AUDITS OF PROTECTIVE SECURITY - CONTRIBUTING TO SOUND RISK MANAGEMENT

ADDRESS BY PAT BARRETT, AM
AUDITOR-GENERAL FOR AUSTRALIA

Security in Government 2001 SES Seminar
Canberra, 27 March 2001

Thanks are due to Richard Rundle of my Office
for assistance in preparing this address

www.anao.gov.au

1. INTRODUCTION

I am pleased to be invited to speak at the ***Security in Government 2001 - SES Seminar*** on the role of audit in relation to Protective Security. While the Australian National Audit Office (ANAO) does include audits described in this way as part of its integrated audit framework, much of its audit activity impacts to a lesser or greater degree on protective security issues. I will illustrate this later when describing our various audit products.

The focus of my address today will be on how auditors, particularly external auditors such as the ANAO, can play an effective role in enhancing the security regime in agencies to improve the overall performance of public administration, as well as providing assurance to our various stakeholders that public sector organisations are meeting their National Security Obligations. It has to be said that there is no shortage of potential audit activity both externally, including by the Privacy Commissioner, and internally, by an organisation's internal audit area complemented by any agency security adviser (ASA) and information technology security adviser (ITSA).

The broad nature and concerns of protective security are well conveyed by *The Commonwealth Protective Security Manual 2000* (PSM 2000) as follows:

> *Commonwealth functions and official resources must be safeguarded from sources of harm that would weaken, compromise or destroy them. These sources of harm could include threats from criminally or politically motivated individuals or groups or foreign intelligence services. An appropriate protective security environment is fundamental, not only to good business and management practice but, ultimately, to good government.*[1]

These wide-ranging implications took me back to observations I made in a similar conference in 1995[2]. At that time, the basic guidelines for security practice were set out in the 1991 Protective Security Manual. I spoke extensively about our various audit products covering security and other related concerns in the world of information technology with more open and distributed systems, use of the Internet and related communications issues, including 'dial-in access'; the focus on risk management with the then draft guidelines for managing risk in the Australian Public Service (APS); and financial reporting, using accrual accounting. As is often the case, the forward look fell short of the mark, as now indicated by PSM 2000 with its extensive coverage of risk management in practice; and competitive tendering and contracting, including the implications of private sector involvement both as contractors and sub-contractors; as well as the enormous ramifications of electronic government. In my view, these are the major challenges currently facing the APS and, consequently, generate a greater need for attention by all concerned, including audit.

The ANAO sees protective security primarily as protection of assets in the form of people, physical assets and information against a specific kind of exposure – National Security. However, in a more contestable public sector environment, increasing attention is also being paid to intangible assets such as intellectual property, reputation and goodwill. The PSM defines a security risk as 'the likelihood and consequences of compromise of official resources'[3]. The role the ANAO takes in relation to Protective

Security can best be considered in terms of reviewing the management of policies and procedures, including information, personnel, physical and information technology and telecommunications (IT&T) operations. The ANAO is not resourced to be expert in the technical aspects of, say, data encryption and information management, nor technical processes involved in securing physical assets. That is best left to specialist agencies and/or firms in the private sector.

The ANAO also has an educative role in raising awareness in agencies of the need to pay particular attention to security matters. This is largely addressed by carrying out audits of protective security issues across agencies and then reporting back to participants about the overall findings. Their involvement in the preparation of any Better Practice Guides is also a significant learning process. Hopefully, such activity will complement, if not enhance, the work being undertaken by internal audit and security advisers. This role will also be expanded upon later in this address.

In the time available, I thought it might be useful, and interesting, to talk briefly about agency risk management and responsibility for protective security in a more privatised public sector; about Protective Security audits as part of our integrated audit approach; and related audit coverage and findings in recent years. I will wrap up the presentation with some concluding remarks.

2. AGENCY RISK MANAGEMENT AND RESPONSIBILITY FOR PROTECTIVE SECURITY

Risk management can be defined as:

> *A logical and systematic method of identifying, analysing, assessing, treating and communicating risks associated with any activity, function, or process that will enable organisations to minimise losses and maximise opportunities*.[4]

The growing recognition and acceptance of risk management, as a central element of good corporate governance and as a legitimate management tool to assist in strategic and operational planning, has many potential benefits for the public sector. That is, risk should be seen as an opportunity, not only as something that should be minimised or avoided.[5]

Nevertheless, the effective implementation of risk management practices continues to be a major challenge for public sector managers. This is particularly so given the apparent risk averse public sector culture of the past and also given the current climate of, in particular, increased integration of the public and private sectors where many would argue there is a need for greater accountability, or even a different type of accountability. The further challenge is to maintain an appropriate level of accountability for the effective delivery of public services, whilst maximising the potential efficiency gains available through such arrangements.[6]

In the last decade, government agencies have put in place many of the elements of good corporate governance. These include corporate objectives and strategies; corporate business planning; audit committees; control structures, including risk management; agency values and codes of conduct; identification of stakeholders;

performance information and standards; evaluation and review; and a focus on client service to name just a few. However, too often these elements are not linked or interrelated in such a way that people in the organisation can understand both their overall purpose and the ways in which the various elements need to be coordinated in order to achieve better performance. Such integration is also necessary to ensure that a mutually supportive framework is properly focused on achievement of required outputs and outcomes and related accountability to identified stakeholders, including for security matters.

Therefore, the real challenge is not simply to define the elements of effective corporate governance but to ensure that all the elements of good corporate governance are effectively integrated into a coherent corporate approach by individual organisations and are well understood and applied throughout those organisations. If implemented effectively, such an approach should provide the strategic management framework necessary to achieve the output and outcome performance required to fulfil organisational goals and objectives. That framework also assists agencies to discharge their accountability obligations with greater confidence and with both internal and external credibility. Clarity and consistency in terminology would also help.[7]

Not to be forgotten in the drive for results and effective risk management as part of good governance, is the need for managers to continue to ensure the effectiveness of the control environment being implemented in their organisations. While agencies should be generally aware of the need to address their responsibilities for, say, fraud control under the *Financial Management and Accountability (FMA) Act 1997*, the importance of providing an effective control environment cannot be underestimated. Good governance means good risk management, effective fraud control, good internal control and, of course, effective management of security for people, physical assets are information as well as other intangible assets, as indicated earlier.

The notion of a control environment has to start from the top of an agency, that is, from the Chief Executive Officer (CEO) and/or a Board, together with senior management. To be effective it requires clear leadership and commitment. This imperative is reinforced by the interrelationship of risk management strategies with the various elements of the control culture. The adoption of a sound and robust control environment at the top of an agency will strongly influence the design and operation of control processes and procedures to mitigate risks and achieve the agency's objectives. The clear intent and message to staff should be that such processes and procedures should be designed to facilitate, rather than to inhibit, performance. This approach should be promoted as good management. In short, the control environment is a reflection of management's attitude and commitment to ensuring well-controlled business operations that can demonstrate accountability for performance in areas such as protective security.

It is useful to point out here that audit committees provide a complementary vehicle for implementing relevant control systems incorporating sound risk management plans. This view is shared by the private sector where corporate representatives have agreed that effective audit committees and risk management plans are an indication of best practice and markedly improve company performance, including decision-making. The internal auditing function of an organisation plays an important

role in this respect by examining and reporting on control structures and risk exposures and the agency's risk management efforts to the agency governance team.

An effective audit committee can improve communication and coordination between management and internal as well as external audit, and strengthen internal control frameworks and structures to assist CEOs and boards meet their statutory and fiduciary duties. An audit committee's strength is its demonstrated independence and power to seek explanations and information, as well as its understanding of the various accountability relationships and their impact, particularly on financial performance, but increasingly not confined to financial issues.

I cannot overstress the importance of the need to integrate the agency's approach to control with its overall risk management approach in order to determine and prioritise the agency functions and activities that need to be controlled. Both require similar disciplines and an emphasis on a systematic approach involving identification, analysis, assessment and monitoring of risks. Control activities to mitigate risk need to be designed and implemented and relevant information regularly collected and communicated throughout the organisation. Management also needs to establish ongoing monitoring of performance to ensure that objectives are being achieved and that control activities are operating effectively.

The key to developing an effective control framework lies in achieving the right balance so that the control environment is not unnecessarily restrictive nor encourages risk averse behaviour and indeed can promote sound risk management and the systematic approach that goes with it. However, it must be kept in mind that controls provide reasonable, not absolute, assurance that organisational objectives are being achieved. Control is a process, a means to an end, and not an end in itself. It impacts on the whole agency; it is the responsibility of everyone in the agency; and is effected by staff at all levels. While 'tone at the top' is important, the success of such governance elements depends importantly on the 'ownership' and commitment of operational managers.

The principles and techniques identified and explained as part of good practice in relation to risk management are also found in Part B of the Commonwealth Protective Security Manual 2000. However, there is a tendency for protective security to be regarded as a separate activity within agency planning for risk management in many organisations. This separation minimises the opportunities for comprehensive and integrated assessments of all risks facing an agency. Another related issue for agencies is, of course, the implementation of Fraud Control plans required under the FMA Act. The same risk management principles should be applied in the preparation of these plans. Therefore, the challenge now is for agencies is to make the process of risk management sufficiently comprehensive to ensure that risks of a protective security or fraud nature are included as part of agency risk management, not as separate activities. In the more complex management environment being discussed, there are inevitably new and/or different factors that need to be addressed in such processes. In other words, it is not a simple one-off exercise to establish a properly integrated risk management framework.

The process of risk assessment and its treatment needs to be dealt with by agencies in an increasingly devolved environment, where they are also facing the challenges of managing outsourced service delivery and support. The following comment by

Professor Richard Mulgan of the Australian National University on the accountability dilemma associated with the greater involvement of the private sector, particularly in the delivery of public services, is very challenging:

> *Contracting out inevitably involves some reduction in accountability through the removal of direct departmental and Ministerial control over the day-to-day actions of contractors and their staff. Indeed, the removal of such control is essential to the rationale for contracting out because the main increases in efficiency come from the greater freedom allowed to contracting providers. Accountability is also likely to be reduced through the reduced availability of citizen redress… At the same time, accountability may on occasion be increased through improved departmental and Ministerial control following from greater clarification of objectives and specification of standards. Providers may also become more responsive to public needs through the forces of market competition. Potential losses (and gains) in accountability need to be balanced against potential efficiency gains in each case*[8].

The other key development impacting on the complexity of required risk management responses is the extent to which agencies are increasingly embracing online service provision. The Commonwealth government has committed to a strategy of Government Online by the end of 2001. Internet services were to complement, not replace, current written, telephone, fax and counter services, and to greatly improve the quality, user-friendliness and consistency of those services. This strategy includes the following elements, all of which have implications for risk management particularly in the area of protecting the information assets of government:

- *improving public access to a wide range of government services, especially by people who live in regional, rural and remote areas or older Australians and people with disabilities;*

- *providing access 24 hours a day, seven days a week;*

- *reducing bureaucratic and jurisdictional demarcation to provide unified services based on user requirements; and*

- *encouraging growth of e-business, both business to business and business to government, and associated opportunities.*[9]

Commensurate with the potential for improved service and reduction in costs is increased risk in the following areas:

- the security of information transferred over the Internet;

- the privacy of information on individual or business; and

- the ability to authenticate the user requesting government services or financial assistance.

These requirements are also reflected in changing skill sets in agencies which need to be managed without unnecessarily raising the risk profile. The rate of staff turnover

in agencies and the associated loss of corporate knowledge has become a matter of some concern in this respect. This issue comes up persistently in the work the ANAO does with agencies and it is impacting not only internal performance, but also on the latter's ability to effectively manage contract relationships with external providers. Parliaments are also expressing similar concerns, which was reflected in a recent Conference of Public Accounts Committees[10].

With the increased involvement of the private sector in the provision of public services, the security of agency data is a critical issue. Contracts negotiated between public service agencies and their private sector providers must include provisions that acknowledge Australian federal government IT security requirements. In addition to the technical issues associated with the protection of the data held by government agencies from unauthorised access or improper use, there are also issues associated with the security of, for example, personal information held by government agencies which falls within the scope of the Privacy Act. A watchful citizenry will want to be certain that agencies and their contractors cannot evade their obligations under such legislation.

Government agencies need to come to terms quickly with the potential applications of Public Key Infrastructure (PKI) technologies to encrypt, decrypt and verify data. In public key technologies, each user of the system has two keys, a public key and a private key, to ensure the privacy, authentication, non-repudiation and integrity of information contained in messages. PKI is of importance to all agencies wishing to embark on initiatives that do more than just disseminate information. It is a core enabler. Key issues addressed by PKI are as follows:

- each person communicating electronically needs to ensure that the recipient is who he or she thinks it is, so that one cannot later deny being the sender of a particular electronic message or transaction. This ability to rebut a party's denial of sending a message is called non-repudiation; and

- the ability to encrypt data transmissions over an open or public network (such as is used by the Internet), so that those transmissions can be read only by the intended recipient.

GATEKEEPER is the Commonwealth Government's strategy for implementing a government PKI.[11] An important element of on-line transactions with the Commonwealth is the ABN-DSC (Australian Business Number – Digital Signature Certificate) which will be used to verify electronic signatures.

Legislative responsibilities

Agencies are responsible for implementing effective arrangements for protective security. This is a matter of government policy and is not backed by specific legislation as such . There is, however, legislative backing for elements of protective security which are identified in the PSM. These deal with disclosure of information with the Crimes Act, the roles of heads of agencies under the FMA Act 1997, and the code of conduct of employees of the Australian Public Service included in the *Public Service Act 1999*. There are also issues to be addressed under the *Privacy Act 1988* as I have earlier indicated. I should also mention the *Freedom of Information Act 1982*. As always, there is an appropriate balance to be struck between openness and

transparency and the need for secrecy. The conundrum often boils down to the differences between public and private interests which is frequently difficult to resolve in practice.

The PSM makes it clear that security decisions are no different to other administrative decisions as follows:

> *They must be formulated on a sound factual, financial, lawful and ethical basis and, most importantly, must be based on an assessment of risk.*[12]

In this latter respect the PSM warns that:

> *The Government needs to be assured that protective security measures are only used when the risk warrants it and that any security measures used are appropriate to the identified risk.*[13]

Implications of the Crimes Act

In general, the Crimes Act contains the legislative provisions for the protection of prescribed official information and the penalties for unauthorised disclosure of that information. This includes penalties for the negligent handling of information that it is a person's duty not to disclose. This Act makes it clear that it is an offence for a current or former Commonwealth officer to disclose any information that he or she is, or was at the time of ceasing to be a Commonwealth officer, bound not to disclose. A Commonwealth officer for these purposes includes a person performing services for or on behalf of the Commonwealth, such as contractors.

Commonwealth officers are also bound by provisions dealing with the protection of official secrets. Section 79 of the Crimes Act deals with espionage and official secrets and makes it a criminal offence for any person to communicate prescribed information that it is his or her duty to treat as secret.

The combined effect of section 70 and subsections 79(3) and 79(4) is that the unauthorised disclosure of information held by the Commonwealth is subject to the sanction of criminal law.[14]

Financial Accountability and Management Act 1997

The FMA Act makes clear the responsibilities of Chief Executive Officers as follows:

> *A Chief Executive must manage the affairs of the Agency in a way that promotes proper use of the Commonwealth resources for which the Chief Executive is responsible.*[15]

APS Code of Conduct

The APS Act 1999 includes an outline of public sector values and an accompanying Code of Conduct. The Code of Conduct requires that an employee must:

- behave honestly and with integrity in the course of APS employment; and

- act with care and diligence in the course of APS employment;

Employees of some agencies have additional responsibilities under functional legislation, for example, staff of the Australian Taxation Office and the Australian Customs Service.

There may be an absence of specific protective security legislation, but it is very clear that it is a management responsibility to be regarded most seriously. The PSM notes that:

> *Agencies that do not provide an appropriate security environment for Commonwealth functions and official resources place at risk the Commonwealth at large, not, just themselves.*

3. AUDITING PROTECTIVE SECURITY AS PART OF OUR INTEGRATED AUDIT APPROACH

The role of the Auditor-General has been described as follows:

> *to provide the elected representatives of the community with an independent, apolitical and objective assessment of the way the government of the day is administering their electoral mandate and using resources approved by democratic processes.*[16]

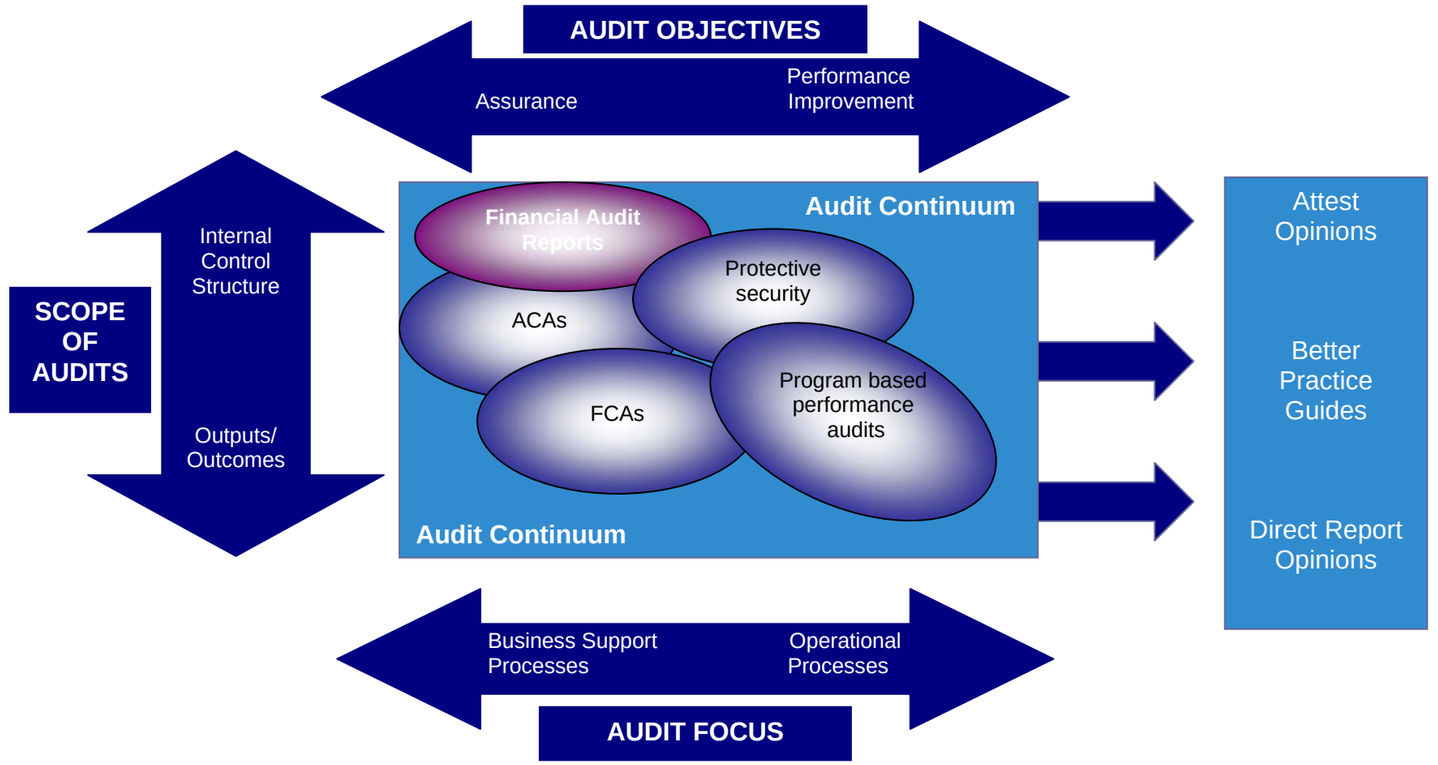
Through reports and other products, the ANAO brings to the Parliament and Commonwealth entities:

- independent audit advice, which contains analysis and supporting explanations and assurances about the operations of public sector agencies;

- a broad understanding of public sector management; and

- a commitment to encouraging the adoption of better practice techniques to improve performance and accountability.

The products are aligned to the outcomes of the ANAO by their contribution to improving public sector performance and also providing assurance outcomes to stakeholders. We have developed a range of audit products to review the full spectrum of activities of the APS and government businesses. At one end of the spectrum, or as we like to call it the audit continuum, financial statement audits contribute significantly to our outcome of providing assurance to stakeholders by examining and reporting on the financial management of the agency. At the other end of the continuum, performance audits assess the management of elements of the APS and contribute mainly to our outcome to improve public sector performance. In between, we have a number of other products that contribute to both our assurance and our performance improvement outcome. This continuum is illustrated in the Figure on page 9.



Australian National Audit Office

Financial statement audits

The Chief Executive Officers of agencies, and the directors of governing boards of other entities, are responsible for the records, controls, procedures and organisation, which underlie the information in the financial statements and the preparation of these statements. The independent audit of the financial statements is conducted in order to express an opinion on them. Auditing procedures include examination, on a test basis, of evidence supporting the amounts and other information in the financial statements and evaluation of accounting policies and significant accounting estimates.

The ANAO's role is directed at reviewing all systems bearing on financial management and reporting and at reporting significant control issues. The audits are planned so that there is a reasonable expectation of detecting material misstatements resulting from irregularities, including fraud. Our reports to Parliament on those audits have consistently shown deficiencies in control environments, particularly in the area of security of information technology based systems.

Performance audits

Performance audits aim to provide information and assurance about the quality of the management of public resources. Performance audits assess the economy, efficiency and administrative effectiveness of the management of public sector entities by examining resource use, information systems, delivery of outputs and outcomes, including performance indicators, monitoring systems and legal and ethical compliance. Performance audits do not ignore assurance objectives and are expected to provide information on the operation of controls and administrative processes supporting the delivery of an output or outcome.

Performance audits can be agency-specific, or cover particular themes or common aspects of administration across a number of agencies. As well as identifying areas for change and improvement, performance audits can provide the opportunity to recognise areas of better practice which can lead to the publication of better practice guides, which are publicly available on the ANAO's website, and are intended to assist improvement in public administration by ensuring that better practices employed in some organisations are promulgated to the whole of the Australian public sector.

Financial Control and Administration (FCA) audits

FCA audits are general performance audits undertaken under section 18 of the Auditor-General Act. These audits have the following characteristics:

- they are across-the-board reviews typically involving up to ten organisations;
- they examine business processes that support the delivery of outputs;
- they are reported generically, that is common findings only are included in the report to Parliament and these findings are not attributed to any organisation; and

- they form the basis of the development of a Better Practice Guide (BPG), where there is a need.

FCA audits have regard to the package of financial management reforms implemented over the last decade or so, covering for example: devolution of authority, management of risk, financial reporting, an emphasis on results and enhanced accountability. These audits contribute to both the Performance and Assurance outcomes

Protective Security Audits

Protective Security Audits are across agency studies, similar to the approach taken for the FCA product. These audits examine three key aspects of security:

- information security;
- personnel security; and
- physical security.

The ANAO commenced audits of protective security in the late 1970s. These audits, developed in conjunction with representatives from ASIO were fairly basic when compared to the modern audit product. The 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. However, there was a period in which no audits of this kind were undertaken. I observed that it is reasonable to surmise that the ANAO decided that its scarce resources could be best utilised in other areas.[17]

At the encouragement of the Protective Security Policy Committee, the ANAO re-engineered the protective security audit and relaunched the product in 1996. This audit is now part of the FCA product range and, as such, is carried out on an across-agency basis with the results being reported generically but with individual management letters to the agencies concerned which indicate how they rated against the criteria used. We are planning a Protective Security audit for the coming year addressing the following issues:

- risk assessments and management of business risk associated with E-Commerce;
- technical design and systems selection and implementation;
- information security of Commonwealth data; and
- information privacy of individual's data.

This audit will follow up the Internet Security audit undertaken in 1997 (No. 15 of 1997-98).

Assurance Control and Assessment (ACA) audits

ACAs were introduced in 1996 to examine basic administrative processes and to provide a positive assurance that agencies are meeting their obligations under the

financial legislative framework. The audits are undertaken under the general performance audit provisions (section 18) of the Auditor-General Act 1997 and principally examine internal control structures that are not specifically covered by financial statement audits or other performance audits.

An evaluation of the ACA audit program was undertaken during 1999-2000 and, as a result, the audit approach was re-engineered. The main aim of audits is now to ensure the proper identification and management of risks affecting the common business activities and processes of public sector organisations A number of ACAs near completion including a review of the controls over the engagement of contractors and consultants.

Fraud Control Audits

The prevention and management of fraud are not new issues in the APS. However, the significant changes that have affected the APS over the last decade, such as new service delivery options, the greater focus on outcomes, sometimes to the detriment of proper processes, and the increasing use of technology and links with communications, have resulted in different challenges for agencies, particularly in focusing their control systems to minimise fraud in this dynamic environment. This, in turn, would provide greater confidence to all stakeholders.

Against the background of changes to the APS environment bearing on fraud, my Office is undertaking a rolling program of fraud control audits to provide assurance to Parliament on the preparedness of agencies to prevent and deal with fraud effectively. Several of these audits have been tabled with more underway and planned. In 1999-2000 the ANAO also tabled a report of a survey of fraud control arrangements across some 150 APS entities.

The ANAO's role continues to be directed not at detecting fraud but to review all systems bearing on financial management and reporting and report on significant control issues in our reports. Any apparent fraud is referred to the Australian Federal Police for investigation.

Better Practice Guides (BPGs)

BPGs aim to improve public administration by ensuring that better practices employed in some organisations are promulgated to the whole of the APS. This can involve examining practices in the public or private sectors, in Australia or overseas. The ANAO’s emphasis is to identify, assess and articulate deficiencies as well as good practice from its knowledge and understanding of the public sector. Depending on the subject and nature of information collected during an audit, BPGs may be produced in conjunction with a performance audit or an FCA audit. Alternatively, a BPG might be prepared as a result of a perceived need to provide guidance material in a particular area of public administration. A BPG on contract management has just been released, This guide focuses on helping managers assess contract risk and examine options for managing that risk through a variety of relationships with contractors and suppliers.

The ANAO has been producing and promoting Better Practice Guides since 1996 and has produced nearly 30 guides since that time. These cover a diverse range of subjects

from asset management, preparing financial statements to Internet security and modern contract management. One of the guiding principles used in the development of guides is to identify the better practice undertaken by particular agencies, wherever this is has been possible. Some of the guides have been produced in collaboration with other agencies. This joint approach is a clear indication of a commitment to promote management improvements that is evident in many agencies.

The Commonwealth Protective Security Manual 2000 is an example of a collaborative effort under guidance from the Protective Security Policy Committee and leadership and support form staff of the Attorney-General's Department. The efforts of the people who contributed to this manual are to be commended.

The ANAO regards the contents of this manual to be guidance on best practice and, as such, will use the requirements set out in the manual as the standard against which to assess agency performance in any protective security audits that are carried out.

Benchmarking services

Benchmarking is a widely accepted approach for achieving business performance improvements. It is defined by the American Productivity & Quality Center as 'the process of identifying, learning and adapting outstanding practices and processes [best practice] from any organisation, anywhere in the world, to help an organisation improve its performance'.

In the ANAO, the benchmarking services product initially comprises functional reviews of the major corporate support areas. The overall results of these reviews will be published generically and tabled in the Parliament. At the audit client level, a customised report will be provided to all entities participating in the study. In 2000 two benchmarking reports were published. The first dealt with internal audit and the second with various activities in the finance function. This study is continuing and complements a new project examining the effectiveness of Human Resources functions in the APS.

Access to information and premises

One of the problems for both auditors and agency managers is having sufficient access to information that allows them to assess, and decide how to treat, risks and to ensure that they are in a position to be accountable for their functional (and statutory) responsibilities. A particular issue facing my Office and, I am sure, many others[18], is that of access to contractor records and other information relevant to public accountability. This matter is of concern not only to Auditors-General, but also to public agencies in their role as contract managers, to Ministers as decision-makers, and to the Parliament when scrutinising public sector activities.

My Office has experienced problems in accessing contractor information both through audited agencies and in direct approaches to private sector providers. Several audits and parliamentary inquiries[19] have focussed closely on what public accountability means in the context of contract management, third party service providers and commercially-based public activities.

As part of his/her statutory duty to the Parliament, the Auditor-General may require access to records and information relating to contractor performance. The Auditor-General's legislative information-gathering powers are set out in Part 5 of the *Auditor-General Act 1997*. These powers are broad but they do not include access to contractors' premises to obtain information.

In September 1997, my Office drafted model access clauses (reflecting the provisions of the *Auditor-General Act 1997)* which were circulated to agencies for the recommended insertion in appropriate contracts. These clauses give the agency and my Office access to contractors' premises and the right to inspect and copy documentation and records associated with the contract.

The primary responsibility for ensuring there is sufficient access to relevant records and information pertaining to a contract lies with agency heads. This responsibility is mandated in section 44 of the *Financial Management and Accountability Act 1997* which states clearly that a Chief Executive must manage the affairs of the Agency in a way that promotes proper use (meaning efficient, effective and ethical use) of the Commonwealth resources for which the Chief Executive is responsible.

For accountability measures to be effective, it is critical that agencies closely examine the nature and level of information to be supplied under the contract and the authority to access contractors' records and premises as necessary to monitor adequately the performance of the contract. I stress 'as necessary' because we are not advocating carte blanche access. Audit access to premises would not usually be necessary for 'products' or 'commodity type services' provided in the normal course of business.

The ANAO considers its own access to contract related records and information would generally be equivalent to that which should reasonably be specified by the contracting agency in order to fulfil its responsibility for competent performance management and administration of the contract. The inclusion of access provisions within the contract for performance and financial auditing is particularly important in maintaining the thread of accountability with Commonwealth agencies' growing reliance on partnering with the private sector and on contractors' quality assurance systems. In some cases, such accountability is necessary in relation to Commonwealth assets, including records, located on private sector premises.

The Joint Committee of Public Accounts and Audit (JCPAA) subsequently recommended that the Minister for Finance make legislative provision for such access.[20] The Government response to that report stated that:

> *its preferred approach is not to mandate obligations, through legislative or other means, to provide the Auditor-General and automatic right of access to contractors' premises.*
>
> and that
>
> *the Government supports Commonwealth bodies including appropriate clauses in contracts as the best and most cost effective mechanism to facilitate access by the ANAO to a contractor's premises in appropriate circumstances.*[21]

The response also stated that:

> *the Commonwealth Procurement Guidelines would be amended to emphasise the importance of agencies ensuring they are able to satisfy all relevant accountability obligations, including ANAO access to records and premises.*[22]

While noting the Government's response, the ANAO continues to encourage the use of contractual provisions as the key mechanism for ensuring agency and ANAO access to contractor's records for accountability purposes. The ANAO is currently in discussions with the Department of Finance and Administration to review the content of the standard access clauses and intend to write again to agencies recommending the use of the clauses once this consultation process is complete. This issue has implications for agencies' security responsibilities particularly where direct control over Commonwealth assets and/or information reside with a private sector provider. Specific responsibility is set out in the PSM as follows:

> *The agency must be able to carry out an examination of the contractor's security procedures when undertaking its regular audit or review of the contractor's methods and procedures. Access must be permitted for a security risk review to evaluate the contractor's security procedures.*[23]

Record-keeping

One aspect of information security that is presenting a particular challenge to agency managers and to auditors is record-keeping, particularly in the electronic environment. In the public sector there is, at the moment, a three tiered communications hierarchy with hardcopy documentation (traditional paper file based records) still at the top in many, if not most agencies, followed by electronic or digitally based information (using virtual office systems or *groupware*, electronic diaries or data and e-mail archives) and verbal communications (which may or may not be supported by notes, diary entries, tape recordings or other evidentiary material). A focus on results requires a capacity to make decisions and act quickly but, hopefully, not at the expense of due consideration, in a robust risk management environment (culture), of possible outcomes, nor of accountability for those decisions and actions.

It is evident that there is an increasing tendency for policy and administrative decisions to be communicated and confirmed through e-mail communications. E-mail, electronic files and e-commerce are replacing traditional paper based records and transactions. This is a function of our changing expectations about the speed of communications, a growing emphasis on timely management of the 'political' dimensions of policy, and the appropriation by the public sector of a 'commercial paradigm' in which 'deals are done' (which is given added impetus by the involvement of private sector 'partners' in various aspects of government operations). Nevertheless, as better practice private sector firms demonstrate, good record-keeping is an integral part of a sound control environment and subject to a regularly reviewed risk management strategy which is integral to their required outcomes and accountability requirements.

As a particular instance of the task facing those of us who are required to oversight public sector operations and to provide important public accountability assurance, I

note that the increasing use of e-mail poses significant challenges in terms of our traditional evidentiary standards (which customarily hinge on paper-based records) and the skills base of our auditors. As the Director-General of the Australian National Archives has pointed out:

> *… there is increasing evidence that significant decision-making is taking place in the electronic environment. It is not just email, although this is an important element. It has been technically possible for some time to have electronic files instead of the traditional paper files we are still accustomed to using for deliberative and policy-making work.*[24]

As auditors, we are already confronting situations in which traditional forms of documentary evidence are not available. In such situations we are having to make links in the chain of decision-making in organisations which no longer keep paper records, or having to discover audit trails in electronic records, desktop office systems or archival data tapes.

The problem is that auditors do not always have on hand the range of skills necessary to do the job. A strategy is required to overcome this deficiency. Essentially, auditors are expected to possess a level of forensic IT skills they have not traditionally had to have at the Commonwealth level. To these forensic skills they also need to add evidentiary standards appropriate to these forms of information—in other words, how do auditors establish whether communication has occurred and obtain assurance about the records they have found? In this respect, the following observation is applicable to all of us:

> *Attention will need to be paid to the management of electronic documents, and in particular, the need to be able to recover, authenticate and read important business documents perhaps after years in archive.*[25]

Perhaps we need to look to the example of our colleagues in the areas of prudential assurance or criminal investigations who are continually refining investigatory methodologies to keep pace with offences such as insider trading, corporate fraud or misuse of drugs. If we go down this path, we may have to consider whether there is need to harmonise more closely evidentiary standards for audit with those of the criminal or civil justice systems in our respective jurisdictions. For the moment it might be that the technology is evolving far more rapidly than governments can respond to with legislative or statutory controls.

Developments in the use of technology for the keeping of records are of particular concern for the management of Commonwealth records by the National Archives of Australia (NAA). The NAA has responded with the launch of an 'e-permanence' campaign and the development of a new Australian Standard (AS4390) for recordkeeping. The campaign is designed to remind Commonwealth agencies both that:

> *Good government relies on good record keeping to be accountable and efficient, and Australians expect it.*
> and:
>
> *… even in this paperless age, records still need to be kept. … we want to ensure that the right records are kept for the right amount of time.*[26]

In supporting the work done by the NAA in this area I have informed its Director-General that, while agreeing that the ANAO should not be required to audit recordkeeping as a matter of course, the range of products developed by the NAA together with the new Standard will be useful benchmarks for future audits to assess the standard of recordkeeping in Commonwealth agencies.[27]

Further, I have made the point in another forum that I see records as being an indispensable element of accountability. In this vein:

> *Agencies have an overriding responsibility for their own recordkeeping, including the establishment of appropriate recordkeeping systems, creation and maintenance of full and accurate records, and appropriate access and disposal arrangements.*
>
> *… The ANAO will continue to examine recordkeeping as part of our financial statement audits and performance audits, … to ensure that decisions are transparent, thereby providing assurance about public sector accountability to both the Government and the Parliament.*[28]

I consider that another risk issue has arisen in regard to recordkeeping and the use of IT in the workplace. This involves the need for the public sector as a whole to address and manage the 'Pandora's Box' represented by the boundary between official and personal communications. Electronic records—especially e-mail records—are likely to contain both official records and personal communications. (A separate, but just as important, issue is the inappropriate use of e-mail.) Any position taken on personal communications on official systems should have regard to the organisation's internal communications policy as well as any applicable legislative framework. In any event, it would seem prudent for an auditor to consult early with the organisation's management to determine an appropriate protocol for extracting required electronic records which not only protects the auditor's right to access such records but also provides protection against unnecessary infringement on personal records and personal privacy.

Finally, I refer to a recent article promoting software that automates the destruction of e-mail correspondence.[29] In a letter, responding to this article, NAA emphasised that e-mail should be treated the same as paper records under the *Archives Act 1983* and that "what the software does is illegal under the terms of the Commonwealth's Archives Act of 1983".[30] This is a pertinent message given that public servants have business, accountability and community requirements to keep evidence of their activities. Without such evidence it may not be possible to respond appropriately to any stakeholder concern in this respect which could have adverse consequences for the organisation's reputation. In the latter respect, we should take note that:

> *Confidence is not a measurable commodity that can be either mandated or purchased. Once lost, this fragile but strong characteristic is almost impossible to rehabilitate*.[31]

4. AUDIT COVERAGE AND FINDINGS

The following summaries of previous coverage of protective security and the related areas of Internet security and fraud control show the convergent nature of issues that have been faced by the APS in the last 5 years.

Protective Security Audit No 21 1997-98

The main objectives of the audit were to assess the management and administration of protective security across Commonwealth agencies and to identify, recommend and report better practice in security management. Particular attention was paid to: compliance with Government policy, standards and guidelines; the role of management in protective security; and the operation of security systems and practices. The audit criteria and procedures to assess the management and administration of the individual organisations examined were largely based on the overall control framework of an organisation and the guidance provided in the current Commonwealth Protective Security Manual.

The major audit findings, grouped under the audit criteria on which the audit opinion is based, are as follows:

Security control environment

- insufficient allocation of responsibility and accountability for protective security to program level;
- incomplete security policy and procedure manuals; and
- limited security training for staff, including security officers.

Security risk management

- risk reviews not updated for changes in the security environment; and
- lack of formal planning detailing the treatment of identified risks.

Security control measures

- inadequacies in the classification, handling and storage of classified information including incorrect classification of material, no controls over the copying of documents and lack of appropriate storage facilities; and
- incomplete recording of visitors and after hours access by staff.

Security monitoring and reporting processes

- inadequacies in the monitoring of security incidents, and in the review of automated recording systems; and
- inadequate reporting of security matters to executive management.

Internet Security No 15 1997-98

The objective of this audit was to form an opinion on the effectiveness of Internet security measures within the Commonwealth public sector. The second objective was to provide better practice guidance for managing an Internet connection. The audit covered a range of Commonwealth agencies, which had established an Internet facility. It specifically addressed the following matters : Internet security policies; site management - including change control processes, virus prevention and detection strategies, and incident response plans; controls over access to the Internet site and to data sources connected to the site; and user education and training. The following is a summary of key findings.

Planning an Internet Connection

A secure and effectively managed Internet connection requires detailed planning prior to establishment. Planning includes the formulation of policies; conducting a risk assessment and analysis; and the design of control activities which, when implemented, will achieve an appropriate level of security.

Most of the agencies audited were found not to have undertaken a comprehensive process of planning their Internet connections. In particular:

- security policies and supporting procedures (eg Internet Security Plans) to define standards for secure Internet usage had not been developed. These included agencies with long established Internet connections, and

- a risk assessment and analysis had not been completed prior to connecting to the Internet. As a result, risk management and contingency plans had not been formulated

Securing an Internet Connection

As a consequence of the above lack of planning, few agencies were found to have selected and implemented controls commensurate with the risks associated with their Internet connection. In particular :

- the configuration, operation and management of 'firewalls' could be improved;

- while most agencies had adequate security logging capabilities, only some undertook regular monitoring and analysis of these logs or used specialised tools or software for the security audit function*;*

- the overall incident response capability could be improved; and

- several agencies did not have adequate policies covering virus prevention and did not have tools or software installed on their 'firewalls' for the detection of viruses.

To some extent these findings arise because, at the time of the initial connection, the risks were minimal and it is not surprising therefore that controls were not fully

considered. Now that the risks associated with Internet usage have increased, agencies need to reconsider their control frameworks.

Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympics No5 1998-99

The objectives of this performance audit were to provide assurance to Parliament concerning the adequacy of Commonwealth security planning and preparations for the Games and to identify areas for improvement early enough for any corrective action to be taken.

The audit coverage included Commonwealth security planning and coordination processes, intelligence gathering and threat assessment, border management processes, security at entry and departure points, visiting dignitary protection and national crisis management arrangements. This coverage recognised that there is a security continuum with intelligence as the first stage, followed by preventive action and lastly supported by crisis management in the event of a threat materialising. The following is a summary of key findings.

A considerable amount of effort has been devoted to developing security arrangements for the Olympic Games. A variety of coordination and consultative mechanisms have been set in place to enable Commonwealth and NSW Government agencies to work together in developing joint plans and procedures. The IOC has expressed its satisfaction with the current NSW and Commonwealth security planning for the Games. The overall audit conclusion is that the development of Commonwealth security planning to date has generally been effective but there is scope for improvement in respect of specific issues.

The issues raised in this report did not indicate fundamental flaws in the Commonwealth's security preparations but represented opportunities to provide a greater assurance that security aspects have been fully addressed in the lead up to the Games. The absence of a Memorandum of Understanding between the Commonwealth and NSW Governments was seen as an important threshold issue. Similarly, the lack of agreement on cost-sharing arrangements may have impeded the ability of agencies to plan effectively.

At the time of the audit, there was no consolidated statement of activities being undertaken by Commonwealth security agencies in preparation for the Olympics. Similarly, there was no particular timeframe set for completing different stages of these preparations or a formal mechanism to ensure regular progress reporting against these timeframes. In view of the number of different committees and agencies involved in Commonwealth Olympic security preparations, a Sydney 2000 Games Coordination Task Force was established recently within the Department of the Prime Minister and Cabinet. This is a significant step in facilitating a consolidated Commonwealth approach to key policy and planning aspects and in monitoring the subsequent implementation of plans to finality.

The ANAO also found some scope for improved integration of border management security and law enforcement responsibilities into Commonwealth security planning for the Games. There is a need to develop a border security purpose statement in

which agency roles and responsibilities are defined and security and law enforcement tasks are identified and assigned.

The success of this audit is reflected by the request for the ANAO to undertake a review of the security planning and preparedness for the forthcoming CHOGM meeting in Brisbane. While the ANAO was not able to meet the request for an audit review staff, who carried out the Olympics audit are providing advice in the planning of the CHOGM meeting.

Operation of the Classification System for Protecting Sensitive Information No 7 1999-2000

This audit was a follow-on to Audit Report No.21 1997-98 Protective Security, which reviewed, among other things, information security other than computer and communications security, against the policy and procedures outlined in the 1991 PSM. That audit found inconsistencies in the identification and marking of classified information and weaknesses in the handling and storage of classified information, as well as other breakdowns impacting on information security.

The findings related to four main issues, namely governance arrangements, security clearances, the IT&T environment, and staff awareness and training as follows:

Governance arrangements

Improved information security requires a higher level of interest and attention from senior management of Commonwealth organisations. In particular, the audit found there was a need for higher level direction and review of security matters, preferably, where practicable, through an executive management committee.

A key aspect of this oversight role is to achieve more effective integration of IT&T security with other security activities to enable a comprehensive and consistent approach to the protection of sensitive information resources.

Security clearances

A high proportion of staff had security clearances above the level that their work commitments would require. While these arrangements are likely to have a positive effect on the overall level of personnel security, they come at a cost, with a consequent impact on efficient resource use.

However, of greater concern from a security effectiveness perspective, was that a number of staff had access to information for which they were not appropriately cleared.

As a consequence of the long lead times to obtain clearances, commonly up to three months, the ANAO found that officers obtained access to information before they were cleared, or without a clearance being initiated. The latter applied particularly in the case of temporary staff and contractors.

IT&T environment

The access management controls on Local Area Networks (LAN) were often not configured or implemented in accordance with the requirements of ACSI 33. Areas requiring attention included passwords, the number of log-on attempts, and inactive user accounts. These weaknesses are of concern as all the networks carried sensitive information.

Staff awareness and training

All organisations incorrectly classified files with over-classification being the most common occurrence. Over-classification has the effect of increasing the costs of protection and restricting the flow of information within the organisation.

Documents were often not provided with protective markings to indicate the level of protection required. There was a need for each organisation to consider the marking of documents in conjunction with the assessed risks and other protective controls in place. In addition, there were breakdowns in relation to the storage and transmission of sensitive information, which increased the risk of unauthorised access and/or disclosure of the information.

Electronic Service Delivery, including Internet use by Federal Government agencies No 18 of 1999-2000

In 1999, the Australian National Audit Office (ANAO) conducted a cross-portfolio review of how government agencies were implementing Commonwealth policy on Internet use. The audit report was tabled in Parliament on 15 November 1999. The audit's conclusions included the importance of promoting good practice in service delivery by the Internet, including in regard to security, privacy, authentication and public key infrastructure.

The audit reported that more than half the FMA agencies surveyed during the audit rated security issues as high or very high impediments to the delivery of online services. The ANAO considered that, where they have not done so already, agencies with websites should develop policies and operational strategies for their security. Further, they should develop similar policies and strategies regarding information related to individuals or organisations available from the site. Central agencies such as the former Office for Government Online, now the National Office for the Information Economy (NOIE), could act as clearing houses to help agencies with the development of advice on these policies.

The audit report also observed how Public Key Infrastructure (PKI) is a security measure of importance to all agencies wishing to embark on initiatives that do more than just disseminate information. The absence of PKI was perceived by most departments and agencies as a significant impediment to the delivery of services online. Since this audit, there have been developments in the use of PKI that may have eased some concerns of agencies.

I should also mention that the ANAO has decided to produce a Better Practice Guide to help program managers use the Internet effectively when delivering government programs and services. Program managers were the target audience because a review

indicated they were less well catered for, in terms of guidance, than information technology managers.

The Guide will identify key questions and issues for managers when deciding whether, and how, to use the Internet. Those questions and issues include those related to IT security. Delivering government services by the Internet does not of itself guarantee a better service than more conventional delivery. Consequently, the Guide is intended to help managers already using the Internet to improve their service delivery. By more adequately informing program managers about the questions they should ask and issues they should consider, this Guide is also intended to better equip those managers to make effective choices in conjunction with their IT managers, rather than attempt to answer all the questions and resolve all the issues in this constantly changing environment.

The Guide will also be used by the ANAO, as part of its audit program, in reviewing agency performance in relation to Internet service delivery.

The ANAO is currently conducting a performance audit of the management of Internet security within selected Commonwealth departments and agencies. Ten departments and agencies are participating in a detailed review of departmental security policies and plans, as these relate to Internet security.

The participants have been selected so as to provide a very broad sample of the Commonwealth's Internet presence: some very large departments, some small agencies, some with significant data holdings containing personal information on individuals and others with data holdings not containing personal information, some with Internet sites which primarily deliver information and others that are more transactional or interactive.

ANAO is working with the Defence Signals Directorate (DSD) in the conduct of the audit and fieldwork is currently under way. As part of the audit discussions, we proposed to NOIE that they needed a simple method of communicating to agency managers what they must do to address internet security issues. As a result, NOIE and DSD decided to develop a suitable checklist which will be included in our Guide and is also now available on NOIE's website.

We expect to provide a detailed technical report to each of the agencies involved and then aggregate the audit findings across the ten agencies, seeking trends and significant messages for inclusion in a public report scheduled for the second half of 2001.

Compliance guidelines

The National Office for the Information Economy wrote to agencies in February 2001 advising of new compliance guidelines to apply to agencies from March 2001. These arrangements include

- CEOs formally warranting that their agencies comply with Commonwealth Security guidelines;

- an enhanced online incident reporting system;

- agencies reporting their online Web security compliance levels as part of 6 monthly reporting to NOIE; and

- a requirement for non-government service providers involved in online service delivery for the Commonwealth to comply with Commonwealth online security standards.

Fraud Control audits

The ANAO has recently undertaken a survey of fraud control arrangements across the APS and a number of agency specific fraud control audits[32]. At the completion of the audits in progress, and of those approved but not started, the ANAO will arrange for the preparation of a Better Practice Guide on Fraud Control. I should note the Commonwealth Law Enforcement Board's 'Commonwealth Fraud Investigations Standards Package' which provides a set of best practice standards for fraud case handling. The package incorporates fraud investigation standards, best practice model procedures and quality assurance review guidelines.[33]

The fraud survey was conducted using a questionnaire designed with the assistance of the Australian Bureau of Statistics and was sent to 150 agencies.[34] Responses were received from 125 agencies. The survey raised some interesting issues concerning the level and distribution of fraud committed against Commonwealth agencies.

The most frequently occurring internal fraud was the inappropriate use of Commonwealth petty cash and other negotiable instruments, such as cheques, cab charges and purchase orders. Improper use of Commonwealth property and the inappropriate use of travel funds were also common. The most frequent form of external fraud was inappropriate claims for benefits and payments, which also cost the Commonwealth the most in cash terms.[35]

Commonwealth agencies have not ignored this substantial and potentially growing level of fraud. The ANAO concluded from the survey results that the majority of agencies had a framework in place that contained key elements for effectively preventing and dealing with fraud in line with Commonwealth policy. Ironically, agencies that experienced the most fraud tended to be the ones with comprehensive fraud control systems in place. One question is whether such systems simply exposed the extent of fraud being perpetrated. However, a significant proportion of agencies lack appropriate fraud control arrangements. For example:

- one-third of agencies had not undertaken a risk assessment within the last two years;

- more than one quarter lacked either a fraud control policy or a fraud control plan, and in some cases both; moreover, some of the plans that did exist had significant weaknesses; and

- one-third of agencies did not have a system for staff to report fraud, and a much higher proportion lacked systems to encourage the community to report fraud. [36]

It has to be said that weak internal controls provide an environment that increases the risk of fraud and undermines confidence in an organisation. There are signs, signals and patterns of behaviour indicating fraud such as:

- weak management that fails to enforce existing controls, supervises the control process inadequately, and/or fails to act on fraud; and

- loose internal controls with inadequate separation of duties involving cash management, inventory, purchasing/contracting and payments systems which allow the perpetrator to commit fraud.[37]

The agency specific audit of the ATO similarly found that outsourcing of information technology functions had increased the risk of fraud, in particular because contractor staff have less exposure to fraud prevention, education and awareness material that ATO employees.[38] The ATO has established a framework to assess the effectiveness of its fraud and ethics awareness training program. The framework is based on regular assessment by an external consultant of the ATO staffs' fraud control knowledge. The audit found that staff knowledge had increased from 40 per cent in 1998 (prior to the training program) to 72 per cent following the program in late 1999.[39] The ATO was also not able to provide evidence that the IT Security Section had monitored outsourced contractors' activity to ensure compliance with taxpayer data security provisions of its IT outsourcing contracts.[40]

The agency specific audit of the Department of Health and Aged Care (DHAC) noted that:

> *the department has established a number of specialist units to provide assistance and support to program areas in relation to various risks identified within the department, including, among other things, the loss and misuse of public funds and resources through fraud and other means. For example:*
>
> - *the Protective Security Section is responsible for managing physical security within the department, including matters of theft;*
>
> - *the Systems Security Team is a newly established unit created to manage DHAC's new information technology (IT) outcourcing contract;*
>
> - *the Procurement Support Unit (PSU) assists compliance with Commonwealth and departmental requirements by providing advice and guidance to officers involved in procurement activities; and*
>
> - *the Contracts, Tendering and Grants Advisory Unit (CTGAU) provides advice and guidance to officers involved in these activities to assist compliance and develop better practices for the department. This unit has an important role in assisting programs to better manage the different risks associated with increased outsourcing of service delivery by DHAC.*[41]

A persistent concern in agencies that have outsourced aspects of fraud control has been the non-availability of APS staff with the necessary skills and experience to manage and monitor purchaser/provider relationships.

A recent paper by the Attorney-General's Department commented on the changing nature of fraud as follows:

> *The rapid development and use of new technologies, together with increased globalisation of markets and financial systems, and changing business practices in the public and private sectors provide new opportunities for criminal exploitation.*[42]

The ANAO is interested in monitoring and supporting the ability of the APS to respond to the threat of fraud both because it is part of our legislative mandate to provide assurance about the effective management of resources and also because we seek to improve public administration through the identification and dissemination of better practices. The key is to implement effective, tailored, risk-based corporate governance arrangements.[43]

Again the message comes back to the issue of holistic risk management. The convergence of recommendations in all of these examples of audits reflects a focus on improving agency risk management.

In this particular context, I note that the requirements for management to establish and maintain policies and procedures that manage the risk of fraud, and on auditors to oversight such arrangements, are to be reinforced at the international level shortly. Action is underway through the International Federation of Accountants (IFAC) to tighten the International Standard of Auditing (ISA) 240 on fraud and error, with an expectation that draft guidelines, presently released for comment by accountants, auditors and managers, will be adopted as a global auditing standard by the end of this year. While the existing standard provides guidance to auditors as to how to treat fraud and error when they detect it, the revised standard will require auditors and, most importantly, management of entities, to take a more proactive role in both prevention and detection.

Specifically, under the proposed new standard:

- *Auditors will be required to quiz managers and boards of directors about what systems they have to detect fraud and glaring errors.*

- *Auditors will also need to check whether incorrect statements in the company books, including omissions of amounts and disclosures, are simply honest mistakes.*

- *Businesses will not only have to notify auditors, in writing of any fraud or suspicious activity; they will also be required to produce any financial statements that turn out to be incorrect and that management claimed were immaterial.*

- *Auditors will be required to pass these details on to those in charge of governance at the company that is being audited.* [44]

In putting out the revised standard for comment, the Chairman of IFAC's International Auditing Practice Committee, Mr Robert Roussey, made the following apposite points that I certainly agree with, as the CEO of an audit practice. I am sure those who support best practice in corporate governance arrangements would also endorse them:

- *It is the responsibility of management to establish and maintain policies and procedures that would contribute to the orderly and efficient conduct of the entity's business.*

- *This responsibility includes implementing and ensuring the continued operation of accounting and internal control systems which are designed to prevent and detect fraud and error.*

- *Further, it is the responsibility of those charged with governance to ensure, through oversight of management, that these systems are in place.*[45]

Personnel vetting - audit in progress

A protective security audit of procedures for security clearances and vetting is currently being undertaken across a number of agencies.

The evaluation criteria for this audit include:

- agency personnel security framework reflects Commonwealth policy and management best practice,

- recruitment processes and pre-employment checks are consistent with personnel security requirements

- the vetting process is effective, adequately documented, and the assessment is appropriate to the agency risk environment, and

- security clearance files are complete and records management and maintenance is efficient and complies with security and privacy principles.

Agencies involved in this audit include some that undertake the vetting and clearance processes in-house and some that outsource parts of the process.

As the audit is still in progress there are obviously no findings to discuss. However it is timely to consider the influences on agencies and the clearance process. Some agencies are still coming out of the influence of the Olympic games held in Sydney last year. The workload imposed by this event has put considerable pressure on the clearance and vetting process. Other agencies face the challenges brought about by outsourcing and ensuring that staff of contractors are subject to the same standards for clearance as are applied to employees of the APS.

5. CONCLUDING REMARKS

Protective security is a central element of public sector focus and Parliamentary concern. It is now generally recognised as an important element of agency risk management. Agencies are operating in more complicated environments and the issues with which they have to deal seem to have become increasingly more complex. The nature and level of risks and security exposures reflect such an environment.

The Commonwealth Protective Security Manual has been a constant source of guidance over many years. While the 2000 manual has only just been released, there are already plans in place to update parts of it to ensure it continues to meet the needs of agencies. However, as the Manual states, regardless of an agency's functions or security concerns, the central messages for managing security risks remain the same:

- security risk management is everyone's business;
- risk management, including security risk management is part of day-to-day business; and
- the process for managing security risk is logical and systematic, and should become a habit.[46]

The impact of information technology and the widespread availability of the Internet impose continuing challenges on agencies. The environment of devolved accountability and outsourcing simply adds to the task of ensuring agencies meet the protective security requirements. A particular problem is emerging with greater involvement of the private sector in public sector activities.

Sometimes access will be required to private sector premises particularly where Government assets, including information are involved. This cannot be a 'grace and favour' arrangement and needs at least the force of suitable contract clauses, if not a legislative requirement. No one wants to resort to precepts or subpoenas to obtain adequate access for public accountability purposes, including security concerns. Unfortunately, inquiries by Public Accounts Committees have revealed that, often, refusal to provide access originates more from public servants than from private sector firms, notably on matters classified as commercial-in-confidence. It is hoped that such action is more about perceptions of proper process, even if sometimes misguided, than about avoiding personal accountability.

Auditors have an important role in ensuring that, in circumstances where government services are being provided by the private sector, public sector accountability is not circumvented or reduced because of agency apathy, inadequate contractual drafting and/or differing standards of record-keeping and accountability in the private sector.

Agencies that continue, and indeed expand, the application of holistic risk management strategies and practices will be well placed to continue to meet the challenges ahead. I am reminded of that often quoted observation by the economist, John Maynard Keynes:

> *The greatest difficulty lies not in persuading people to accept new ideas, but in persuading them to abandon old ones.*

NOTES AND REFERENCES

[1] Attorney-General's Department 2000. *Commonwealth Protective Security Manual 2000*. Part A, Canberra, October, p. A5 (para. 1.2).

[2] Barrett Pat 1995. *The Role of Auditing in Promoting Security Awareness and Best Practice*. Address to the Security in Government 1995 Conference, Canberra, 2 November.

[3] Commonwealth Protective Security Manual 2000. Op.cit., p. B12 (para 4.4).

[4] Standards Australia 1995 Risk Management Australia/New Zealand Standard 4360, Standards Association of Australia, Sydney.

[5] Barrett Pat 2000. *The Compatibility of Risk Management and the Survival of Accountability in the Public Sector Environment*, November, p. 12.

[6] Ibid., p. 1.

[7] Barrett Pat 2001, *Risk management in the Australian Public Service Today and Tomorrow*. Presentation at launch of the Australasian Risk Management Unit at Monash University February, p. 4.

[8] Mulgan R 1997, *Contracting Out and Accountability*, Discussion paper 51, Graduate Public Policy Program Australian National University abstract.

[9] Government Online - *A Strategy for the Future* - Media Release 6 April 2000.

[10] Two papers were requested for discussion as follows:

Hayward Ken The Hon. 2001. *Retention of Corporate Memory and Skills in the Public Service - Is the public sector losing its minds.* 6th Biennial Conference of the Australasian Council of Public Accounts Committees, Canberra, 6 February.

Barrett Pat 2001. *Retention of Corporate Memory and Skills in the Public Service - More than survival in the new millennium*. 6th Biennial Conference of the Australasian Council of Public Accounts Committees, Canberra, 6 February.

[11] Office of Government Information Technology 1998, *Government Online – GATEKEEPER – A strategy for public key technology use in Government*, OGIT, Canberra.

[12] Commonwealth Protective Security Manual 2000, Op.cit. p. A6 (para 1.6).

[13] Ibid., p. A6 (para 1.5).

[14] Ibid., p. A18 (para 5.4).

[15] FMA Act 1997 Part 7.

[16] Barrett Pat 2000. *What's New in Corporate Governance*, Presentation to the Annual Congress of CPA Australia, Adelaide, 17 November, p. 18.

[17] Barrett Pat 1995. *The Role of Auditing in Promoting Security Awareness and Best Practice*, Op.cit., p. 24.

[18] The South Australian Auditor-General noted in his report for the year ended 30 June 2000 to the House of Assembly, fourth session, forty-ninth Parliament (Part A Audit Overview p. 205) tabled on 4 October 2000 that:

'It is essential that the private sector provides considering projects involving the storage, processing and security of government information and systems, be advised at an early stage of both government agency and Auditor-General rights in regard to access and audit. This matter requires due contractual and legal consideration by the Government and its agencies to ensure the adequacy of safeguards over the security, integrity and control of government information and processes, and to accommodate the Auditor-General's statutory audit responsibilities.'

19 The issue was given particular prominence in ANAO Report No.22 1992-93 *New Submarine Project*, ANAO Report No.31 1994-95 *Defence Contracting*, Joint Committee of Public Accounts, Report 337 *A Focus On Accountability: Review of Auditor-General's Reports*, ANAO Report No.34 1997-98, *New Submarine Project* and Joint Committee of Public Accounts and Audit Report 368, *Review of Audit Report No. 34, 1997-98, New Submarine Project Department of Defence.*

20 Joint Committee of Public Accounts and Audit 1999, *'Review of Audit Report No. 34, 1997-98, New Submarine Project Department of Defence'*. Report 368, June, p. xiv:

'***Recommendation 5:*** *The Committee recommends that the Minister for Finance make legislative provision, either through amendment of the Auditor-General Act or the Finance Minister's Orders, to enable the Auditor-General to access the premises of a contractor for the purpose of inspecting and copying documentation and records directly related to a Commonwealth contract, and to inspect any Commonwealth assets held on the premises of the contractor, where such access is, in the opinion of the Auditor-General, required to assist in the performance of an Auditor-General function. (paragraph 6.20).'*

21 Government response to Recommendation 5 of the 368th Report of the Joint Committee of Public Accounts and Audit : Review of Audit Report No. 34 1997-98, New Submarine Project - Department of Defence. Letter from the Prime Minister to the Minister for Finance and Administration dated 12 August 2000.

22 Ibid.

23 Commonwealth Protective Security Manual 2000, Op.cit., p. F45 (para 6.19).

24 Nichols, George. 1998, Personal correspondence with the Auditor-General dated 12 December.

25 Gilbert Mike, Pettigrew Ian, and Salt Nigel 2000. *The Impact of IT on accountability and audit*, UK National Audit Office Paper. ATAX Conference, Sydney 28-29 April, p. i.

26 National Archives of Australia 2000, *Archives heralds the new stone age*, Memento, Number 14, May, pp. 1, 10.

27 Barrett, P. 2000, official correspondence to the Director-General, National Archives of Australia, 4 May.

28 ibid., p. 19.

29 Van Dijk, Sandra, and Mills, Kelly. 2000, *Deleting email illegal warns archive director*, Computerworld, 9 October, pp 1 and 6.

30 Stuckey, Steve, 2000 *Digital Deluge May Prompt Illegal Acts*, Letter to the Editor, Computerworld, 9 October, p16.

31 Levitt, Arthur, Chairman US Securities and Exchange Commission, 2000, Address Washington 10 May.

32. Audits have been completed at (former) Department of Employment, Education, Training and Youth Affairs (DEETYA), the Department of Industry, Science and Resources (ISR), the

Department of Health and Aged Care (DHAC), the Australian Taxation Office (ATO), and the Department of Defence Audits are in progress at the Department of Family and Community Services (FaCS) and Centrelink Audits are approved to be undertaken at the Department of Foreign Affairs and Trade and Agriculture, Forestry and Fisheries Australia and Veterans'Affairs.

[33] Commonwealth Protective Security Manual 2000, Op.cit., p. G20 (paras 4.20 to 4.24).

[34] ANAO Report No. 47 1999-2000, *Survey of Fraud Control Arrangements in APS Agencies*, ANAO Canberra, 20 June.

[35] Thurley A 2001, *Evaluating the Results of the ANAO reports on Fraud Control.* Presentation to IIR Conference on Fraud Control, Sydney, 15-16 February, p. 5.

[36] Ibid., pp. 5-6.

[37] Falwider D.G 1999, *Recognizing Fraud Indicators*, International Journal of Government Auditing, Vol. 26, No. 2, April, p. 13.

[38] ANAO Report No. 16, 2000-2001, *Australian Taxation Office Internal Fraud Control Arrangements*, ANAO Canberra, 29 November, p. 20.

[39] Ibid., p. 19.

[40] Ibid., p. 20.

[41] ANAO Report No. 6, 2000-2001, *Fraud Control Arrangements in the Department of Health and Aged Care*. ANAO, Canberra, 23 August, p. 28.

[42] Department of the Attorney-General 2000, *The Changing Nature of Fraud in Australia*, Office of Strategic Crime Assessments, 25 August.

[43] Thurley A 2001. Op.cit., pp. 12-13.

[44] Gettler, L. 2000, *New rules to put heat on fraud*, The Age, 15 April, (Business p. 2).

[45] Ibid.

[46] Commonwealth Protective Security Manual 2000. Op.cit., p. B6 (para 1.6).