AUSTRALIAN NATIONAL AUDIT OFFICE

Conference on 'Surviving the Year 2000 Computer Crisis', Canberra

Audit – The Best Management Tool in Year 2000 Resolution

21 August 1997

Pat Barrett
Auditor-General for Australia

Australian National Audit Office

I. Introduction

Thank you for inviting me to address this conference. My objective is to create an appropriate climate of urgency about the Year 2000 computing problem. In doing so, I am acutely aware of the amount of hyperbole about this issue including legal imperatives and pitfalls. However, I do not wish to traffic in doomsday scenarios or participate in a scare campaign. Nevertheless, there is an imperative for all of us to 'know what we do not know' in connection with this particular problem. We will also do so by taking a systematic agency-wide approach to identifying all the issues involved which can be assisted by a more broadly based focus.

I want to convey a number of key "take home" messages to senior managers of Commonwealth agencies at the outset as follows:

the Year 2000 date field changeover is predominantly a business problem with potentially significant adverse implications for Commonwealth agencies and their stakeholders;

the problem is not just about information technology (IT), or computers, or software (although all of these are business inputs which are 'at risk' of Year 2000 related failure and are basically the thrust of this conference);

as with most other business problems, the issues involved are fundamentally about ***corporate governance*** including the application of ***risk management*** disciplines and client service delivery - in other words, the question is primarily about how organisations act to ensure business continuity and protect the interests of all their stakeholders (these matters will be amplified later in the address) ;

safeguarding business continuity will require the identification, in a broad risk management context, of the organisation's 'business critical systems' and an assessment of the extent of the Year 2000 exposure of these systems and its likely impact on the achievement of core business outcomes, and possibly even on the continued viability of the organisation;

we are running out of time - the longer organisations delay, the more they will be trapped into 'band-aid' solutions and risks for their functions, staff, other stakeholders and clients; and finally,

the Year 2000 problems can be resolved satisfactorily provided they are accepted as issues to be addressed by the <u>whole</u> organisation as a

matter of urgency. As well, it could be possible that such a focus will provide agencies with options to turn a survival imperative into business opportunities by coupling Year 2000 compliance activity with business process re-design to achieve better outcomes with more efficient and effective management processes.

This address is basically in three parts. The first underlines the importance of taking a whole-of-business approach to the problem. The second reinforces this view by indicating how such problems can be dealt with effectively through an integrated corporate governance framework which has a robust and systematic application of risk management principles. The third looks at the audit contribution, particularly by the Australian National Audit Office (ANAO) in its current audit of this topic, and indicates some lessons learnt from other public sectors through audit work. I conclude with some summary observations.

II. A Whole-of-Business Approach

A message we frequently hear about the Year 2000 Computing Problem, and which needs to be strongly reinforced, is that it is ***not*** simply an *information technology*, or *IT* problem. Rather, it ***is*** a *whole of business*problem, with potential ramifications which go well beyond immediate impacts upon particular business systems or processes and which places at risk the credibility and, indeed, the viability of individual businesses and organisations. Put simply, organisations which have not taken steps to identify their Year 2000 exposures and implement strategies to minimise the likelihood of Year 2000 compliance failure run the risk of an inability to deliver results. (For this reason, the title of the Conference could well have been "Surviving the Year 2000 ***Business*** Crisis").

Furthermore, if we extrapolate the consequences of Year 2000 failure for individual enterprises to broad industry sectors and the national economy, it becomes clear that the Year 2000 problem has much wider implications. Certainly, the public sector is not immune to the Year 2000 problem, although, for a variety of reasons, the public sector generally - both here in Australia and abroad - appears to have been slower to acknowledge the problem and mobilise the necessary resources to address its risk exposures. Among the possible reasons for this are that the business drivers of the public and private sectors are fundamentally different and that there is a perception that the private sector will ‘fix it’.

The public sector lacks the focus and financial imperative of the profit motive. As well, public sector equivalents of private sector accountability to shareholders for prudential and fiduciary management are still evolving.

Performance management with its attendant disciplines of targets, performance measures and assessments, benchmarking, monitoring and evaluation is only gradually being developed in most public sectors. Moreover, the consequences of lack of action do not seem to achieve the same status or attention as those where errors are made, despite the high profile given to the need for effective risk management in the public sector in recent years.

The fact is that public sector organisations ***are*** subject to Year 2000 risks with potentially adverse consequences for program outcomes. These risks may be exacerbated by the absence of timely action, an inability to compete effectively for a shrinking pool of (increasingly expensive) specialist services, and by deficiencies in corporate governance structures and risk management activities. Historically, many public organisations have to a considerable extent been shielded from the vicissitudes of market and economic forces by their monopoly on what were regarded as "public functions". The staffing, resources and functions of public sector organisations might expand or contract around the margins but their core mandate has been reasonably solid and certain. However, as we all are aware, this situation is changing with privatisation, commercialisation and outsourcing with the requirement, at the Federal level, to market test all our activities and/or at least ask the question as to whether they need to be undertaken within the public sector or not.

In the current environment virtually everything public sector organisations do is considered to be contestable, and what were once considered to be "natural monopolies" are increasingly under challenge. The public sector over the last few years has had to seriously confront the performance imperative. This is about producing mandated public outcomes economically, efficiently and effectively, and about putting in place the necessary management information systems to measure and demonstrate performance. The Year 2000 problem places the achievement of mandated public outcomes at risk. If public sector organisations fail to deliver mandated programs, services and outcomes, it is quite likely that alternative means of delivery would be considered.

Having said that, it is important to acknowledge that the potential impacts of Year 2000 compliance failure will be unevenly distributed, both between and within organisations. Just as differential effects are anticipated for small, medium and large businesses in the private sector, we might expect to see differential impacts across small, medium and large agencies in the public sector. For some public sector agencies, the Year 2000 problem may pose negligible risks to the community, clients or the Commonwealth, even in the event of some computing or system failure. For others, the risks may be significant and the effects potentially catastrophic. Some agencies may be able to cope with the failure of some business systems for a period as long as their core systems continue to be operational. Nevertheless in ***all*** cases, prudent management requires that senior managers take steps to:

identify all foreseeable and avoidable risks;

assess the potential impacts of any possible Year 2000-related failure(s); and

develop and implement strategies to eliminate sources of risk that are within the agency's control, minimise exposure to risks that are outside the agency's control, and have contingency plans to deal with failure scenarios including setting clear priorities for action and identifying resource implications.

Possible Barriers to a Whole-of-Business Perspective

There is a tendency in some organisations to 'compartmentalise' responsibility for their constituent functions, processes, inputs and outputs. This can lead to the creation of individual 'fiefdoms' which are defended on the grounds of devolution of authority and management flexibility. Unfortunately, one result may be the erection of barriers that prevent the organisation from taking a 'whole of business' perspective on a variety of business problems at the corporate level and can leave it unnecessarily exposed to risks that are not identified, only partially dealt with, or involve many so-called solutions that duplicate, overlap or simply waste resources. Anecdotal evidence of 'compartmentalisation' exacerbating risk is found in the reported extent to which the Year 2000 problem has been considered by some senior managers as being primarily an 'IT problem' which has marginal relevance to the wider business. This view is somewhat surprising as, for many agencies, IT is endemic to the delivery of their core functions.

It is possible that the above view has been reinforced by the fact that the earliest and most comprehensive coverage of the Year 2000 problem occurred in the information technology literature and, more recently, on the internet. These media are predominantly accessed by IT specialists and are unlikely to be read by non-IT senior managers. Consider this alongside the findings of a recent survey (conducted by Korn/Ferry International in June 1996) that Chief Information Officers (CIOs) often feel functionally and culturally isolated within their organisations and report that they have little impact on strategic business decisions[1]. However, I also note the recent warning by the President of the Australian Computer Society to his members about failing to take action in respect of the Year 2000 problem will be 'in breach of the ACS Code of Professional Conduct and Practice'. He went on to say that:

IT professionals have an obligation to assess and report the extent of the problem in all systems for which they are responsible.[2]

Taken together, these observations suggest a number of issues which senior managers should take into account when thinking about the Year 2000 problem:

first, the IT specialists in your organisation are likely to have a strong base level of knowledge about technical aspects of the Year 2000 problem and its potential implications for key business systems;

second, because of the problems of functional compartmentalisation in organisations, senior managers cannot simply assume that IT specialists have taken a whole-of-business perspective when assessing the scale or potential impacts of your Year 2000 exposure;

third, a narrow IT focus on the Year 2000 problem not only exposes the organisation to foreseeable (and avoidable) risk, it may also prevent organisations from recognising important strategic opportunities associated with business process re-design; and

finally, senior managers should not conclude that if their organisation has outsourced the management and delivery of its IT services, they have outsourced the Year 2000 problem. The ultimate responsibility and accountability for taking appropriate action to minimise exposure to related risks continues to reside with the agency. As the Ombudsman has pointed out, on more than one occasion, responsibility and accountability cannot be outsourced.

In short, the Year 2000 problem cannot be ignored or ‘got rid of’. It is a business risk and it needs to be squarely and effectively addressed as such. It is incumbent, therefore, on senior public sector managers to become informed about the problem and to take a direct and active interest in the progress of Year 2000 planning and implementation activities in their agencies even if they think their activities are not affected. As I am sure you will recognise, saying after the fact that "I was not aware of the problem", or "I was not sufficiently advised of the possible risks", or "responsibility for resolution of the problem was delegated to the IT functional area", will not provide a sufficient defence in the event of any Year 2000-related failures which lead to adverse financial, stakeholder or community impacts. It is simply a case of ‘forewarned is forearmed’.

The key to taking a wider perspective on the Year 2000 problem is to embrace it as a corporate governance problem. Organisations which have in

place an integrated suite of governance structures which cascade upwards to support informed strategic management should be well placed to deal with the complexities of the Year 2000 problem. These are the kinds of organisations which are most likely to have a holistic appreciation of their operating and business environments. They are better able to exercise timely strategic thinking and effectively harness all elements of their organisations to tackle business problems in a coherent way.

III. Year 2000 as a Corporate Governance Issue

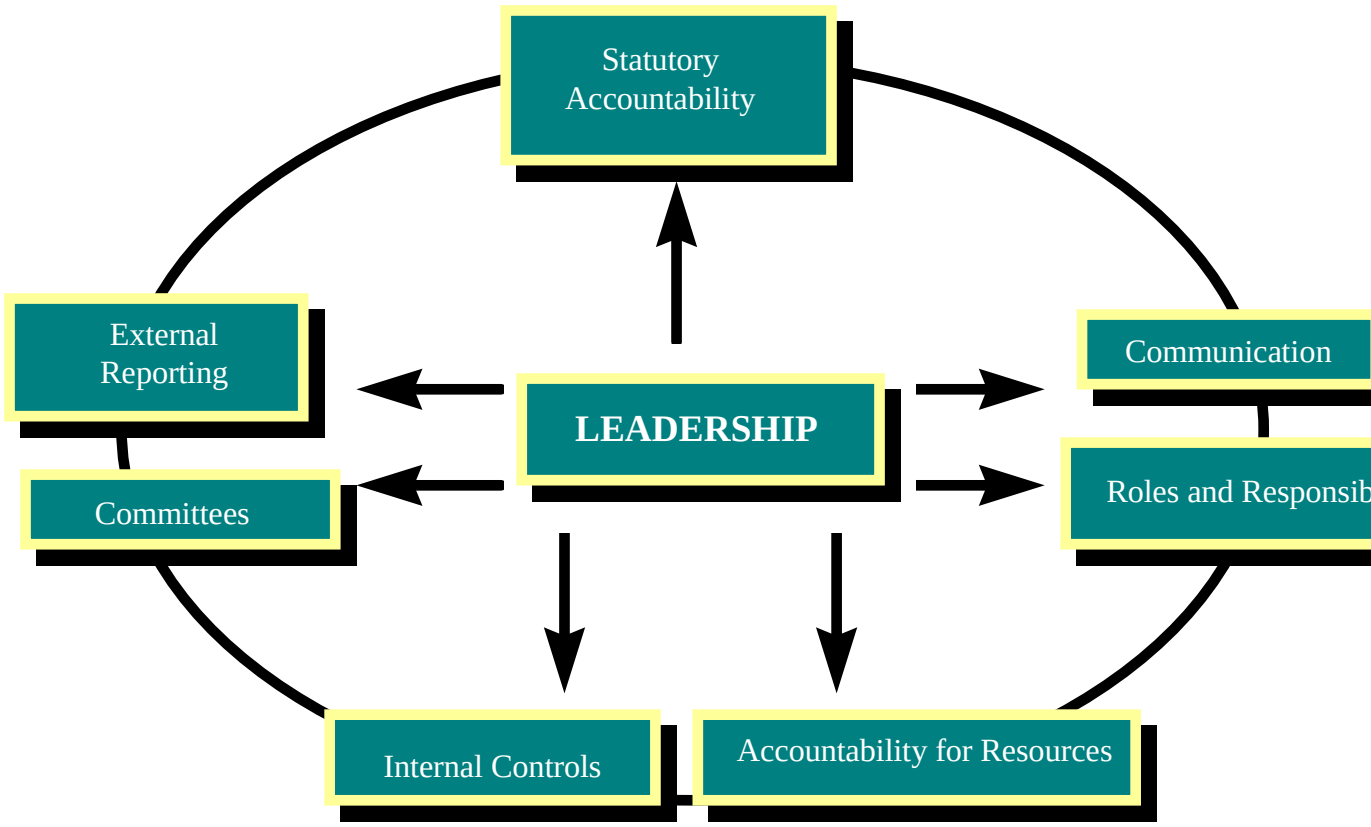
Many - if not most - people here today will have encountered the term 'corporate governance'. However, it would be unusual, in my experience, if everyone who has heard the term has a uniform understanding about what it means. In general terms, corporate governance is about accountability for an organisation's performance and focuses on the integration of the various processes used to direct and manage the business and affairs of an organisation with the objective of balancing:

the attainment of corporate objectives;

the alignment of corporate behaviour with the expectations of the community; and

accountability to recognised stakeholders.

The main elements of corporate governance are depicted in the following figure:



Corporate governance requires senior management to put into place an integrated system of controls to monitor risks; safeguard the organisation's resources, functions and assets; and provide reasonable assurance of:

cost effective and efficient operations;

internal and external financial integrity and validity;

compliance with laws and regulations; and

confidence in the integrity, credibility, viability and future prospects of the organisation.

There is a real risk that such assurances might not be able to be provided by organisations which cannot adequately show how they have addressed the Year 2000 problem. In this regard, it important to recognise that under the proposed new Commonwealth financial management legislation the Chief Executive Officer (CEO) of a public sector agency will have a clear legal liability for its performance. By extension, it is the duty of the CEO to identify

the business risks associated with the Year 2000 problem and implement effective strategies to mitigate those risks.

The necessary assurance for the CEO, in the above respects, can be provided by a robust corporate governance framework which is understood and implemented at all levels of the organisation. While such assurance is necessary to fulfil accountability requirements, the real gains from an effectively integrated framework come from the opportunities provided to improve performance. In short, management is in a far better position to deal with difficult issues such as the Year 2000 problem within such a framework.

I hope you had an opportunity to read one of the ANAO's most recent publications, Principles for Core Public Sector Corporate Governance[3]. The Principles identified fall under eight broad headings, and, while they have been expressed in more generic terms in the publication, they can be re-expressed in terms of the Year 2000 problem. As such, I suggest that the eight Principles provide a useful template for agencies' approach to the Year 2000 problem. Let me illustrate as follows:

The first principle relates to **leadership**. This means that senior management need to have a clear understanding of the implications of the Year 2000 problem for their organisation and the extent to which it could impact on each of the major elements of corporate governance in the organisation. Senior management also need to be fully apprised of risks associated with the Year 2000 problem and act to ensure appropriate action to minimise such risks;

Principle two relates to **statutory accountability**. Among the risks associated with the Year 2000 problem is the risk that agencies might be placed in breach of applicable statutes and regulations and relevant guidelines and statements of sound administrative and financial management practice. As a result, senior management need to ensure that statutory and regulatory compliance of their agencies is not compromised by Year 2000-related failures;

Principle three is concerned with c**ommunication with clients and other stakeholders**. Agencies need to identify the clients and stakeholders whose interests and needs might be affected by the Year 2000 problem and establish clear channels of communication to provide appropriate assurance and to seek information which might be instrumental in reducing risk and/or adverse impacts. In this context, stakeholders should be taken to include the Parliament, Ministers, employees and third party providers of services or other inputs and the interests of Australian citizens as clients;

Principle four is about **roles and responsibilities**. It is essential that agencies clearly define the division of responsibilities for managing aspects of Year 2000 work within a framework of strategic control. Senior management should ensure that each element of corporate governance in the agency has access to appropriate advice and resources to enable a realistic appraisal of their respective risk exposures; management and implementation processes should be clearly documented and the effective coordination and delivery of information and related technology ensured;

Principle five relates to **accountability for agency resources**. It is clearly essential to have an early assessment of the resource implications of any action needed to deal with the Year 2000 problem as well as to establish priorities. Senior management should ensure, for example, that Year 2000-related risks to employee health and safety are comprehensively addressed and that risks to the value and service potential of assets are minimised;

Principle six relates to the use of **internal controls**. It is important that Year 2000 related activity is subject to internal controls within the context of the agency's corporate plan or business charter. It is essential to ensure the provision of timely and appropriate management information to enable business managers to appraise Year 2000-related risks and acquit actions to reduce their risk exposure. The internal audit function should also be a key element of the agency's Year 2000 assurance mechanisms;

Principle seven pertains to the role of **committees**. The management and coordination of Year 2000-related activities could be maximised through the utilisation of the committee structures established to maximise effective governance of the agency. Care needs to be taken to promote effective linkages across business and/or administrative units and provide for independent external review of the systems of internal control used to address the Year 2000 problem; and

finally, principle eight refers to the role of **external reporting**. Agencies should ensure that timely, objective, balanced and readable information is available which provides assurance about the actions taken to minimise Year 2000 risks to stakeholders. This information should, at a minimum, be included in a statement of major corporate governance practices as part of the organisation's Annual Report.

As well, Senior management also needs to prepare for the possibility that, despite all reasonable efforts, their organisation's business systems may experience some level of Year 2000-related failure. Thus, contingency plans,

disaster recovery plans and business resumption plans are essential features of a responsible approach to the problem.

The Year 2000 Problem as an exercise in effective Risk Management

Risk management is an integral element of an organisation's corporate governance framework. As such it is central to an organisation's culture, involving all staff, and requires clear leadership and example from the top. Risk management requires that an organisation's decision-making be underpinned by:

a systematic approach to the identification of possible risk;

the analysis of the potential risk impacts;

the evaluation of strategies for the treatment of risk; and

monitoring risk minimisation strategies to allow for corrective action where necessary.

I acknowledge that it is not an easy task to identify, assess and prioritise risks. There is no substitute for doing the 'hard yards' when it comes to sound risk management. A major issue is how to convince management and staff that a systematic approach to risk is likely to result in the best corporate outcome. Contrary to bad press, process is important and, in this case, can yield real dividends in terms of outcomes achieved.

The Year 2000 problem has the potential to impact adversely on the level of assurance that can be provided to management, particularly in the control environment, as well as on the preparation of agency financial statements and the external audit opinion. The MAB/MIAC Guidelines for Managing Risk in the Australian Public Service (APS) state that:

> *'Risk arises out of **uncertainty**. It is the exposure to the possibility of such things as economic or financial loss or gain, physical damage, injury or delay, as a consequence of pursuing a particular course of action. The concept of risk has two elements, the **likelihood** of something happening and the **consequence** if it happens*.'[4]

Good corporate governance and good risk management require that all public sector organisations ask at least two questions in relation to the Year 2000 problem:

first, what is the likelihood of the organisation being affected by the Year 2000 problem? and

second, what will be the consequences of Year 2000-related systems failure?

Since prevention is better than cure, the key to the risk management of the Year 2000 problem is being proactive and well informed. Continued monitoring and review are necessary for the successful management of Year 2000-related risks because of the possibility that they may change over time both in terms of their nature and their relative significance, as may the mechanisms and tools to manage the Year 2000 risks efficiently and effectively. As with other sources of potential risk, constant vigilance is the price to be paid where there is a possible loss or less than satisfactory use of the public's resources. This also includes ongoing review of the resource costs involved, particularly in relation to the identified benefits.

The ANAO considers that the documentation of key risk management principles and management decisions is an essential element of risk management. Documentation should be sufficient to enable a decision on the design of a process to be reviewed and evaluated. From the perspective of an auditing organisation, and in view of the duties of senior management, there is a need for tangible evidence that the risk management process has been conducted properly. With this in mind, the key elements of a public sector agency's Year 2000 risk management strategy should be well documented in order to:

help ensure that the analysis has been done;

make it available for review;

ensure that it is communicated to staff and others involved in the processes or program so there is a shared understanding of directions and associated risk; and

ensure that it is available in defence of the organisation's decisions and/or of the particular program involved.

It may be useful at this point to outline briefly the six major steps that have been identified in the risk management process and their relevance to the Year 2000 problem:

Step one requires agencies to **establish the risk management context**. With respect to the Year 2000 problem, this means establishing the criteria by which it is decided whether a risk is acceptable or not. These criteria will form the basis for controls and management options and are fundamental to ranking risks. The establishment of risk criteria requires an analysis of those aspects of the organisation's operating, compliance and external environment which would be affected by the Year 2000 problem, such as its ability to fulfil statutory obligations; deliver programs and services; or provide financial assurance. The criteria may be indicative at first until analysis establishes the likely impact and the costs and benefits involved. As a result such criteria need to be constantly reviewed throughout the period until management is satisfied that there is no longer a Year 2000 problem created internally or externally.

Step two involves identification of the risks. This step requires a comprehensive examination of the Year 2000 problem in terms of:

- *possible sources of risk* (involving questions such as: 'will the agency be in breach of contractual or statutory obligations in the event of year 2000-related failure?'; 'what might be the social and political repercussions of any failure of key government functions such as payments or revenue collection?'; 'will the health and safety of employees or clients be placed at risk if building safety or environmental systems fail to operate?');
- *possible areas of risk impact* (involving questions such as: 'will the organisation's assets and resources be placed at risk through the failure of safety or security systems such as locking and monitoring devices, sprinklers, climate control systems or fire alarms?'; "what are the direct costs of fixing the problem and the indirect costs in terms of diverted effort and failure to achieve program outcomes?'; 'what are the potential impacts on people and the community of any failure in the delivery of programs and services?'; or 'what will be the impact on individual and corporate performance of any failure of core business systems?');
- *possible methods of identifying risks* (including through audit and inventory of IT and non-IT systems; surveys or questionnaires of key suppliers and vendors; examining local and overseas experience; and/or modelling and testing systems. I reiterate my earlier warning that we need to establish what we do not know about possible risks); and
- determining the *key questions to be asked in identifying risks* (including, 'who are the stakeholders and how will they be

affected? ‘when, where and how are the risks likely to occur?’; ‘what external and internal accountability mechanisms can be utilised to manage the risks?’; or ‘how reliable is the information used to assess the likelihood and impact of the risk?’);

Step three requires the **analysis of the risks** to assess the likelihood and consequences of each risk factor and to decide which risks will have the greatest potential effect (organisations may decide on the basis of a comprehensive analysis of risks and likely impacts that it is impracticable to repair or replace every affected business system or piece of equipment and opt to focus attention on business critical systems only);

Step four involves the **assessment and prioritisation of the risks**. This is about deciding whether risks are acceptable or unacceptable and then ranking the risks in terms of management priorities. (The prioritisation of risks needs to take into account the wider context of the risk, including: statutory requirements; legal obligations; the degree of control over each risk; and the impact, cost and benefits involved. On this basis, organisations might decide to use a ‘triage’ approach to their Year 2000 problem although quality and urgency would normally be integral to priority setting);

Step five, requires organisations to **treat the risk**. Among the options which might be considered for treating the risk are:

- *avoid the risk* by not proceeding with the activity that would incur the risk or choosing an alternative means of action that produces the same outcome (for example, by deciding not to add major new functionality to business systems which have not yet been made compliant);
- *reduce the level of risk* by reducing either the likelihood of occurrence or the consequences or both (for example, through the repair, retirement or replacement of affected systems and equipment and through management controls to minimise adverse consequences, such as contract conditions or contingency planning);
- *transfer the risk* by allocating responsibility to the party which can exercise the most effective control over the risk or by sharing some part of the consequences of the risk in an agreed manner. (Certainly, insurance for Year 2000 related failures is emerging but coverage will be premised on organisations having taken reasonable care to prevent the risk occurring and the premiums could well be beyond the resource capabilities of many government agencies. Also, as mentioned previously, outsourcing IT does not amount to the transferral of the responsibilities for risk); or

- *accept and retain the risks* in the organisation where they cannot be avoided, reduced or transferred, or where the cost to avoid or transfer the risk cannot be justified. (An example might be a non-critical business system which would not be cost-effective to repair or replace. Such a system might be allowed to remain in place until it fails to operate, after which a business decision can be taken about replacement or retirement).

Decisions about priority also involve an analysis of the significance of the at-risk activities and the likely costs of managing the risks. The latter requires a broader consideration than just the input costs of rectifying the problem. The analysis needs to also consider the potential costs of failure, in terms of the impact on stakeholders, legal liability, damage to property and assets and diminished accountability; and

finally, step six requires the on-going monitoring and review of the risks, the effectiveness of the risk management plan and the strategies and systems established to control the implementation of the risk treatment. Few risks remain static and in a volatile public sector environment agencies will need to be capable of responding to new sources of Year 2000 risk such as: administrative restructures, the transfer of functions and organisational amalgamations; requirements to implement new policies and programs and attendant business systems; the on-going out-sourcing of non-core functions and increasing levels of third party contracting; and, perhaps, the declining affordability of Year 2000 related services coupled with the leakage of IT expertise and corporate knowledge to the private sector.

I would again remind you that, at each stage of the risk management process, it is essential to document the manner in which risks were identified and quantified and the bases for all decisions taken. This is essential, not only for reasons of corporate accountability, but also in the event that the agency is required to defend its actions in the event of a failure causing harm or loss. The discipline involved in 'sign-offs' by responsible managers, to the CEO or to any Executive Board for proper and effective performance in relation to the various elements of corporate governance, reinforces the robustness and confidence promoted in the framework for all stakeholders. The discipline is indicative of good practice not least in the area of risk management.

IV. The Audit Contribution

The ANAO is a key element of the external accountability framework for Commonwealth agencies. In relation to the current audit of Commonwealth

Government agencies' Year 2000 preparedness, the ANAO is aiming to be in a position to:

- provide assurance to the Parliament and Parliamentary committees about Commonwealth agencies' progress;
- identify any gaps or deficiencies in corporate governance, risk management, planning and implementation in relation to the issue;
- identify the core elements of good practice which, if followed, would assist agencies with the management of the Year 2000 problem, particularly over the next two years.

As part of its audit role, the ANAO needs to understand, inter alia, the basis of public sector agencies' decisions in relation to their management of the Year 2000 problem. Auditors are not blessed with clairvoyance. We need information on how decisions are made. We therefore ask questions such as:

- were all relevant factors considered by the decision maker;
- was a fair, reasonable and transparent method used by the agency to reach a decision; and
- was the decision conveyed appropriately to relevant stakeholders?

Decision-makers should, desirably, identify and consider all relevant factors and develop a sound approach in arriving at any significant decision. What auditors do is to look for evidence that management functions in an efficient and defensible manner to ensure program objectives and performance requirements are met cost effectively. Put another way, we are primarily in the business of providing quality assurance about, and added value to, public administration. Particularly in this audit we should collectively contribute to this aim with benefits to all parties, including those not directly involved.

Scope and Progress of the Year 2000 Audit

The ANAO began its across portfolio performance audit of Commonwealth agencies' responses to the Year 2000 problem in January 1997. The purpose of the audit is to review agencies' approaches to achieving Year 2000 compliance, with a focus on planning, risk assessment and implementation activities. Among the aims of the audit are:

- raising agencies' awareness of the need to achieve Year 2000 compliance;

outlining the risks to the Commonwealth of any failure to achieve compliance; and

encouraging Commonwealth agencies to implement effective strategies to achieve compliance.

The audit is premised on the recognition that the Year 2000 problem presents a material risk to the Commonwealth which, if not adequately addressed, could have significant adverse impacts on the Australian community. It is concerned to address two broad questions:

first, what steps have Commonwealth agencies taken to assess and implement solutions for the Year 2000-related risks to their 'business critical' functions; and,

second, what are the possible risks to key government functions, such as revenue collection, the delivery of services, payments to beneficiaries, national security, law and order and health and safety?

These functions are provided through a diverse range of agencies, inter-organisational arrangements and business processes. Some Commonwealth agencies will be responsible for the delivery of multiple functions and will exhibit a high level of internal diversity in terms of core business systems and processes. This level of complexity introduces potentially high levels of risk, particularly when you consider the extent to which agencies' core business systems are directly dependent on IT-enabled processes, as I observed earlier.

When you add to the equation issues such as: legal liability for the safety of the public, clients and employees; reliance upon suppliers of key business inputs; the security of buildings and other assets; and the variety of other 'non-IT' Year 2000 issues, it becomes clear that this is not a business problem that can be neatly compartmentalised and relegated to the (CIO) to resolve.

The audit utilised a questionnaire survey of 73 Commonwealth budget-funded agencies selected on the basis of their size and the nature of their core functions. While the sample does not include every agency - such a task would be well beyond the bounds of a normal performance audit - I consider that the results will be representative of the broader Australian Public Service and will, therefore, be instructive for those agencies which did not participate in the survey. I have to add that the sample does not include Government Business Enterprises (GBEs), because under the present legislation, the Auditor-General does not have a mandate to conduct performance audits in GBEs unless requested to do so by the Parliament.

The questionnaire proceeds from the core assumption that the resolution of the Year 2000 problem requires a 'whole of business' approach. The whole of business approach assumes six threshold questions:

- will the Year 2000 impact the agency's customers and stakeholders?
- will the Year 2000 problem impact the agency's production of its products and services?
- does the agency have an experienced team working on the Year 2000 problem?
- is the Year 2000 problem being addressed at the appropriate level within the organisation?
- will all of the agency's business processes be able to function through the turn of the century and beyond? and
- is any of the technological infrastructure which supports the agency's business processes affected by the Year 2000 problem?

To provide reliable assurance in relation to any of these threshold questions, I consider that agencies would need to have conscientiously followed the corporate governance principles and risk management steps I described earlier. To answer any of these questions with certainty and authority requires a systematic analytical process and this process should be capable of being evidenced.

For example, if an agency responds that its clients and stakeholders will ***not*** be affected by the Year 2000 problem, I would then ask how the agency arrived at that conclusion. If the conclusion was reached by means other than a systematic analysis of the agency's possible Year 2000 risks in accordance with the risk management framework, I might conclude that the agency's assurances are of questionable merit. In contrast, if an agency responds that its clients and stakeholders ***will*** be affected, I would similarly expect to see the rationale for that judgement ***and*** obtain some idea of the approach proposed by the agency to minimise the chances of the risk occurring.

The questionnaire will be complemented by case studies in five agencies which provide critical government functions. These are:

- the Australian Taxation Office, in view of its key revenue collection function;
- the Commonwealth Services Delivery Agency, in view of its payments and program delivery functions;

the Department of Finance, in view of its responsibilities for the coordination of government resource management functions and its role in the payments system;

the Reserve Bank of Australia, in view of its role as an economic regulator and its role in the payments system; and

the Australian Maritime Safety Authority, in view of its role as a safety and environmental regulator.

The object of the case studies is to evidence their responses to the ANAO questionnaire and to explore the extent to which they have assessed and put into place strategies to minimise risks to their business-critical systems (especially those which might in turn compromise the delivery of critical government functions). The case studies will allow an enriched understanding of the way in which the Year 2000 problem might affect agencies' business and provide a greater level of insight into the identification, assessment and treatment of their risks. The case studies will undoubtedly illuminate some significant differences in risk exposure and approach, but they should also illustrate important commonalities and possible lessons for all of us.

As far as our analysis of the results of the questionnaire is concerned, it is early days yet. I am not in a position, therefore, to offer a view about the preparedness of the agencies in the sample. It would be fair to say that early indications suggest a high degree of variability within the sample, as one might expect. However, we have not yet pursued our analysis to the point of offering explanations for any observed variability. I would add that variability, in itself is not necessarily a bad sign. It suggests that agencies are located along a continuum of preparedness and this provides important opportunities for the better prepared to offer advice and assistance to the less well prepared. I consider that some form of strategic partnering between agencies could assist to overcome some of the resource and information gaps confronting agencies - particularly the smaller agencies which may have a lesser capacity to devote sufficient human and financial resources to the problem.

The ANAO plans to table its report in December 1997. You may be thinking "Isn't December too late for the results of this audit to have an impact?". Good question! My answer is that the audit has already had an impact. In the first instance, the questionnaire has achieved a response rate of close to 100 per cent, which I take to be an indicator of the level of interest in the issue on the part of many agencies. As well, it has created greater awareness and activity at management levels.

The questionnaire itself follows a logical pattern which, if used properly, provides an opportunity for agencies to self-assess their Year 2000 preparedness. Indeed, the ANAO has received feedback from a number of

agencies which suggests that the questionnaire has served as a catalyst for internal discussion and communication about the Year 2000 problem as well as providing some sign-posts to agencies about the range of issues they need to address. This is a useful outcome which points to our having met, in part, one of the key audit objectives of raising agencies' awareness of the need to achieve Year 2000 compliance.

We are well aware of the limitations of survey questionnaires even where relevant expertise has been extensively involved. It is important, therefore, to note that extensive consultation will be undertaken with each of the participating agencies, including the Office of Government Information Technology (OGIT), about the findings from the questionnaire and case studies as part of the report preparation. This will provide the opportunity, for example, to verify the ANAO's analysis, to provide clear signals to those agencies which appear to be less well prepared, and to promote key messages about what agencies need to be doing to provide necessary assurances about their actions to minimise their Year 2000 exposures. Thus, it is my expectation that the audit process, as opposed to the actual report, will have had a positive impact on agencies' preparedness for the millennium change.

I would like to add that throughout this audit the ANAO has worked closely with OGIT in order to maximise our respective efforts. This is not to say that the ANAO will not offer objective and balanced comment on the role played by central coordinating agencies such as OGIT, but it is indicative of a shared sense of 'mission' in terms of adding value to public administration and a mutual sensitivity to the challenges and demands being placed on Commonwealth public sector agencies. I use this opportunity to thank OGIT staff sincerely for their contribution as well as those in all the agencies covered by the survey.

Lessons from Other Jurisdictions

The design and implementation of this audit has taken into account Year 2000 planning and audit activity elsewhere in Australia and internationally. It is readily apparent that the Year 2000 problem is a matter of some interest to Government Audit Institutions in most States and a variety of work is under way. The issues facing State and Territory governments are similar, although given the States' greater role in direct service provision, the issues of client and community impacts may be much greater. The ANAO is constantly liaising with State and Territory colleagues and I expect that we will benefit from insight into each others' work in the period ahead.

The ANAO is also taking account of work being done overseas, principally by the General Accounting Office (GAO) in the United States and the National Audit Office (NAO) in the United Kingdom, both of which have published

broad guidelines about the approach they expect agencies to take to the Year 2000 problem in their respective jurisdictions. In February 1997, the GAO published the Year 2000 Computing Crisis: An Assessment Guide[5] which detailed a structured approach to Year 2000 conversion in five phases:

phase one is about ***Awareness*** and refers to the need to:

- define the Year 2000 problem;
- gain executive support and sponsorship;
- establish a year 2000 program team; and
- develop an overall strategy;

phase two is about ***Assessment*** and refers to the need to:

- identify core business areas and processes;
- inventory and analyse systems supporting the core business areas;
- prioritise conversion or replacement;
- develop contingency plans to handle data exchange issues, lack of data or bad data; and
- identify and secure the necessary resources;

phase three is about ***Renovation*** and refers to:

- the conversion, replacement or elimination of selected platforms, applications, data bases and utilities; and
- the modification of interfaces;

phase four is about ***Validation*** and refers to the need to:

- test, verify and validate converted or replaced platforms, applications, data bases and utilities; and
- test the performance, functionality and integration of converted or replaced platforms, applications, data bases, utilities and interfaces in an operational environment;

phase five is about ***Implementation*** and refers to:

- the implementation of converted or replaced platforms, applications, data bases, utilities and interfaces; and
- implementation of data exchange contingency plans, if necessary.

Furthermore, the GAO recommends that an agency's Year 2000 program be planned and managed as a single large information system development effort in which good management practices are promulgated and enforced at the program and project levels.

The NAO, in its May 1997 report Managing the Millennium Threat[6], made the following key findings in relation to government departments and agencies in the United Kingdom:

most are aware of the Year 2000 problem;

most are at the stage of auditing their systems;

four-fifths are confident that they will complete the work on time; and

it is not possible, at this stage, to estimate the costs with confidence.

The NAO notes that many government departments have not completed the audit of their systems, nor, in some cases, have they established who has legal liability for modifications. The report makes the point that:

> *…there is a need for managers at all levels to be aware that this is not just a technical issue, but one which can have a profound impact on the ability of the organisation to continue functioning in the next millennium.*[7]

The NAO outlines eight key stages of an action plan to ensure that all information systems can cope with the millennium. These are:

assign clear responsibility for Year 2000 compliance;

create an inventory of systems;

audit all systems for compliance by January 1997;

produce a prioritised list of systems requiring modification;

estimate costs;

finalise a prioritised, costed, timed program of action by October 1997;

manage the program to budget and time; and

test all modified systems by January 1999.

The NAO goes on to observe that a serious constraint is the shortage of suitably skilled staff in the community at large to manage the program and make modifications. The report also observes indications that the cost of employing suitably skilled people is rising as demand for their services increases.

V. Concluding Remarks

The Year 2000 problem is an issue that demands an effective risk management approach as part of good corporate governance. As I mentioned at the outset of my talk, time is running out, especially for those organisations which have not commenced the vital task of carrying out inventories of their Year 2000 affected business systems, let alone begun testing their business systems.

The problem extends way beyond the IT area, not the least into legal issues, the buildings we work in and the way we deliver our services. However, today we are focusing mainly on the IT issues. In that latter respect IT projects are notorious for exceeding their implementation time-frames, even with the best of management intentions. The potential scale and complexity of the Year 2000 problem greatly amplify the uncertainty that is usually associated with the staging of systems implementation. It is probably what we do not know that should create the greatest anxiety and attention.

The Year 2000 project may well be the most complex and demanding project many agencies have ever encountered. For example:

- many Year 2000 projects will require long lead times to allow for the testing and re-testing of systems;
- attaining a whole-of-business perspective on the problem may significantly challenge the existing culture of the organisation;
- superior risk assessment, project management and commercial skills are required to ensure that the project keeps to its time frames and to deal effectively with contractors and suppliers happily in a productive partnership; and
- because this is unfamiliar territory for all concerned, it will be difficult to anticipate all of the potential problems which may in fact change over time.

The ANAO fully appreciates that for many agencies the Year 2000 problem will not a be simple ‘quick fix’. We acknowledge the diversity of Government business and accept that different organisations will exhibit important differences in terms of their management culture, their operating environment, their capability to invest the required effort in resolving the Year 2000 problem and the appropriateness of particular solutions. Despite these differences, there are likely to be common lessons which will assist agencies to find their way through the Year 2000 maze. We are certainly not interested in, nor have the time for, reinvention of the wheel. There needs to be forums and other means of exchanging relevant experiences in the period ahead. We expect that OGIT will take a lead role in this respect.

As we can see from the work done by the GAO and the NAO, no matter how you cut the cloth, the basics remain fairly constant: agencies need to demonstrate executive awareness and sponsorship; they need to take complete stock of their business and operating environments; they need to have commenced a full inventory and audit of their systems; they need to have assessed their risks; and they need to put into place a sound program and project management structure to see their activities through to completion. Moreover, I trust that it will be apparent to you that this process describes nothing more and nothing less than the core corporate governance principles and the key steps underpinning risk management. This is not 'rocket science'. It is good management.

As I mentioned at the outset of my talk, one of the biggest risks for agencies lies in the Year 2000 problem being portrayed as a computer or information technology problem of little interest or relevance to senior management. I hope I have helped to convince you - if you needed convincing - that nothing could be further from the truth. The Year 2000 problem is a 'whole-of-business' problem which potentially affects every aspect of a company's or an agency's operations. It is not only a threat to organisations, it also has the potential to adversely impact on individuals and the community generally.

To the extent that the viability of Australian firms may be placed in jeopardy, there is also a potential for significant adverse effects on the international competitiveness of key industrial sectors and, by extension, the national economy. While the public sector's concerns are necessarily different to those of the private sector, there remains a risk that unless the Year 2000 problem is comprehensively addressed, we may see the failure of key government functions. This could entail economic and social costs which we, as a community, can ill afford.

Management also needs to recognise that this is not a problem which is exclusively internal to the organisation. In addition to the Year 2000 risks associated with the tools that support an organisation's productive processes, there are many sources of potential Year 2000 risk which are outside the immediate control of the organisation. Most organisations are dependent to some degree on suppliers of essential goods and services which are the key inputs into their productive processes. Others are dependent upon strategic linkages with other organisations. Through these dependencies and linkages organisations are vulnerable to third parties' failure to address the problem. From a risk management perspective, there is a simple axiom which provides a handy self-test for this situation:

if the risk is within your control, fix it; or

if the risk is outside your control, minimise it.

In the private sector, large firms - particularly in the banking and telecommunications sectors - are vigorously assessing the Year 2000 status of the range of companies and organisations which intersect with their business and developing contingency plans to cope with third party failure. It is my view that public sector entities should be doing likewise.

There is undoubtedly a degree of scepticism and even outright denial in some quarters that a problem exists. Equally, some of the repercussions of Year 2000 failure purveyed by the media are overstated at best, and irresponsible at worst (which, in turn fuels cynicism and uncertainty). I cannot overstress the need for public sector chief executives and managers to take personal responsibility for managing the risks to their organisations, stakeholders and clients posed by the Year 2000 problem. This is a foreseeable problem and one which is capable of being solved provided organisations act in a timely manner and apply sufficient resources to get effective results. In the end, a responsible executive has to arrive at a point where he or she can say with confidence that they have assessed their exposure to any business risks and are able to respond positively to the Year 2000 challenge with the assurance required to the Government, the Parliament and to the Australian community.

NOTES AND REFERENCES

1. The survey conducted by Korn/Ferry International in June 1996 found that the CIOs' managerial exposure occurs mainly within their functional area, and that CIOs tended to differentiate very little in their relationships with internal customers, external customers and vendors. The survey findings tended to confirm the view that the CIO position can be insular and without sufficient exposure to the entire business. ('*Survey of Chief Information Officers 1996'*, Korn/Ferry International, September 1996, pages 5 & 7).

2. Information Age 1997 *'Ignorance no defence against millennium bug'*, August (page 33).

1. Australian National Audit Office (ANAO) 1997 *'Principles for Core Public Sector Corporate Governance'*. Discussion Paper, Canberra. June.

4. Management Advisory Board/Management Improvement Advisory Committee (1995), '*Guidelines for Managing Risk in the Australian Public Service'*, Exposure Draft, MAB/MIAC report No.17, AGPS, Canberra.

5. United States General Accounting Office, Accounting and Information Management Division, 1997, *'Year 2000 Computing Crisis: An Assessment Guide'*, (Exposure Draft). Washington, February.

3. Report by the Comptroller and Auditor General 1997, *'Managing the Millennium Threat'*, National Audit Office, London, UK, 21 May. (page 3).

7. Ibid., (page 3).