre of Excellence, ASCPA. Melbourne, 1995 (page 9)

The Centre went on to assert that it is the responsibility of management to encourage all staff to participate in, and accept, the overall concept of system security and to ensure that an appropriate education program is developed and conducted throughout the organisation so that the significance of security is understood. In short, it is difficult to disagree with the Centre that security must be driven by management and that security is a state of mind. In the latter context, staff have to be educated about security requirements and best practice.

I consider that auditing can make a useful contribution to greater awareness, and dissemination, of security principles, guidelines, systems and practices. In these ways it can aid the promotion of security standards. As well, it can assist agencies in fulfilling their accountability requirements in these regards.
In discussing the issue of security, it is important for all of us to recognise that security is not an end in itself but is an important means of, inter alia, maintaining and possibly enhancing the performance of the asset base of the Australian Public Sector. While much emphasis is quite correctly placed on the imperative to safeguard the security of physical assets owned by the Commonwealth, the vast array of information held by Australian Public Service (APS) agencies, and related systems, are arguably of even greater importance to overall performance. As such, there is growing recognition of the need to ensure its protection, integrity and confidentiality are fully understood at all levels of our organisations as well as by the Parliament and the community at large. I particularly relate to the following observations by the then Western Australian Information Policy Committee in 1992:

Government acts as the trustee of the peoples information, so the ethics associated with such a role are applicable. Government must achieve a balance between protecting and safeguarding information on the one hand and providing information to achieve efficiency within government and to benefit the community and the economy on the other. Managing the Information Resource. Western Australian Information Policy Committee.

Government of Western Australia, Perth, 1992 (pages 27 and 28)

Statistics are available on the land, buildings, property and equipment which are under the control of the APS and which are most impressive, particularly in terms of national aggregates. What is less readily available are details of information which is held in a variety of mediums by every APS agency. However, it is becoming more generally recognised that information is our second most important asset after our people. Unfortunately, the value of our people has also only been belatedly recognised in the various public service reforms over the last twelve years. Real security depends importantly on their honesty, integrity and commitment as custodians of public resources.

Preservation of this important information base is the responsibility of each one of us. I have no doubt that the Parliament and the community will be continuing to seek assurances in various ways that we are maintaining its integrity and security, both in a physical and qualitative (including confidential) sense. As well, as public service managers, we have come to understand and value the extent to which information has become integral to our functions and our organisational performance. Attention has therefore increasingly been focused on the need to create an accessible but secure environment for our information in whatever form it takes.

But, like almost everything else today, security comes at a cost and long gone are the days where we might have considered the issue of security in isolation from other resourcing decisions. In other words, the challenge is not about maintaining security at any cost. Our responsibilities are to apply the concepts and principles of risk management to help ensure we have a security regime which is appropriate to the environment in which we operate, and a proper assessment of the various risks made
in the context of this environment. Any security regime must also, of course, be flexible enough to take account of the ever-changing public sector environment reflecting in large part the economic, social and other developments, as well as the changing values, in the wider community.

In particular, I contend that our consideration of security must be guided by the framework of public sector reforms which have been developed over the last twelve years, and which will continue to have a significant impact on the way the APS does its business in the future. Nowhere is this more evident than in the use of greater contracting out to the private sector in the provision of services not only to agencies but also to the general public. For example, we are now talking more about partnering arrangements and purchaser/provider splits. An important issue is just how far do the security and audit trails need to go. The Ombudsman recently warned of a no mans land of accountability which is developing between departments and contractors as more and more government services are privatised. This is an issue for all of us. The reform process is indeed ongoing in a changing public management environment.

Impact of the public sector reforms on our thinking about our resources and their security

As most of you would be well aware, the ongoing reform agenda in the APS includes:

· a focus on outcomes and therefore on customer/client satisfaction, constrained by the economic management imperative of doing more with less, in order to deliver a better performing public service;

· matching of authority with responsibility by devolving the authority for making management decisions to those actually charged with the responsibility for administering particular programs and services;

· development of a risk management approach with accountability for results as a management focus;

· alterations to the framework for financial resource management and reporting, including:
  - the requirement for accrual reporting for all Government agencies;
  - the move to more market type mechanisms;
  - changes to program performance statements in annual reports;
  - the presentation of the Commonwealth Budget in May;
  - the changes to the portfolio budget measures statement; and
  - the package of Bills introduced into the Parliament to replace the Audit Act 1901 (these
alterations to the framework for Human Resource Management, including greater staff management flexibility, equal employment opportunity and other Human Resource Management initiatives as well as workplace bargaining, performance appraisal and the increasing recognition of good performance and partial reward through performance pay. The drafting of a replacement of a new Public Service Act is also in progress which will reflect the changing culture and environment of public service to take us into the next millennium. Importantly, that drafting will be influenced by the enhanced public service values recently described by Dr Michael Keating, Secretary of the Department of the Prime Minister and Cabinet. Public Service Values, Dr Michael Keating, AO. Peter Wilenski Memorial Lectures 1995.

Canberra, 27 July 1995 (see particularly pages 6-10) These values are also set out in detail in the revision this year of the Guidelines on Official Conduct of Commonwealth Public Servants. Guidelines on Official Conduct of Commonwealth Public Servants, Public Service Commission.

AGPS, Canberra, March 1995 (page 2) The Guidelines are also very important in helping to form the necessary attitude or state of mind towards security issues, particularly in relation to ethical behaviour.

In making judgements about matters of security, as with any other important aspect of administration, we all need to take account of the directions set by the Management Advisory Board and its Management Improvement Advisory Committee - MAB/MIAC in the various publications such as Building a Better Public Service Building a Better Public Service, a joint MAB/MIAC publication, No. 12, 1993 and Ongoing Reform in the Australian Public Service Ongoing Reform in the Australian Public Service, An Occasional Report to the Prime Minister by MAB, No. 15, October 1994. I still like to think we are part of one public service even though we are now working in an environment of devolved authority.

A reasonable summary of the major themes identified in Building a Better Public Service is:

- making performance count: by looking closely at client needs and service quality, evaluating achievements, rewarding good performance at all levels, learning from and building on past performance, and being accountable;
- leadership: emphasising the key responsibilities of agency heads in managing for results, and clarifying the roles of central agencies and other mechanisms for sharing knowledge and experience; and
- strengthening the culture of continuous improvement: through better people management and development, and by embedding attitudes in the culture that unequivocally seeks to find better ways to achieve desired results.

These disciplines apply as much to public service managers consideration of security issues as they do to any other aspect of our management responsibilities. The imperative is to raise awareness, as this conference is doing today to change attitudes and even the culture of public service. It is my intention to ensure that the ANAO will contribute positively to that cultural and attitudinal change by more direct
involvement in the various initiatives and developments of the kind I have referred to as well as through its audit reports, both financial and performance.

Risk Management

Risk Management is an important, and one might say pervasive, element underlying many of the reforms which have taken place. A useful way of defining a risk management approach is that it is one which identifies all material areas of possible loss/error/opportunity, assesses the benefits and costs of the available options and enables informed judgements about the level and costs of risks involved in achieving cost effective outcomes. To many, it is a challenge to traditional public service thinking. This has been reinforced by Parliamentary concerns about accountability, although there has been growing support within the Parliament for the concept to be applied by public service management's within firm guidelines.

The ANAO is a strong supporter of the concept of risk management - after all managing risk is, or should be, an essential element of good management practice, particularly in today's climate of increasing financial constraint, greater competitiveness and contestability for both advice and services. However, we are also having to address a perception that auditors have inhibited the development of the concept by being unduly critical of initiatives taken and mistakes made. The Australian Public Service Reformed - An Evaluation of a Decade of Management Reform, Task Force on Management Improvement, AGPS Canberra December 1992 (page 101) As with the Parliament, our concern is to establish firm accountability guidelines for those taking such decisions. But, I stress, it is important to focus primarily on the outcomes we are seeking to achieve not just the methods used to do so.

The overriding aim of all the ANAO does is to improve public administration in the accountability framework through which its own performance will largely be judged. Managing risk efficiently and effectively reflects one concrete way in which this can be achieved. In this regard, the ANAO is interested to see whether agency management has assessed the organisational risks, included in this would be security risks, in a structured manner and planned accordingly. Costs/benefit analyses are an important part of managing risk. However, it is not cost-effective, nor appropriate, to cover every risk. As good managers, we should all look to continuously assess risks, assign priorities and probabilities and establish a controlled environment for managing those risks. Risk identification has become an important element of management's responsibilities.

The MAB/MIAC Exposure Draft on Managing Risk Managing Risk - Exposure Draft (Guidelines for Managing Risk in the Australian Public Service) MAB/MIAC Report No 17, AGPS Canberra, July 1995 is, in my view, a very timely publication which will help us all focus greater attention on the importance of risk management. As my colleague Ian McPhee recently said:
The publication is well written and illustrated, and strongly emphasises the need to manage risk; and in doing this to focus on two elements:

- the likelihood of something happening; and
- the consequences if it happens.

It also underlines the desirability of developing a mind set of being conscious that managing the risks in relation to every decision:

- it means you can’t assume everything will go right.  

Address by Ian McPhee, National Business Director, Australian National Audit Office, MAB/MIAC Seminar, Managing Risk, Canberra, October 1995

The Exposure Draft underlines a point I would like to stress in relation to security and that is the importance of the issue of documenting key elements of a risk management strategy. The Exposure Draft suggests that the answer to the question of when documentation is important is when it could count. It goes on to indicate the benefits of documenting the risk management strategy are to:

- help ensure the analysis is done;
- be available for review;
- facilitate communication to staff and others involved in the program so there is a shared understanding of directions and associated risks; and
- if ever required, it is available in defence of the program.

That is, documentation facilitates understanding and accountability.

I suggest that this approach is as relevant to security as it is in any other area of administration. This was borne out by the case study submitted by the Australian Security Intelligence Organisation (ASIO) in relation to Protective Security Risk Management. Op. cit., MAB/MIAC Report No 17 (pages 32 to 34) For example, ASIO has developed what they term a subject risk matrix methodology whereby an assessment made of all known potential sources of security risk in terms of the intention and capability, the threat they pose and the level of harm this could cause. This methodology allows a ranking in priority order of security concerns.

As we move more into paperless offices as a reality, there has been growing concern about how to handle electronic documentation. In this respect I commend to you the Guidelines for Improving Electronic Documents Management prepared by the Electronic Data Management Sub-Committee of the then Information Exchange Steering Committee (IESC). Improving Electronic Document Management - Guidelines for Australian Government Agencies.

Electronic Data Management Sub-Committee of the IESC. AGPS, Canberra, 1995
In response to an audit report on the results of the Departments 1994-95 financial statements, the Secretary of Transport recently informed me, inter alia, that he has commissioned a security risk review by ASIO. His expectation is that the review will provide the Department with a strategic focus for the Departments security arrangements. He noted that ASIO's approach aims to identify risk exposure, assess the level of that exposure and propose options for controlling risks at levels that are acceptable to the Department. This is part of a departmental review of security procedures. Other action is also in train which indicates the priority and importance attached to the review. I was particularly interested in two issues being addressed, one being system access by Information Technology (IT) staff and the other the installation of procedures to improve system recovery in the event of a major disaster. These initiatives are part of the Departments approach to risk management and reflect the need for risk assessment by management as a means to improve departmental performance. This is a tangible example of the principles involved in managing security and other risks for greater efficiency and effectiveness and a successful outcome from a co-operative effort.

Accrual Reporting

Another important element of the APS reform agenda which has had an impact on the management of the Commonwealth's asset base is the introduction of accrual reporting.

As most of you would be aware, the Commonwealth's financial reporting - at least in the core public sector - has traditionally been based on cash accounting principles with little or no requirement to account for assets and liabilities. That changed in 1988-89 when the Commonwealth introduced a system of modified accrual reporting for departments. This was the first step in the move to full accrual reporting which was achieved for 1994-95. This initiative represented a tangible recognition of the need to bring to account and report on the assets under the control of departments. Under the previous cash base system, while assets needed to be adequately controlled, there was no need for them to be valued and for this figure to be reported in the accounts of Government. Not surprisingly, many managers regarded their assets virtually as a free good. A policy of virtually self insurance by the Commonwealth largely reinforced this view. I say virtually because there was no necessary guarantee that the departments might not have been asked to look first at their own budgets to replace any losses. However, for the most part, the budget could be relied on to replace lost, damaged or destroyed assets. Perhaps more importantly, there has been a growing realisation, particularly in the information technology (computer) arena, of the possible enormous disruption to an agency's business from such occurrences where the likely impact goes well beyond just the budgetary cost.

Perhaps not surprisingly, therefore, one of the major problems encountered in the move to accrual reporting has been the identification and valuation of information. Arising out of this situation has been the recognition of the need to instil an attitude of mind, or put another way, a change in culture, which recognises information as a corporate asset, the integrity and security of which is the responsibility of all of us. I have been quite surprised over the years at the apparent relaxed attitude of many managers about protective security issues and disaster recovery (or, latterly, described as business resumption) arrangements. As I mentioned earlier,
information is a very valuable resource and its preservation and effective utilisation are essential if we are to achieve our performance targets or, even more basically, simply meet our functional (business) responsibilities.

THE CONTRIBUTION OF AUDITING AND OTHER REVIEW ACTIVITIES

The ANAO’s contribution to enhancing the security framework within the APS must be seen in the context of its statutory responsibilities.

The Audit Act and other Commonwealth Acts provide that the Auditor-General’s responsibility, in essence, is to:

- audit the financial statements of Commonwealth owned or controlled public sector entities, whether they be departments, statutory authorities or companies; with one or two exceptions, the financial statement audit mandate of the Auditor-General currently applies to all Commonwealth owned or controlled entities, whatever their legal form; and

- to conduct efficiency and project performance audits of public sector entities. It is currently Government policy that the Auditor-General can only undertake efficiency audits of Government Business Enterprises at the request of both Houses of Parliament, or if requested by the responsible Minister.

I would mention in passing that the legislation to replace the Audit Act refers to performance audits as a generic term rather than as efficiency or project performance audits. Performance audits have received increasing international recognition and acceptance. And, I might add, attract a great deal of debate.

The ANAO is therefore a very important element of public accountability. When it performs its functions, the ANAO brings to its task the benefits of independence and objectivity, professionalism and commitment, ethics and integrity, skills and experience and the knowledge of various best practices. I suggest to you that it is these attributes which make the external audit function a valuable contributor to the accountability process for issues such as security.

It is not my task today to canvass the roles of Attorney-Generals or its various portfolio agencies such as the Australian Federal Police and the Australian Security Intelligence Organisation (ASIO) or of Defence (for example, the Defence Signals Directorate), nor of other bodies such as the Ombudsman, Privacy Commissioner, Australian Archives and the Merit Protection and Review Agency (MPRA), which, inter alia, play important advisory and/or enforcement roles in the accountability framework. Nevertheless, it is ANAO’s responsibility to complement these organisations on, inter alia, security issues to ensure economy, efficiency and administrative effectiveness in the implementation of any relevant plans, guidelines or policies. Within agencies, internal audit and evaluation functions provide useful review mechanisms, similar to those of external audit, to assist managers in meeting their security control responsibilities. And it is these latter functions that I would like...
to stress as vehicles for providing performance assessments and assurance about security issues as well as identifying any deficiencies and action needed to overcome the latter. Importantly, these functions can also contribute to putting such issues in a proper and useful perspective for managers.

First internal audit. The ANAO has long been a very strong supporter of the need for viable and effective internal audit functions in the public sector. The ANAO strongly believes that internal audit is an integral element of the internal control structure within agencies. Management in both the public and private sectors is under increasing pressure to attest to robust and reliable internal control arrangements as well as being more accountable for corporate governance. Both internal and external audit have important roles to play in assisting management to meet its obligations in these areas.

Our overall aim is to establish a co-operative relationship with internal audit. In this way, we can build on rather than duplicate important work that internal audit does. Internal audit being an essential element of the workings of an agency has the benefit of working closely with agency management and being aware of the risks and the priorities of an organisation at any point in time. Internal audit therefore should be very well placed to contribute significantly to an agency's internal control structure, including its security environment. Internal audit can get in on the ground floor so to speak, and be an integral part of the development and maintenance of a security regime which best meets the business needs and imperatives of an agency. Internal audit should, in my view, be involved in a positive way, in the development of all major systems, helping to ensure that there are appropriate controls put in place from day one. This applies particularly to the prevention and detection of fraud and any subsequent court action. From its position of relative independence, internal audit can also periodically test the adequacy of security arrangements and assist management in system improvements where this is found to be necessary.

Second, program evaluation. The evaluation function is also an integral part of the accountability process, and has an increasingly important part to play in the overall APS environment.

Central to the focus on outcomes has been the introduction of program evaluation in the APS, reflecting the importance placed on the monitoring and reporting of performance information and overall program performance. Increasingly, benchmarking techniques are being used to both develop and assess such performance. From its across the Service perspective, the ANAO should be able to identify and report on best practice in this respect to leverage up the benefits derived by individual agencies to other government programs.

The importance of evaluations has been highlighted in the MAB/MIAC report No. 15 of October 1994 Ongoing Reform in the Australian Public Service, An Occasional Report to the Prime Minister by MAB, No. 15, October 1994. After noting a number of significant instances where external scrutiny has raised concerns about issues in the quality of administration in the APS, the report stated that internal evaluations undertaken across the service are also vital for managers in appreciating where and how improvements can be made. The report also noted that:
Working Nation, for example, relied heavily on findings from extensive evaluation activity in the employment, education and training portfolio; and

several other evaluations in recent years have had a significant impact on Government decision making.

The report also mentioned the Department of Finance view that portfolio evaluation plans had shown a marked increase in quality and strategic usefulness but noted also that more could be done to link evaluation activity to the improvement of APS advice to Government and to enhancing program outcomes to the benefit of the nation.

It would be interesting to know the extent to which evaluations undertaken up till now have included security aspects as part of their terms of reference. It is probably reasonable to speculate that very few in fact have done this.

**ANAO’S APPROACH TO, AND ISSUES ARISING FROM, REVIEWS INVOLVING SECURITY**

**The Importance of Security Guidelines**

For all Government Departments, the basic guidelines for security practice is the *Protective Security Manual* Commonwealth of Australia - Protective Security Manual, AGPS, Canberra, 1991 issued by the Attorney-General's Department. The ANAO uses this manual in the conduct of its audits taking account of the agency-specific conditions, as a guide in assessing the adequacy of an agency's security regime. As well, there is the Australian Communications Electronic Security Instructions No. 33 entitled Security in Electronic Information Processing Systems. Other guidelines, for example in relation to ethical behaviour, fraud control and privacy, are also a starting point for relevant audits.

While security issues are pervasive across agencies, it seems inevitable that a largely information technology focus is likely to dominate our attention. In this respect, the ANAO is particularly conscious of the statement made in the report `Clients First, Clients First- the Challenge for Government Information Technology. Information Exchange Steering Committee, Canberra; 1995 (page 32) Where information is stored and exchanged electronically it must be secure and properly maintained to ensure privacy. It is clear from this report that security and privacy of client information is accepted to be a core responsibility of government.

When I was Chair of the then Information Exchange Steering Committee (IESC), I was very pleased to promote the work of the Committees IT Security Working Group. This Group had a rather rocky road to navigate over for some time, but produced earlier this year a widely acclaimed set of guidelines Security in Information Technology - Guidelines for Agencies, Information Exchange Steering Committee, Canberra, March 1995 to assist agency managers to manage their IT environments
more effectively. Those guidelines were meant to be complementary to the existing security guidance material. The guidelines cover three major themes - an overview of security standards, an examination of security and authentication issues arising from the interconnection of IT systems under the control of Commonwealth Agencies, and guidance on the implementation of secure interconnections. They build on the first set of guidelines produced by the Group entitled Interconnection User Authentication and Security Issues which was a brief overview of security requirements for agencies which operate approved automated information systems for unclassified, restricted and in-confidence information.

Information Technology Audits

The main thrust of what the ANAO looks for in an Information Technology (IT) audit is summed up in the statements What does representing good value for money in IT mean? It depends on two things:

1. What does the business want to achieve? and


Security is considered within this context. In large part, this is because of the possible impact on modern businesses of security breaches of their information bases.

The ANAO conducts two broadly different types of audits. The first type of audit supports the ANAO's financial statement audit program. The controls provided by computer systems are assessed to determine the level of reliance that can be placed upon them in supporting the financial data maintained on, or provided by, the computer systems. Simply put, the more reliable the controls, the less testing of actual financial transactions that needs to be carried out. These computer security controls provide a large measure of assurance as to the viability and completeness of financial data.

The second broad category of computer audits comes under the purview of performance auditing. The aim here is to ensure that resources are allocated and used in an efficient and administratively effective manner to meet legislative and government objectives.

These audits are more comprehensive and address security systems in more detail. The level of security required is largely dependent upon the sensitivity of the data held and on the risks associated with the accidental or malicious disclosure of this data. This is the yardstick used by the ANAO to assess the adequacy or otherwise of an organisations security environment.
ASCPA's Audit Centre of Excellence classifies security controls in relation to information technology into three broad areas:

(1) Administrative controls: policies and procedures relating to the administration and protection of the computing infrastructure such as screening computer facilities personnel, controlling the use of hardware, diagnostic and repair utility programs and licensing and copyright enforcement, including adherence to corporate standards and integration policies.

(2) Logical security: access to data and programs needs to be controlled against inappropriate modification, authorisation, access, use, disclosure and disruption. The major risk with logical access is that the integrity, confidentiality and availability of data and resources may be compromised.

(3) Physical security and business continuity: it is essential that procedures exist to safeguard the hardware and its environment in order to protect the storage and transmission of data. Business risks arise through, for example, accidental or malicious damage to hardware, unauthorised use of equipment, inappropriate disposal procedures and poor recovery strategies. Op. cit., Information and Technology Risks and Responses (pages 9-13)

There is a body of evidence that points to most breaches of security being traced back to current employees or people who have recently left the employer. The ANAO is cognisant of this intelligence. As a result, this aspect of security is given due consideration in its planning of an audit. The audit methodology is therefore designed to cover the risk of both internal as well as external intrusion.

In every case, however, the overriding consideration is the value and nature of the data and equipment that need to be protected. In short, threats to security must always be weighed up against the consequences of security breaches and an appropriate security regime put in place. The ANAO's reports on IT security aim at adding value, that is, recommendations that are practical and cost effective.

Some Security Issues Identified in ANAO Audits

The ANAO has undertaken several major reviews of computer security in Commonwealth agencies. In the conduct of these audits the ANAO has attempted to address each agency's business needs, the available technology and the policies in place to manage the information and security requirements of the agency. You might be interested in some of the main findings.

The ANAO has found that, while there are many activities that agencies do well in the area of security, the main area for improvement is the need for a well considered policy and strategic framework which takes account of changing technologies. In essence, there is a need for a more open and flexible computing environment which can react reasonably quickly to changing functional and business needs.
Other major issues identified in ANAO audits as being important were:

- that high level policy making bodies in agencies show leadership, provide direction and promote the value of security consciousness;
- that agency security policies be agency specific while keeping to within general government security guidelines; and
- that agencies follow best practice by making best use of available software and hardware utilities and information available.

For example in one agency, the main security policy making body had not met in two years. The ramifications of this and the "flow on effects of this high level inaction was to restrict the organisations ability to adjust to changing circumstances in a planned and co-ordinated way. Other examples involve the ANAO examining service levels to clients and making recommendations to help improve the turnaround times on a range of services.

Generally most recommendations made by the ANAO have been accepted by agencies, often quite enthusiastically. There are times, however, when an agency has disputed the recommendations made on the grounds that they are impractical. This highlights the fact that the ANAO must take all reasonable steps to ensure that its recommendations are practical and if implemented will result in improvements in administration.

Importantly, I believe, the ANAO has also played a role in making agencies aware of systems, methods and policies that are available in comparable organisations thus helping to introduce "best practice across agencies. This perception is reinforced by the recommendations of the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into the protection of confidential personal and commercial information held by the Commonwealth, which states that the Australian National Audit Office conduct security efficiency audits of computer systems and that sufficient resources be allocated to the Australian National Audit Office to support this role. In Confidence: a report of the inquiry into the protection of confidential personal and commercial information held by the Commonwealth, House of Representatives Standing Committee on Legal and Constitutional Affairs, Parliament of the Commonwealth of Australia. AGPS, Canberra, 1995 (page 52). The Attorney-General has indicated that he would respond to the report by December 1995.

The following is an indicative analysis on the types of considerations the ANAO adopts in its IT audits bearing on security issues and standards in particular computing environments.

Computer Systems Security
As I stated earlier, the general thrust of an IT audit is to assess if an agency's computer system processes data in a complete, accurate and reliable manner so as to enable the agency to carry out its business efficiently and effectively. A basic requirement is that all systems should incorporate an audit trail or audit log. Systems security audit trails should be monitored on a regular basis by the Systems Supervisor or an agency's Computer Security Officer(s). The IESCs Security Guidelines indicate that security audit logs covering a period of at least twelve months should be kept in the system or archived to tapes or floppy discs. The ANAO issued a guide to auditing computer based application systems for its staff in 1992 which, inter alia, outlines the general audit framework in which such audits should be conducted. Auditing Computer Based Application Systems. Australian National Audit Office. AGPS, Canberra., September 1992 (pages 1-5)

Due to the various technologies used and different platforms that generally combine to make what we call a computer system and its associated networks this subject will be considered in several parts. It is an axiom of security that a mechanism for protection should be incorporated into the lowest layers of a system. The Protection of Information in Computer Systems; Saltzer J. H. & Schroder M. D. Proceedings of the Institute of Electrical and Electronic Engineers (IEEE), Volume 63, 1975 (pages 1278-1308)

This is a key area for investigation.

- **Mainframes**

Most large repositories of data are stored on mainframe computers. On most mainframes in use in the government, a security access software operating system is used to protect access to the systems resources. The basic principle on which these products operate is to define system resources and then grant users or groups of users with similar access requirements, access to these system resources in a controlled manner.

The ANAO looks for a good access security regime with well structured and documented functions that address the agency's specific requirements.

The ANAO first needs to understand the agency's business. Second, it needs to understand what the computer systems are meant to achieve in relation to the business needs. This intelligence is gained from discussions with agency management and an examination of corporate and business plans. Third, there is a need for the ANAO to understand the actual systems which are often quite complex. The audit team does this in a variety of ways, for example by running system reports, interrogating the system and examining the allocation of resources to various users. Statistical samples are taken of groups of users and a detailed analysis is done of the access rights verses the actual requirements for that sample.

On the other side of the equation, having set up the system, is there appropriate and adequate monitoring of the use of systems resources? Reports are run against
system information to extract data from previous months, enabling a historical picture to be constructed. Systems are examined in detail including, access security, change control, application development, problem management (for example, error tracking) and business resumption planning, to name some of the areas investigated. Throughout an audit, agency staff are kept informed of progress and are consulted as a matter of course.

The ANAO has found that because mainframe systems have been in operation for many years, the systems are mature and staff generally have well developed specialist skills and know-how, and there is generally a good sense of discipline in the running and security of these systems.

The auditors examine policies and procedures to gain an understanding of how these relate to the business requirements of an agency. Explanations are sought for perceived problems and the audit team attempts to gain an understanding for the reasons behind agency decisions. Individual circumstances are weighed up and an opinion formed along with any recommendations the ANAO considers would improve the performance and the efficiency of the running of the systems in a cost effective manner.

- Midrange and PC/LAN/WAN Systems

Midrange systems are also often referred to by their manufacturers names or by the operating system running on the particular machine. It is therefore not unusual to hear midrange machines referred to as UNIX machines. LAN/WAN systems are generally a collection of PCs linked together to form a network. These systems are often built around distributed, client/server or open systems. The definition of open in this respect is a matter for debate but not in this forum.

When compared to mainframe systems, there are generally not the security utilities available to secure satisfactorily these smaller systems. By nature, these systems are decentralised and are managed by few staff who tend to manage and control all of the functions on the systems. From a security point of view Distributed and open systems create fertile soil for security hazards to develop Operating System Security for Midrange and Large Computers, Herman, Gary. DataPro on CD-ROM, April 1995.

One of the main drawbacks of these kinds of systems is that staff are often required to undertake a broad range of duties minimising the opportunities for them to specialise. This leads to over reliance on the one or two system gurus which in turn creates potential control and security concerns.

What the ANAO looks for in these systems is the existence of a security regime involving mainly management of user access, password control, access control and monitoring arrangements. In the experience of the ANAO, these computer facilities tend not to be secured as well as mainframe computers, as I have previously noted. This trend from an audit point of view is of concern, as this is an expanding sector of
the industry which meets the demands of an increasingly decentralised and devolved public service.

The Information Exchange Steering Committee (IESC) noted earlier this year that:

> The security of client/server transactions being sent from the client across a network and completing at the server is a major concern for agencies. Client/Server Computing in the Australian Public Service: The Next Wave? Information Exchange Steering Committee. AGPS, Canberra, January 1995 (page 73).

The section on security (5.6) from pages 73-77 is well worth a read.

The IESC went on to say that, while agencies are generally aware of the security management issues of distributed systems (such as LANs), client/server introduces the extra complication of transactions being held on workstations, even if only temporarily, particularly given security issues associated with client-based operating systems. One industry respondent argued that use of applications which store data on the client should be avoided where the data is subject to privacy laws.

The IESCs Security Guidelines Security in Information Technology - Guidelines for Agencies, Information Exchange Steering Committee, Canberra, March 1995 (page 22) indicate that research shows that the main causes of data loss on client/server networks are as follows:

<table>
<thead>
<tr>
<th>Main causes of data loss</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee errors</td>
<td>50%</td>
</tr>
<tr>
<td>Dishonesty</td>
<td>15%</td>
</tr>
<tr>
<td>Disgruntled employees</td>
<td>15%</td>
</tr>
<tr>
<td>Outside intruders</td>
<td>10%</td>
</tr>
<tr>
<td>Physical threats</td>
<td>10%</td>
</tr>
</tbody>
</table>

The Governments emphasis placed on stored data - on any platform - is made clear in the statement that The Commonwealth considers that it is the owner of all information entered into any Commonwealth computer and this information must be treated and protected as any other Commonwealth asset IBID, (page 5)

- Networks
Networks audited by the ANAO vary from the extensive nation wide networks of the large departments to the LANs of the smaller agencies. Greater attention will be paid to security aspects of those networks with the wider adoption of electronic commerce. As you would be aware, the Government has decided to implement electronic commerce for purchasing by 1997 and has issued a Statement of Direction. Electronic Commerce - Commonwealth Government Statement of Direction. AGPS, Canberra, April 1995

The ANAO reviews the nature and extent of information that is transmitted on the network. This is evaluated against the level of protection afforded to that data. This is done by investigating the protocols of the networks, the type - if any - of encryption used and the security of computer equipment at various points in the network. The use and location of printers are also an important consideration. The ANAO reviews the security around computer rooms, backup storage sites and central printer, cheque and microfiche printing facilities.

Due to the complex nature of some of the larger networks, there are special facilities and utilities provided to network managers to help them troubleshoot the network. These utilities are very powerful and there is a risk they can be misused. Hence the ANAO looks at the security of these utilities as part of its network auditing program.

Broader Security Reviews

For some years, the ANAO undertook audits in a number of agencies which were known as protective security audits. These audits varied in size and complexity, but had as their main focus the review of an agency's general security environment. Selected ANAO staff were provided specialised training to assist in the conduct of these audits. From some brief research I have undertaken, it appears that the results of these audits were of assistance to agencies in making improvements in their security regimes.

It is little unclear why the ANAO stopped undertaking audits of this nature, although it is reasonable to surmise that the ANAO decided that its scarce resources could be best utilised in other areas.

The ANAO has recently introduced a program of audits known as audits of financial controls and administration which will focus on common areas of administration in APS agencies. These audits will adopt an empathetic approach, that is, they will not be ensuring all is are dotted and t's crossed, but rather that platforms and mechanisms have been appropriately implemented. In part, the decision to undertake these audits is based on an apparent Parliamentary perception that devolution of management authority under the public sector reforms has not been matched by commensurate evidence of accountability. These audits will assist in providing that required assurance.

The major thrust of these audits will be to identify what can be described as best practice, and assist individual agencies to assess the adequacy or otherwise of their control environment, if that is in fact required, in the context of a best practice model.
I stress they will be generic in nature covering, for example, implementation of security guidelines in agencies.

I have an open mind at the moment on the benefits of including in our program, audits which address issues of security across agencies. Our aim is to focus on areas where we can add most value to public administration. I certainly am keen to obtain the views of agencies themselves on particular areas where there would be mutual benefit through the conduct of such audits.

LOOKING IN OUR OWN BACKYARD - THE ANAO'S ENVIRONMENT

From a security perspective, the ANAO is in one respect a relatively easy environment but in another, seems quite complex. Let me explain.

The ANAO is a relatively small agency with approximately 350 staff at present. These are primarily located in Canberra, Sydney and Melbourne with all staff being in one location in each city. Between each location there is the usual range of communication facilities such as telephone, facsimile and computer links. On the face of it therefore, maintaining an appropriately secure environment should not be a difficult task. However, overlaid on this situation is the fact that the way the ANAO does business is through its staff being located in the premises of other agencies for appreciable periods of time, thus generating the need for links between those staff and their colleagues and systems located at ANAO premises. The ANAO also engages a large number of contractors to assist it in undertaking its work.

The nature of our work requires us to have access to a vast array of information obtained from the agencies which we audit. Finally, the Audit Act, quite rightly, imposes strict secrecy requirements on the ANAO in respect of the information it obtains in the course of conducting its audits.

These elements make the task of ensuring that appropriate security framework is maintained a rather challenging one.

In this context, I would like to briefly discuss a number of aspects of the ANAO's own computing environment.

ANAO's Computing Environment

The ANAO aims to provide its staff a functional and secure computing environment. As the ANAO's product is the reports it produces, great emphasis is placed on providing auditors with the tools required to produce the finished product. To this end the ANAO has a network of midrange UNIX computers together with a range of personal computers (PCs) running software products that assist in the conduct of the audit and in providing all the necessary support functions.
As I have mentioned, the ANAO has access to a great deal of information, some of it quite sensitive, sometimes for example, with national security implications and at other times having a personal privacy perspective.

Those who are familiar with the various levels of security on different platforms, that is, mainframes, midrange machines and PCs, would know that the level of security afforded by the various platforms generally decreases with the size of the machine. In other words, one would expect a large mainframe to be inherently much more secure than a small agency's PC based LAN. This is so because of the limitations of the software and, to an extent, the technology currently available on smaller systems. The administration built into large mainframes has been developed over more than thirty years and the processing is centralised as I mentioned earlier. In a more decentralised environment, the necessary administrative systems, including security, are still being developed to complement what is presently available in what are clearly more exposed operating conditions.

This raises the question of how the ANAO with its LAN based system can sufficiently protect sensitive data obtained from other agencies, particularly where audit staff are issued with portable PCs.

The answer, in general terms, is ensuring that all staff are very conscious of the need to ensure all information held is afforded an appropriate level of security and putting in place arrangements which suit the specific requirements in each case. We operate on the premise that prevention is better than cure.

Consider an auditee that has very sensitive client information. This data is stored on the agency's computer systems and is normally well protected. The ANAO, as part of both its financial statement audits and performance audits needs to examine and extract records for verification purposes. The ANAO does this by running CAATs (Computer Assisted Audit Techniques), which are computer programs which interrogate computer files and extract information based upon certain predetermined criteria.

An agency's data may be analysed using computer programs written by the ANAO and installed on the agency's own computers. Alternatively, the agency's data may be downloaded onto an ANAO PC and analysed using commercially available software (PC-based CAATs) or the data may be downloaded onto various forms of magnetic media and analysed on the ANAO's own UNIX based standard CAATs system.

Obviously the ANAO has to enforce rigid controls to protect the confidentiality of this data and in doing so is in no different position in this respect than any other agency. We are also now experiencing the problem of having to determine appropriate security arrangements for the use of portable PCs by our audit staff in the field. This has been accentuated by the recent establishment of a strategic relationship with Price Waterhouse to equip those staff with state of the art hardware and integrated audit technology software products. The wider use of such technology will facilitate the sharing and quality assessment of information (including agency data) and general audit activity. However, there is also greater exposure for our clients and our
audit business in such an environment. We are currently undertaking a risk assessment of this situation and developing appropriate guidelines to ensure risk minimisation in this new method of operation.

- **External Communication Connections**

A major area for potential exposure comes from the connection to external networks. These connections provide the physical access path required to gain entry to the ANAO's computer environment. The ANAO has at present two types of external connections with a third under consideration.

- **Connection to the Internet**

The first is the ANAO's link into the Internet. The ANAO Internet network, is independent of the ANAO's corporate network. This arrangement satisfies the ANAO's requirement of quick and easy access to currently available information without compromising the ANAO's network and its security in any way.

This arrangement provides the best of both worlds. This is because there is no physical link from the Internet into the ANAO's corporate network making any access physically impossible from out side. This arrangement is often referred to as providing an air gap between the Internet network and the ANAO network. As time goes on, the robustness of fire walls will improve to the point when it will be possible to have a physical connection at low risk to the integrity and security of our information bases.

- **Connection to the Parliamentary Database**

The ANAO needs to be in constant touch with events taking place in the Parliament. One of the mechanisms through this is done is by giving ANAO staff access to the Parliamentary Databases. This access is set up such that the ANAO can access Parliament but access the other way is not possible, once again protecting the integrity of the ANAO's network. Again, it should only be a matter of time before two way links are not only reasonably secure, but also that this security can be provided at reasonable cost.

- **Connections into the ANAO (Dial in)**

As auditors spend much time out in the field, there is a requirement for them to have access to ANAO systems. A pilot is currently underway to investigate the effect of limited dial-in access to part of the ANAO's network. Various options are being investigated and the effect of these changes will be considered in the context of the overall security of the ANAO's network. Rest assured the ANAO will take steps to ensure that there is no degradation of its current security regime.

**The Performance Imperative**
Put simply, we need to protect our two main business units, financial and performance auditing, from any security weaknesses. Importantly, we also need to protect the information of agencies we audit. We put considerable emphasis on information as a corporate asset. We can scarcely recommend credible security best practice to other agencies if we ourselves do not implement such practice. It is a case of physician heal thyself. We are committed to continuous improvement in our practices and have established breakthrough and continuous improvement teams dedicated to developing ideas and initiatives aimed at real quality improvement in our audits. The focus is very much on improving our professionalism and performance. We regard peer reviews as being very important in these contexts.

CONCLUDING REMARKS

The ANAO sees the implementation and management of an appropriate security regime as an important element of effective public sector administration. In that respect we will be reviewing performance against relevant guidelines in our audit reports. Security is particularly important in protecting the Commonwealth’s vast and valuable information base which in turn is essential to the performance and credibility of the APS. However, there is a need to engender greater concern about the security of all our assets whatever their security classification. Public service managers need to recognise and adequately assess the implications of any disruption to their businesses or functions from security deficiencies and breaches, their responsibilities to those who provide personal or other confidential data as well as any international obligations that apply.

Security in general, and the management of security issues in particular, need to be considered in the context of the broader APS reform agenda. Failure to do so or to look at security in isolation is likely to produce, at best, only partial solutions that will not be conducive to high levels of performance. In particular, initiatives such as accrual reporting both facilitate and demand attention to all the resources that are entrusted to us. The ANAO has taken a high profile in this area and is anxious to assist agencies in implementing their systems and in managing at all levels on an accrual basis. In particular, the ANAO is heavily involved in the conceptual development and dissemination of best practice across the public service in both accrual reporting and accounting.

Collectively, we need ensure that well informed risk assessments are made in any security review so that we fully comprehend the potential impact on program results as well as on public confidence. Maintaining security of our assets is an element of our performance, not an outcome. Put another way, security is not an end in itself.

Audits conducted by the ANAO suggest that we have some way to go in the implementation of fully effective, value-for-money security regimes. Within its resource capabilities, the ANAO will continue to assist in raising awareness about the importance of security through the conduct of targeted audits which address security and related issues. We will be aiming to work closely with Audit Committees and internal audit units in developing a co-operative, strategic approach to such audits to complement any initiatives and reviews being undertaken by, or on behalf of, the agency. We will be particularly interested in the way agencies have applied the
various security guidelines with the aim of identifying best practice in our reports. If there is generally considered to be the potential for adding value to public administration by a generic report on security issues, this could be assessed under our recently announced audits of financial controls and administration. Financial Control and Administration Audit - Charter. The Australian National Audit Office. AGPS, Canberra, October 1995

The ANAO will be focused on ensuring that its own environment accords with the various security guidelines and classifications and that we better understand the possible exposures and other risks particularly to our information base including, importantly, that provided by other individuals and organisations. Our responsibilities in the latter respect extend well beyond our organisational boundaries. The aim is to raise the levels of awareness of the threats and opportunities presented by implementation of best practice both within the ANAO and across the public service.

The general message for all of us lies in the old saying that an ounce of prevention is worth a pound of cure. Many would agree with ASCPA's Audit Centre of Excellence that security is a state of mind. In that respect we need to raise awareness and change attitudes as this conference is doing. I am therefore grateful for the opportunity to speak to the issue from an audit perspective.

Grateful thanks are due to Russell Coleman and Ian McShane for their assistance in preparing this address. However, they do not have to bear any responsibility for views expressed.