Australian National Audit Office

IT Performance Review

May 2010

KPMG

Australian National Audit Office

IT Performance Review

Performance Audit

May 2010

ISSN 1036–7632

ISBN 0 642 81129 6

COPYRIGHT INFORMATION

KPMG

20 May 2010

Dear Mr President
Dear Mr Speaker

I have undertaken a performance audit of the Australian National Audit Office, in accordance with the authority contained in the *Auditor-General Act 1997*. Pursuant to *Senate Standing Order 166* relating to the presentation of documents when the Senate is not sitting, I present the report of this audit. The report is titled *Australian National Audit Office—IT Performance Review.*

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's Homepage—http://www.anao.gov.au.

Yours sincerely

Geoff Wilson
Independent Auditor
Appointed under Section 41 of
The Auditor-General Act 1997

Contents

Diagrams

Disclaimer

This report has been prepared at the request of the Joint Committee of Public Accounts and Audit (JCPAA) in connection with our engagement to perform services as detailed in Section 2 of this plan. Other than our responsibility to the JCPAA and management of the ANAO, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on these terms of reference. Any reliance placed is that party's sole responsibility.

We believe that the statements made in this report are accurate, but no warranty of accuracy or reliability is given in relation to information and documentation provided by ANAO management and personnel.

Inherent Limitations - Because of the inherent limitations of any internal control structure it is possible that errors or irregularities may occur and not be detected. Our performance audit is not designed to detect all weaknesses in control procedures as it is not performed continuously throughout the period and the tests performed are on a sample basis. As such, except to the extent of sample testing performed, it will not be possible to express an opinion on the effectiveness of the internal control structure. Any projection of the evaluation of control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate. The findings expressed in the subsequent report will be formed on the above basis.

1. Executive Summary

1.1 Introduction

The Australian National Audit Office (ANAO) assists the Auditor-General to provide an independent view of the performance and financial management of public sector entities. The *Auditor-General Act 1997* sets out the Auditor-General's functions, mandate and powers. The Act establishes a unique, independent relationship between the Auditor-General and the Australian Parliament.

The primary client of the ANAO is the Australian Parliament. The ANAO's main point of contact with Parliament is the Joint Committee of Public Accounts and Audit (JCPAA), although interaction does occur with other parliamentary committees and parliamentarians in order to obtain an understanding of parliamentary priorities, public administration matters and the outcomes of audit coverage.

The ANAO's purpose is to provide the Parliament with an independent assessment of selected areas of public administration, and assurance about public sector financial reporting, administration, and accountability. This function is delivered through the Assurance Audit Services Group (AASG) and the Performance Audit Services Group (PASG). The Professional Services Branch (PSB), through the provision of technical assistance, and the Corporate Management Branch (CMB), through the provision of practice management related services, support the two 'operational' areas.

Efficiently running Information Communications Technology (ICT) applications and systems are critical to the delivery of the services provided by the ANAO. Given this and the current focus on the use and management of Government ICT, stemming from the Gershon Review, KPMG, as part of the *Contract for the Appointment of an Independent Auditor for the ANAO* (The Contract of Appointment) has been requested to undertake an Information Technology (IT) Performance audit.

1.2 Independent Auditor

Mr Geoff Wilson, the *Independent Auditor* for the Australian National Audit Office, who is also a Partner of KPMG, arranged for KPMG to undertake this IT Performance Audit.

1.3 Background

The future direction of ICT for the ANAO is documented in the *Information Communications Technology Strategic Plan (ICTSP) 2009-2012*, which is a linked strategy to the *ANAO Corporate Plan.*

The current ICTSP for the ANAO clearly links to the business drivers of the organisation, which is a vital element in ensuring that the business aspects drive the direction. These business drivers include four Key Result Areas (KRA):

- **KRA 1** – *Clients recognise the value of ANAO's people, product and services which is underpinned by our reputation and integrity.*
- **KRA 2** – *High quality performance and assurance procedures and services in accordance with the professional standards. Visibility and accessibility of products and services.*
- **KRA 3** – *Responsive and flexible working environment that includes appropriately skilled workforce aligned with business practices.*
- **KRA 4** – *Cost effective management of our work program and office in a responsive and adaptable environment.*

The focus of this performance audit was on the ICT Strategic Planning Framework and its key linkages to the broader corporate strategic framework. In addition, the key elements of ICT application security, back-up and recovery/business continuity and software licensing were considered.

1.4 Objective

The objective of this performance audit was to address the effectiveness of ICT management across the ANAO's key applications and systems. Using guidance from leading methodologies including the Information Technology Infrastructure Library (ITIL®) and the Control Objectives for Information and related Technology (COBIT®) this performance audit included:

1. *Assessing the effectiveness and appropriateness of current IT strategic planning to suit the organisation's short and long term needs (including any key application upgrades/acquisitions);*
2. *Assessing if the access management to key applications and data is managed effectively such that access to sensitive data is restricted to authorised staff and that additions and deletions of rights is performed in a timely and efficient manner;*
3. *Reviewing the effectiveness and adequacy of the ANAO's current backup regime;*
4. *Assessing if the ANAO is effectively managing the software licensing; and*
5. *Reporting on any identified areas of improvement.*

1.5 Summary of Findings and Suggested Improvements

As per the agreed Audit Work Plan, this performance audit assessed the ICT Strategic Planning Framework and its associated components (refer to **Sections 3 to 8** for detail on each element considered).

Our predefined methodology, derived from COBIT®[1], rates the overall maturity level[2] of the *ICT Strategic Plan* (through our review of key documentation and discussions with key ANAO staff) at 3 – 'Defined Process' state (in some cases ANAO's practices displayed a maturity level at 4 – 'Managed and Measurable'). This is certainly where we would expect the ANAO to be, considering its size and operations, and is noted that no formal recommendations were made as part of this review.

That said, there were **three areas** for improvement identified to better align and manage the ICT performance of the ANAO, and include:

- *A clear link of corporate risks to the ICT Strategic Plan;*
- *The definition of Key Performance Indicators in order to measure the ICT Strategic Plan; and*
- *The documenting of the monthly data recovery procedures and results.*

It is noted that these suggestions are considered 'business improvement' opportunities that will further strengthen the ANAO's control environment.

These suggestions are detailed in **Section 9—Audit Findings and Suggested Improvements** of this report.

The diagram over the page provides a diagnostic assessment of the ANAO's ICT Strategic Planning Framework, showing the ANAO's actual score against acceptable practice. As can be seen from the overview, the ANAO are either above or in line with the 'acceptable practice' maturity, with notable highlights in the areas of defining the current and future governance arrangements and in relation to selecting best fit options/solutions for the organisation.

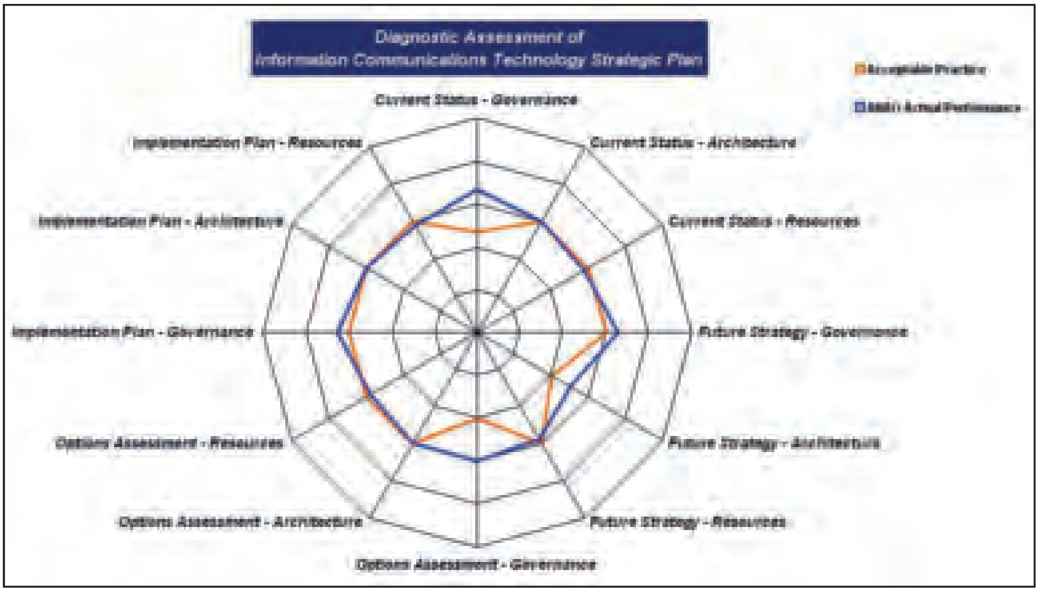
This diagnostic overview collates the information which is detailed in **Section 4—ANAO's Strategic Planning Framework.**

[1]. Information Systems Audit and Control Association (ISACA), *Control Objectives for Information and Related Technology (*COBIT®*)*, version 4.1

[2] Refer to COBIT® Maturity Model in **Section 3 - IT Strategic Planning Framework - Background and Context**

Diagram 1

Diagnostic Assessment of ANAO's ICT Strategic Plan



Previously KPMG have assessed thirteen Government agencies using the COBIT® framework, with each assessment focussing on the ICT Strategic Planning element. This benchmark data shows maturity scores ranging from two to four, with the average being **2.538**[3]. When comparing this to the ANAO, it clearly shows that they are well positioned (within other Government agencies) in terms of ICT strategic planning maturity.

ANAO's Overview Comment:

The ANAO welcomes the audit conclusion that our ICT management is effective and we agree with the suggestions for improvement. We will progressively plan and implement initiatives to improve on our information technology strategic planning. The audit provides useful insights into the effectiveness of the ANAO's governance and planning, and on areas to further enhance our information technology capability.

[3] This average score is based on COBIT® assessments conducted by KPMG Canberra Office over the period 2001 to current.

1.5.1 ANAO's ICT Strategic Plan

The purpose of an organisation's *ICT Strategic Plan* is to highlight the current ICT environment, discuss the future ICT goals, the options available to realise these goals and how it will endeavour to implement the planned objectives.

The ANAO have documented an *ICT Strategic Plan* (ICTSP) that has a well defined outline of its key ICT technical infrastructure and application elements. Future business objectives are clearly defined through the identification of key projects that clearly link to the high-level corporate business drivers. Each project that the ANAO initiates passes through their formal business case framework that includes input from various levels of management, from the Deputy Auditor-General to the Chief Information Officer. Each key project is also formally reported and discussed through the Information Strategy Committee (ISC) governance forum, which is chaired by the Deputy Auditor-General. The process also includes clear lines of governance, through project boards and identification of risks.

In arriving at the maturing rating for the ANAO, the following key highlights around its ICTSP are noted:

- The ICTSP has a clear link to the *ANAO Corporate Plan*, with future projects clearly aligned to the business drivers outlined in the *ANAO Corporate Plan*.
- Strong Executive level support around the ICTSP and the objectives it seeks to achieve.
- The ICTSP is regularly referred and considered as an element of the Information Strategy Committee agenda, which is chaired by the Deputy Auditor-General. In addition, a yearly assessment process is undertaken in relation to the ICTSP to track progress against its objectives.
- In order to support the limited in-house ICT capability and to meet the objectives outlined in the ICTSP, the ANAO have outsourced the management of ICT to Unisys. This arrangement has been in place for a considerable period[4] and Unisys support the overall ANAO initiatives.

[4] The Unisys contract first began in 1997 and was then market tested in 2000 and 2003. In 2007 the ANAO executed a contract extension option of 2 years and again market tested in 2009. The current contract is for 5 years with a 4-year option.

- Whilst the *ICT Strategic Plan* covers a 3-year period, the ANAO have established a framework to review the objectives on a yearly basis. This allows the ANAO to adapt its strategies to emerging opportunities or Government initiatives.

The Gershon review, released in 2008, was a Federal Government sponsored review that focussed on the effectiveness and efficiency of the Government's current use of ICT. The Gershon review provided recommendations to assist Government agencies in achieving increased efficiency within the ICT environment.

The impact on the ANAO from the Gershon review, as with most Government agencies, was to achieve efficiency dividends. The ANAO was required to achieve total cost savings of approximately $360,000 for financial years 2008-09 and 2009-10.

This was broken down into $90,000 of savings for the financial year 2008-09 and $270,000 of savings for the financial year 2009-10. The ANAO has reported that for the first year of this requirement, that it has achieved this level of cost saving and attributes this to:

- An assessment and review of its software licensing arrangements, with the removal of unnecessary software and licences; and
- A retesting of its primary ICT contract for ICT services with Unisys.

Whilst the ANAO ICTSP framework and maturity is in line with acceptable practice, the following improvement opportunities (to further strengthen its ICTSP framework) were noted:

- ***To better align the corporate Information Technology risks to the ICT Strategic Plan***

  Whilst there is a separate risk management process established within the ANAO, it is suggested that the ANAO consider, in its future consideration of the *ICT Strategic Plan*, creating a clear link from the identified ICT Corporate Risks to the ICTSP.

- ***Definition of Key Performance Indicators to measure the ICT Strategic Plan***

  Whilst the following is acknowledged:

  – The ANAO has a range of KPIs and reports for its ICT activities (including monitor of ICT spend, staff surveys, Unisys service delivery reports, post implementation reviews, individual project KPIs and reporting to project boards); and

  – The ANAO reviews the ICTSP on a yearly basis.

Additional benefit can be derived from the consolidation of such reports against a selection of KPIs so as to inform progress against broader strategic ICT objectives. It is suggested that the ANAO incorporate the relevant KPIs and targets into the ICTSP so as to assist the yearly deliberations of performance against the ICT strategy as a whole. Refer to **Section 9 – Audit Findings and Suggested Improvements** of this report for detail.

Whilst not in the scope for this review, the ANAO is continuing to identify opportunities to reduce the costs associated with ICT, with a recent move to host some services through a 'cloud' computing arrangement, whereby costs are saved by not having to establish infrastructure and support. In addition, and through another key Gershon initiative, the ANAO has also started to consider how the process of 'shared services' might be implemented, whereby like-agencies or portfolios establish common Human Resource and Finance system platforms.

See **Section 4—ANAO's Strategic Planning Framework** for further detail.

1.5.2 ANAO's Application Environment

The ANAO has a diverse set of corporate and business applications within its ICT environment. These applications enable the ANAO to achieve its business goals and ICT strategies. The ANAO ICT environment consists of 5 core systems, which include PeopleSoft, Finance One, eHive, ChangePoint and Team Mate.

The ANAO is not considered, from an application environment perspective, at the 'bleeding edge' of technology. The applications that are implemented into its environment follow the strategy/principle of being 'commercial off-the-shelf' (COTS) in nature.

This strategy reduces ICT spend, as implemented applications require minimal software development and bespoke modification, which can be of increased cost to the organisation and increased risk to an ICT environment. It therefore relies on its vendor relationships to support this function. That said, the ANAO undertakes considerable analysis prior to the introduction of a new application, both from a 'business fit' perspective and in relation to its 'established infrastructure'.

As part of its ICT Strategic Planning Framework, the ANAO applications are reviewed on a regular basis to ensure its ICT and business objectives are being met with two recent examples that include a planned upgrade of Team Mate and the consolidation of its practice management systems into the ChangePoint product.

No improvement opportunities were identified in relation to this component.

See **Section 5—ANAO's Application Environment** for further detail.

1.5.3 ANAO's Data Security

Overall the ANAO has a sound security policy framework in place that covers the key components of both physical and logical security. Of note is the importance the ANAO places on the protection of information and its framework that surrounds this requirement. In addition the ICT Security policies (outlined below) are considered mature and ensure that staff are aware of their responsibilities.

The Security Policy suite encompasses the following components:

- *Agency Security Policy;*
- *IT Security Policy;*
- *Information Classification and Handling Guidelines;*
- *Personal Computer Facilities Guidelines;*
- *Email and Fedlink Usage Guidelines;*
- *Internet to the Desktop Usage Guidelines;*
- *Internet Café Usage Guidelines; and*
- *Home-Based Computing and Secure Remote Access Guidelines.*

User Network and Application Security

A key element that was considered was in relation to the ANAO processes for the creation, modification and removal of users from the network and key applications (both corporate and business applications). These processes are well defined and documented within the ANAO environment. This includes a 'user access' process flow that is neither cumbersome nor onerous on staff to complete and includes the key elements to ensure access is only granted to the network and applications on an 'as needs' basis.

As part of our investigations a random selection of user creation and removal forms have been tested against the current configuration of the ANAO network. The purpose of this testing is to ensure user creation and removal processes are followed and correct data security restrictions are maintained. In each case tested correct processes have been followed.

No improvement opportunities were identified in relation to this component.

See **Section 6—ANAO's Data Security** for further detail.

1.5.4 ANAO’s Backup and Recovery and Business Continuity

Backup and Recovery

ANAO’s backup and recovery services are performed and monitored by Information Technology services company Unisys.

The existing documented backup procedures (for both the ACT and NSW) consist of three components being the daily, weekly and monthly processes. Each scheduled backup is clearly described and outlines the tape rotation, the type of backup (e.g. full backup) and the respective day(s) of the backup. Backups are monitored and the results, successful or otherwise, are recorded in a backup log.

Overall the backup procedures are efficient and adhere to industry standards in terms of backup schedules, the checking and logging of backups and tape rotation cycles.

Whilst the backup and recovery process appears well documented, the following performance improvement suggestion is made:

- ***The documenting of the monthly data recovery procedures and results.***

  The backup and recovery document briefly mentions data recovery, however very little detail is provided in terms of specific procedures for the recovery of data, even though monthly tests of data retrieval from backup tapes is carried out. We would suggest further documented detail be provided for the monthly data recovery procedures and the results from this testing be recorded.

Refer to **Section 9—Audit Findings and Suggested Improvements** of this report for detail.

Business Continuity

The ANAO have a Business Continuity Plan (BCP) document which outlines response procedures in the event of a disaster occurring. The BCP breaks down procedures into four phases being Response, Resumption, Recovery and Restoration Phase.

Each phase contains a checklist of actions to be conducted in the event of a disaster and the roles and responsibilities for those actions. The framework that has been established appears adequate to support the needs of the ANAO (refer to the observation below).

No improvement opportunities were identified in relation to this component, however the following observation is made:

As part of this performance audit (and recognised by ANAO management) is that there are currently minimal Disaster Recovery (DR) contingencies if major ICT infrastructure was unavailable (e.g. fire damage to the data centre). Minimal DR contingencies would obviously result in a delayed recovery time for key ICT services. ANAO management however has indicated that this is not a high priority, with the ANAO willing to accept the risk associated with this as its ICT applications are non-critical to delivering on its role within the Commonwealth.

See **Section 7—ANAO's Backup and Recovery and Business Continuity** for further detail.

1.5.5 Software licensing

The ANAO employs the use of a software tool called Express Meter to monitor software and licence usage across its ICT network. Express Meter is an off-the shelf product (metering solution) that lets an organisation manage software usage to ensure that an appropriate level of licences are maintained. The ANAO has placed a focus on this area in the last 12 months and have been able to identify a number of products/licences that could be removed/reduced and has 'cleaned' this aspect of operations up considerably. This has resulted in cost savings for the ANAO.

The ANAO have deployed Express Meter to track usage across its Standard Operating Environment (SOE) and includes monitoring PeopleSoft, Finance One, eHive, ChangePoint and Team Mate. Express Meter is configured to monitor non-standard applications and prevent the execution of non-standard applications should they be installed on local computers.

Licensing conflicts, should they occur, are communicated to the end user by the Express Meter client, which is installed as a part of the Standard Operating Environment. The end user would ultimately receive a message indicating that the accessed software has exceeded its licence limit and a record of this would be logged in Express Meter.

Detailed reporting is generated from Express Meter, with the ANAO generally running them on a monthly basis. Usage and licensing reports are reported to the Chief Information Officer, who is responsible for taking the necessary actions to address software licence excess or shortcomings.

No improvement opportunities were identified in relation to this component.

See **Section 8—Software licensing** for detail.

2. Scope and Methodology

2.1 Scope

The scope for the audit was developed after consultation with key stakeholders and consideration of a number of ANAO ICT related documents.

Personnel interviewed as part of the scoping process included:

- The Auditor-General;
- The Deputy Auditor-General;
- The Chief Information Officer; and
- The Executive Director, Corporate Management Branch.

The scope of this audit is to focus on the key ICT applications and systems that contribute to the ANAO ICT suite with a focus on the effectiveness of ICT management. This is undertaken with the broader ICT Strategic Planning Framework in mind.

Scoping identified 'current', 'future', 'options' and 'implementation' processes in relation to the execution of the ICT strategy to be of the greatest concern to management. Our fieldwork was necessarily undertaken at a high level and was limited to interviews with key staff from the ANAO and the consideration of relevant information (including available industry data). An inherent limitation in the conduct of this type of audit is that our findings, suggestions, recommendations and resultant conclusions are limited largely by the availability of documentation and staff from the ANAO.

Not included in the scope of this performance audit were the ICT related reviews currently included in the internal audit plan to be carried out by the ANAO's internal auditor, Ernst & Young. The reviews include:

- Records management - focus likely to be application management and controls (security); and
- Risk management planning, including BCP and DRP.

At the time of writing this report neither review to be conducted by Ernst & Young had commenced. The Records management review is due to commence in April, with the Risk management planning review scheduled to be completed during the 2009 / 2010 financial year, although no specific commence date has been set.

During scope discussions with ANAO's Chief Information Officer it was agreed that this review could run simultaneously alongside (without duplication) the reviews being carried out by Ernst & Young.

2.2 Audit Methodology

Our work was conducted in accordance with Australian Auditing and Assurance Standards, specifically relating to performance auditing (AUS 806). To achieve our objectives and conclude on the objective of the performance audit, we undertook this audit in accordance with an audit program.

Specifically, we held interviews with the:

- The Deputy Auditor-General;
- The Chief Information Officer;
- The Executive Director, Assurance Audit Services Group;
- The Group Executive Director, Performance Audit Services Group; and
- Technical support staff from Unisys.

The focus during interviews and review of key documentation was to:

- Identify the key ICT applications and systems;
- Identify and document those responsible for these key ICT applications and systems;
- Identify the controls and access surrounding sensitive data ensuring it is restricted to authorised staff;
- Identify the existing backup arrangements ensuring they are sufficient for ANAO's current and future ICT requirements;
- Identify existing software licences and ensure they reflect ANAO's software licensing requirements;
- Identify any risks surrounding the key ICT applications and systems;
- Identify ANAO's short and long term ICT needs;
- Identify current ICT strategic planning to determine if this meets ANAO's short and long term needs; and
- Gain an understanding of the nature and timing of future ICT initiatives at the ANAO.

2.3 References

In addition to the internal ANAO documentation reviewed, the following documents were referred to in completing this audit:

2.3.1 Key ANAO related documents[5]

- *ANAO Corporate Plan (2007-2010)*;
- *ANAO Business Plan (2008-2009)*;
- *Information Communications Technology Strategic Plan (2009-2012)*, Version 1.0, (24 April 2009);
- *Unisys Backup and Recovery Procedures*, Version 1.0, April 2008;
- *Business Continuity Plan,* Version 2.0, May 2008;
- *ANAO Security Policies*, Version 3.0, September 2008;
- *ANAO Risk Management Plan 2010-11*;
- ICT *Security Threat and Risk Assessment* (2008 Update), Version 1.0, 5 June 2008, Verizon Business;
- *Information Strategy Committee Charter*, February 2009;
- *Unisys Enterprise Architecture Review for the ANAO,* Version 2.0, 5 February 2010;
- *Unisys / ANAO Monthly Service Delivery Report*, Version 1.0, August 2009 and October 2009;
- *Oakton Consolidated Snare Report*, June, July and August 2009;
- *Meeting Minutes of the Information Strategy Committee* (3 September 2009, 14 October 2009, 5 November 2009 and 3 December 2009);
- *ANAO Specific IT Issue Survey*, Survey 1, 2009, ClientWise; and
- *Schedule 5 Service Level Requirements* of the ANAO and Unisys IT Services contract, version 3.0, 30 March 2009.

[5] All key ANAO related documents have been sourced from the Chief Information Officer during the fieldwork stage of this performance audit. (Covering period December 2009 to March 2010).

2.3.2 External References

- Information Systems Audit and Control Association (ISACA), *Control Objectives for Information and Related Technology (COBIT®)*, Version 4.1;
- Office of Government Commerce (OGC), *Information Technology Infrastructure Library (ITIL®)*, Version 2;
- InfoSys, *Recommendations for Performance Benchmarking*, January 2008; and
- KPMG (Canberra), *COBIT® benchmarking data*, collated from 2001 to present.

2.4 Structure of this report

The findings, risks, suggestions and recommendations identified by this audit, and additional information are presented in the report in the following way.

Section 3	**ICT Strategic Planning Framework - Background and Context**
Section 4	**ANAO's Strategic Planning Framework** • **ICT Governance** • **Architecture** • **Resources**
Section 5	**ANAO's Application Environment**
Section 6	**ANAO's Data Security**
Section 7	**ANAO's Backup and Recovery and Business Continuity**
Section 8	**Software licensing**
Section 9	**Audit Findings and Suggested Improvement**

3. ICT Strategic Planning Framework - Background and Context

3.1 KPMG's ICT Strategic Planning COBIT® Framework

The *ICT Strategic Plan* (ICTSP) is a critical planning document in the context of today's information-driven organisation and, as such, deserves the significant attention of Senior Management.

For the basis of our analysis, in particular for ICT Strategic Planning, we have followed a pre-defined methodology. The areas considered necessary are conveniently summarised in the following Matrix:

ICTSP Diagnostic MATRIX	***Current Status***	***Future Strategy***	***Options Assessment***	***Implementation Plan***
ICT Governance Context, Performance Monitoring, Management Commitment, Risk, Control, Ethics, Legal / Regulatory and Quality	Assessment of Past / Existing Governance Practices	Assessment of Planned / Proposed Governance Practices	Assessment of certain Governance issues re Options e.g. Risks.	Assessment of specific Governance Issues re the Transition Plan.
Architecture Technology & Applications.	Assessment of Past / Existing Architectures.	Assessment of Planned / Proposed Architectures.	Assessment of Architectures Options.	Assessment of transition / implementation Architectural issues.
Resourcing Finances & HR.	Assessment of Past / Existing Resourcing	Assessment of Resourcing	Assessment of Past / Existing Resourcing	Assessment of Past / Existing Resourcing

The diagnostic material developed (and which has been used in the assessment of the Australian National Audit Office's *ICT Strategic Plan*) has been derived from COBIT® (**C**ontrol **OB**jectives for **I**nformation and related **T**echnology)[6].

[6] COBIT® is Copyright of the Information Systems Audit and Control Foundation (ISACF)

Why "Current Status"?

It has often been said – *"if one fails to assess the past then one is inevitably doomed to repeat it in the future"*. On a practical level, without a ruthless and honest assessment of the failures of ICT in the past the ICTSP may not adequately address fundamental legacy weaknesses which could exist in either ICT Governance, Architecture and / or Resourcing areas.

Why "Future Strategy"?

Appreciably, the primary focus of the ICTSP is to provide the architectural and strategic framework for the 'Future' of the organisation. This should be the predominant emphasis in the ICTSP. A proportion of the Plan should be dedicated to describing and defining the future ICT strategy environment.

Questions addressed by the ICT Strategic Planning's handling of "Future Strategy" issues include:

- How will ICT Governance be implemented?
- How will management commitment be acquired and retained?
- Will key ICT-related risk / control issues be dealt with?
- Will performance measurement and quality considerations be in place to govern 'future strategy' delivery?
- What will the application architecture look like?
- What will the technology architecture look like?
- What financial resources are required to implement the ICTSP (i.e. over the planning horizon)?
- Will the existing profile of ICT skills be sufficient to address the skill sets envisaged by the ICTSP? If not, what training or resource management strategies are envisaged?

Why "Options Assessment"?

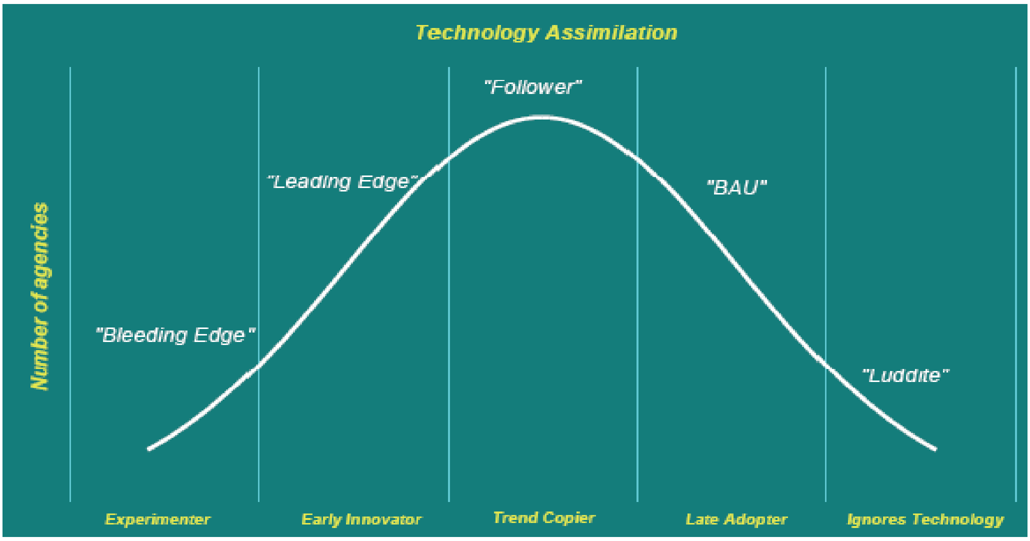
Performing an assessment of available and applicable technology options is a critical component of the ICTSP, especially if the ICTSP is to realise greater efficiencies to the organisation through the timely and considered assimilation of new and emerging technologies.

An organisation such as the ANAO should aim to be somewhere between the 'Trend Copier' and 'Late Adaptor' point on the innovation curve (refer Diagram 2).

Please see below for a diagram outlining this relationship.

Diagram 2

Technology Assimilation



Why "Implementation Plan"?

The ICTSP Implementation Plan, includes two planning 'envelopes'. These are the initial planning phase of 'transition' and the subsequent phase of fully planning for and delivering the ICT Strategy or in simpler terms implementation completion.

In the first phase, the core 'Transition Plan' aspects, deal with the key logistical requirements that need to be deployed in order to transition the existing ICT architecture / environment to the proposed architecture / environment. This would take into account the 'future strategy' aspects of the ICTSP. Typically, transition can last from 6 to 18 months. The Transition Plan needs to be assessed in order to ensure that it is realistically resourced from both a financial and HR perspective. Better practice aspects of Transition Planning will also include a strong ICT Governance consideration. This should include appropriate management commitment, risk management, quality management and performance measurement.

Over the longer planning envelope of 3 to 5 years, the Implementation Plan covers the full articulation of the ICTSP from a planning and delivery perspective. As with the Transition Planning phase, the Implementation phase needs to be realistically resourced (financial and HR) and embrace sound ICT Governance principles. Of particular importance are those that measure performance, assess quality in service delivery and track progress against Plan delivery.

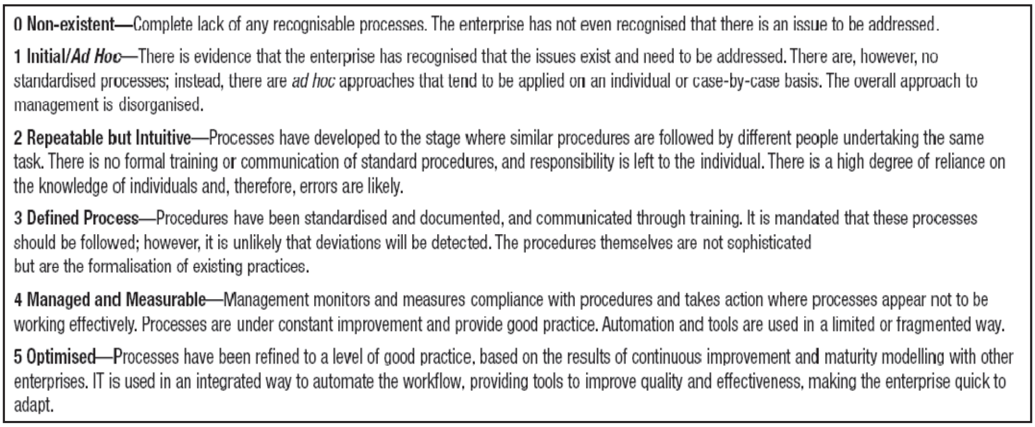
3.2 COBIT® Maturity Model

The COBIT® Maturity Model[7], as displayed below in Diagram 3, is a structured framework designed for management to assess the maturity of an organisation's ICT capability. The maturity level is rated from non-existent (0) to optimised (5).

This model gives management a clear representation of the capability of their ICT processes and procedures and an idea of what is involved to reach an improved performance if required. It is noted that an organisation does not need to be at an optimised level to be operationally effective. There is a cost/benefit consideration to be determined at each maturity level, which is critical in determining what maturity should exist. For this performance audit, we have determined that the ANAO should at least be at a maturity level of ***3 – Defined Process***, which is considered acceptable practice within Australian Government agencies.

Diagram 3

COBIT® Maturity Model



0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

1 Initial/*Ad Hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2 Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined Process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

[7] COBIT® Maturity Model extracted from the COBIT® 4.1 Framework

4. ANAO's Strategic Planning Framework

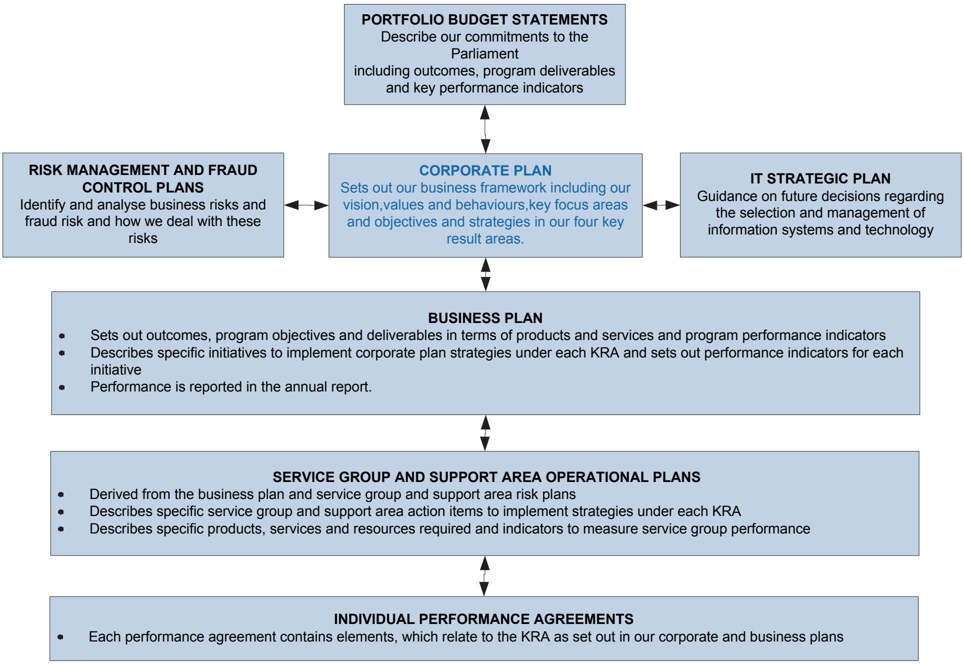
The Australian National Audit Office (ANAO) assists the Auditor-General to provide an independent view of the performance and financial management of public sector entities. This important function relies on a modern and robust ICT environment. As a result, the ANAO has developed an *ICT Strategic Plan* covering the period 2009 to 2012.

The *ANAO Corporate Plan* is the overarching and central document in ANAO's Strategic Planning Framework. It describes the ANAO's business context and outlines key organisational strategies for the period 2007-2010. The *ANAO Corporate Plan* is reviewed on a three yearly basis.

As demonstrated in *Diagram 4*, the *ANAO Corporate Plan* is the central focus and key driver for the ICT Strategies. The *ICT Strategic Plan* supports the *ANAO Corporate Plan* vision, values and business drivers.

Diagram 4

ANAO Strategic Planning Framework[8]



PORTFOLIO BUDGET STATEMENTS
Describe our commitments to the Parliament
including outcomes, program deliverables and key performance indicators

RISK MANAGEMENT AND FRAUD CONTROL PLANS
Identify and analyse business risks and fraud risk and how we deal with these risks

CORPORATE PLAN
Sets out our business framework including our vision,values and behaviours,key focus areas and objectives and strategies in our four key result areas.

IT STRATEGIC PLAN
Guidance on future decisions regarding the selection and management of information systems and technology

BUSINESS PLAN

- Sets out outcomes, program objectives and deliverables in terms of products and services and program performance indicators
- Describes specific initiatives to implement corporate plan strategies under each KRA and sets out performance indicators for each initiative
- Performance is reported in the annual report.

SERVICE GROUP AND SUPPORT AREA OPERATIONAL PLANS

- Derived from the business plan and service group and support area risk plans
- Describes specific service group and support area action items to implement strategies under each KRA
- Describes specific products, services and resources required and indicators to measure service group performance

INDIVIDUAL PERFORMANCE AGREEMENTS

- Each performance agreement contains elements, which relate to the KRA as set out in our corporate and business plans

[8] The ANAO Strategic Planning Framework is referenced from the ANAO Corporate Plan 2007-10.

The *ANAO Corporate Plan* outlines two key outcomes which are directly related to the role and vision of ANAO, being, *Improvement in public administration* and *Assurance*. These outcomes are to be achieved through its four Key Result Areas (KRA):

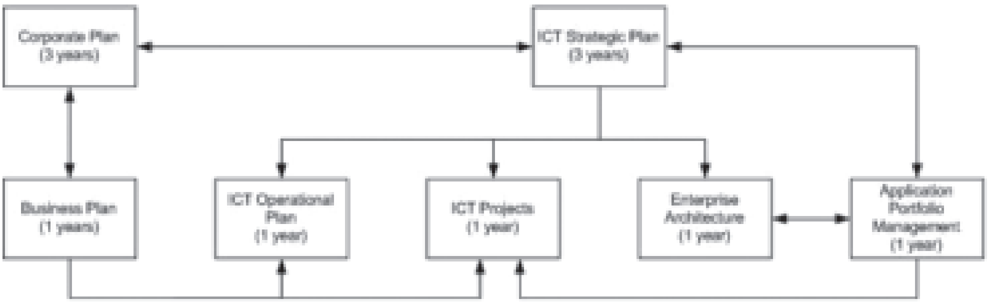
- ***KRA 1*** *– Our clients;*
- ***KRA 2*** *– Our products and services;*
- ***KRA 3*** *– Our People; and*
- ***KRA 4*** *– Our business performance.*

Details of the specific initiatives which result in achieving the outlined strategies for the ANAO are contained in the *ANAO Business Plan*, which is considered a sub-level document that supports both the Corporate and *ICT Strategic Plan*. The *ANAO Business Plan* flows from the *ANAO Corporate Plan* and describes the specifics of implementing the strategies for each KRA. The *ANAO Business Plan* is reviewed yearly and sets out objectives and strategies to guide future progress.

The *ICT Strategic Plan* aligns itself with the *ANAO Corporate Plan* and acts as a guiding document for the delivery of ICT services to ANAO. The *ICT Strategic Plan* is a reflection of managerial input and direction for the future of ANAO's ICT environment.

Further to this, the below diagram demonstrates the cycle the ANAO follows in regards to reviewing and updating the *ANAO Corporate Plan, ANAO Business Plan* and *ICT Strategic Plan*. This framework is used to assist in dealing with the dynamic nature of ICT. This framework allows for flexibility in the ANAO to adapt its strategies to emerging opportunities or Government initiatives.

Diagram 5
Application Portfolio Management Policy Relationships


Corporate Plan (3 years)
ICT Strategic Plan (3 years)
Business Plan (1 years)
ICT Operational Plan (1 year)
ICT Projects (1 year)
Enterprise Architecture (1 year)
Application Portfolio Management (1 year)

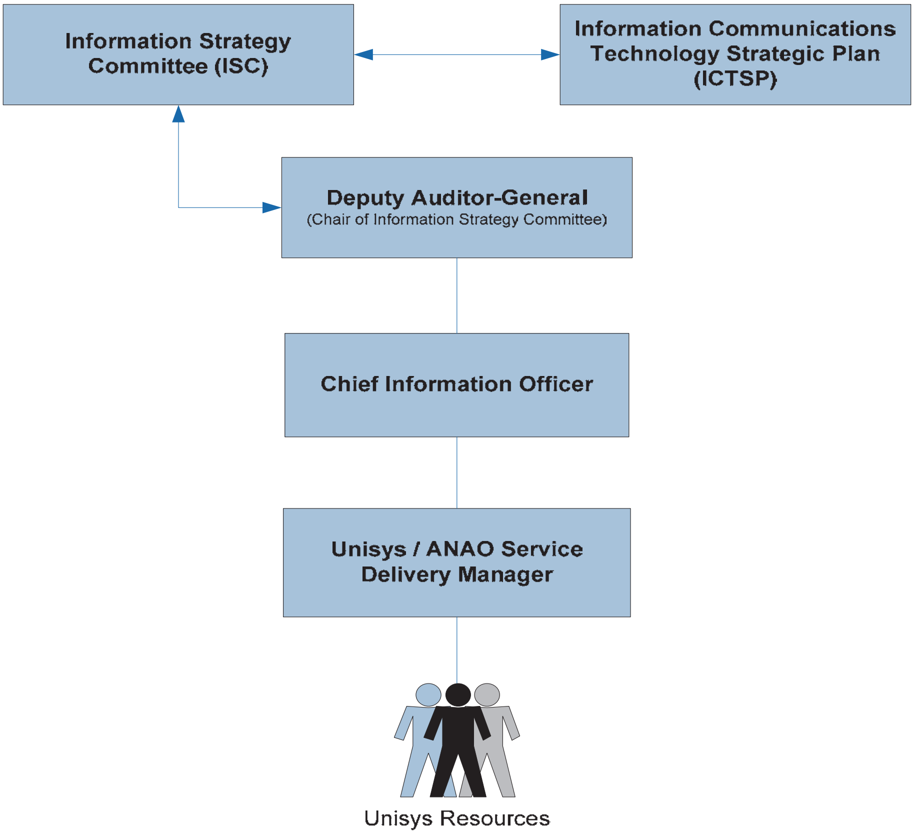
This diagram shows the policy framework associated with Applications Portfolio Management. This diagram is sourced from the ANAO.

4.1 ANAO ICT / Unisys Organisation Chart

To further outline the key ICT Structures within the ANAO, the diagram below provides a high-level overview of the reporting and governance structure. It is acknowledged that the ANAO places a reliance on the services on contract provider, Unisys, to supplement its relatively small in-house ICT capability.

Diagram 6

ANAO ICT / Unisys Organisation Chart


Information Strategy Committee (ISC)
Information Communications Technology Strategic Plan (ICTSP)
Deputy Auditor-General
(Chair of Information Strategy Committee)
Chief Information Officer
Unisys / ANAO Service Delivery Manager
Unisys Resources

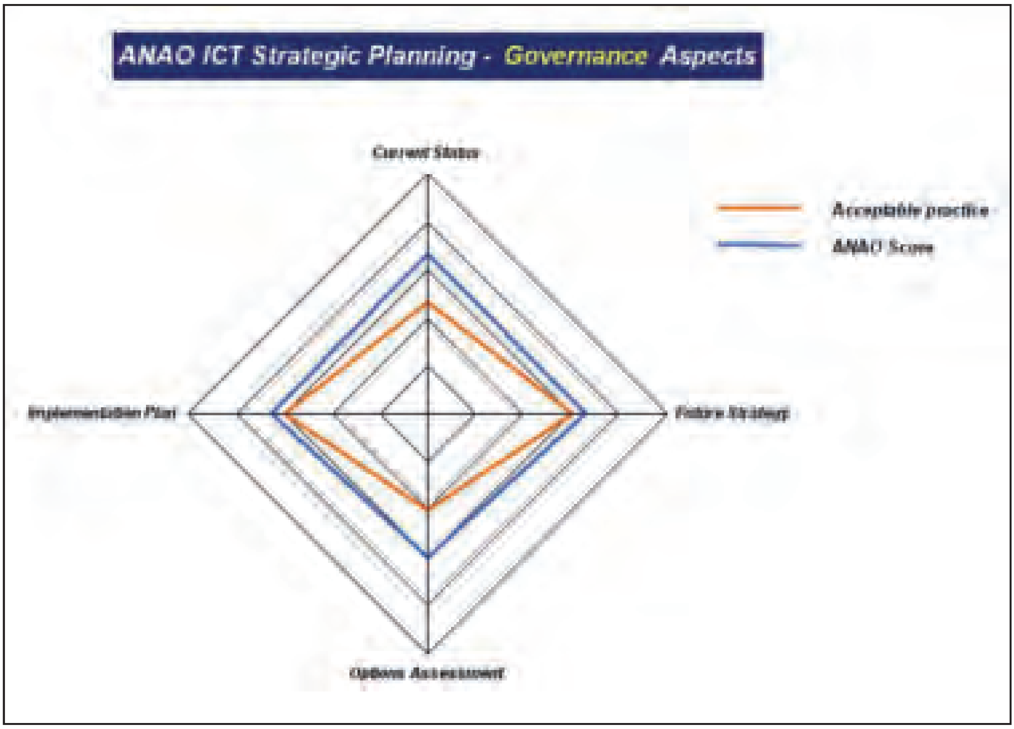
4.2 ICT Governance

The ANAO's *ICT Strategic Plan* was considered within the wider context of the organisation's *Corporate Plan* and whether:

- It receives visible top-level support within the organisation;
- Strategic risks of the organisation and impact of ICT are considered;
- ICT is used within an appropriate ethical context and legal requirements are met; and
- Measures of performance are specified and monitored and quality parameters are in place.

Diagram 7

ANAO ICT Strategic Planning – Governance aspects.



The assessment against the COBIT® framework for the *Governance* aspect of its ICTSP indicates that it is above the 'acceptable practice' score in all four components. The assessment indicates that the current and future governance arrangements that surround the ICTSP are clearly defined and have Executive level support. In addition the governance that surrounds the options assessment for future activities is also defined and ensures that appropriate approval and visibility surrounds the selection process.

Below are the key points surrounding the current, future, options and implementation areas of ANAO's governance aspects:

4.2.1 Current - Governance

- The ICT Governance that surrounds the current *ICT Strategic Plan* is considered mature with a clear link to the *ANAO Corporate Plan*. Projects are clearly aligned with the business drivers KRA 1 to KRA 4 as defined in the *ANAO Corporate Plan*.
- The ICTSP receives visible top-level support within the organisation.
- The Information Strategy Committees' primary role is to establish a control mechanism surrounding the *ICT Strategic Plan*. The committee meets regularly to assess the plan.
- A key component of the current status is the monitoring of ICT performance. Unisys generates a monthly report which monitors service level agreements, service desk enquires and current incidents, ICT environment changes, systems availability, network traffic volumes and usage and continuous improvement activities.
- As part of the ANAO's continuous improvement process, a yearly ICT satisfaction survey is completed, with the most recent one being undertaken in November / December 2009. With all staff invited to participate in this survey, the ANAO had a response rate of 39 percent. The survey covered aspects such as overall sentiment and performance of Unisys, initiative evaluation, ICT problems within ANAO and priority improvement comments. This survey has been a valuable tool to assist in the current state of ICT and potential improvements.

- In the interest of ICT controls and management an independent ICT Security Threat and Risk Assessment was conducted in June 2008. This assessment looked at the ANAO ICT systems implementations and the risk mitigation strategies and whether system implementations comply with Government regulatory requirements. The overall conclusion of the risk assessment was 'very sound'[9].
- Whilst there is a separate risk management process established within the ANAO, it is suggested that the ANAO consider, in its future consideration of the *ICT Strategic Plan*, creating a clear link from the identified ICT Corporate Risks to the ICTSP. (Refer to **Section 9—Audit Findings and Suggested Improvements** of this report for detail).

[9] The overall risk assessment conclusion of 'very sound' is referenced from Section 1.4 of the ICT Security Threat and Risk Assessment, version 1.0, dated 5 June 2008, conducted by Verizon Business.

4.2.2 Future - Governance

- Through the active management support from the Deputy Auditor-General to the Chief Information Officer (and input into the Information Strategy Committee) future projects and strategic directions are clear.
- The *ICT Strategic Plan* identifies key projects that support the corporate business drivers. Future projects are outlined and consider the business priority, estimated cost and proposed year of implementation. In addition to this, future strategies/projects are given a basic risk assessment.
- A comprehensive security policy framework (suite of documents) exists and will ensure future compliance within the organisation. This suite of documents considers the ethical context for the level of sensitivity data the ANAO collects.
- The ANAO regularly refers to the ICT Strategy Plan through the Information Strategy Committee, which is chaired by the Deputy Auditor-General. A yearly review process is undertaken to track progress against the ICT Strategy Plan.
- Whilst it is acknowledged that the ANAO has a range of KPI's and reports for its ICT activities and reviews the ICTSP on a yearly basis. It is suggested that the ANAO incorporate the relevant KPIs and targets into the ICTSP so as to assist the yearly deliberations of performance against the ICT strategy as a whole. Refer to **Section 9—Audit Findings and Suggested Improvements** of this report for detail.

4.2.3 Options - Governance

- The consideration and selection of projects within the ANAO involves key aspects including formal business cases and the involvement of senior layers of management.

4.2.4 Implementation - Governance

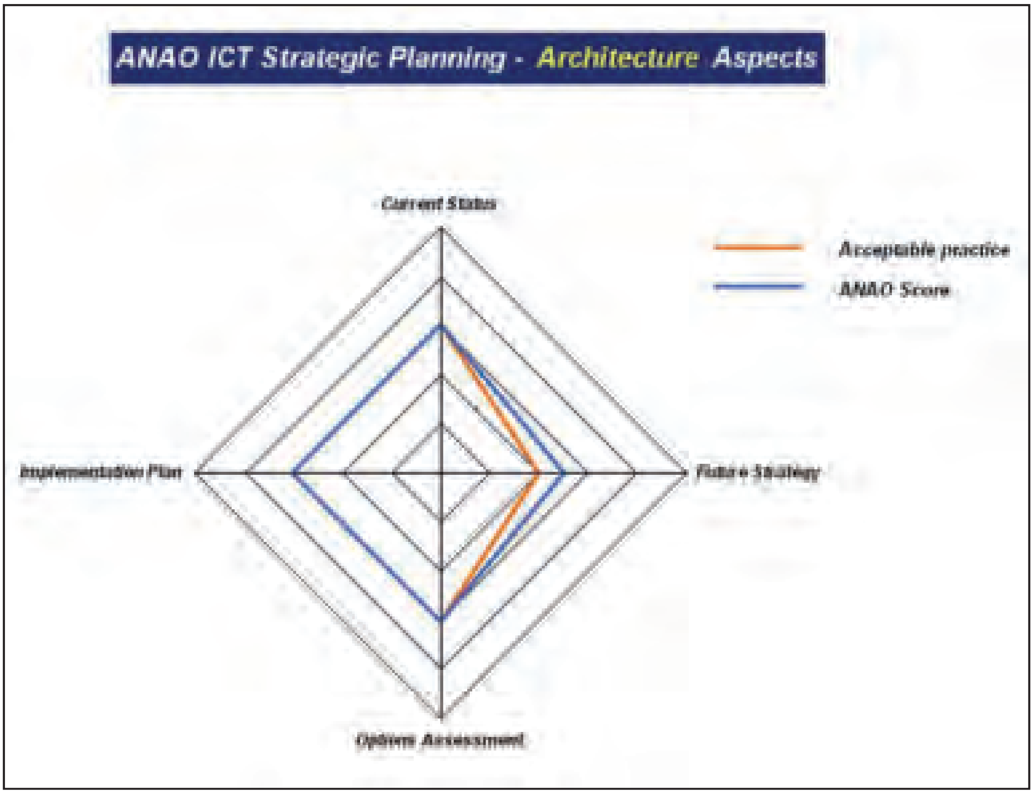
- Agreed upon project implementations are structured with focussed project boards, which incorporate a clear line of governance and escalation procedures. The yearly review of progress of implemented projects against the ICT Strategy Plan gives a visual representation of achieved activities.
- For planned future projects a basic risk assessment is listed in the *ICT Strategic Plan*, ratings are low, medium and high.

4.3 Architecture

The area of *Architecture* covers the area of technology and applications. Primary considerations include whether appropriate technologies have been selected for the organisation and whether application systems are focused on the business requirements of the organisation.

Diagram 8

ANAO ICT Strategic Planning – Architecture aspects.



The assessment against the COBIT® framework for the *Architecture* aspect of its *ICT Strategic Plan* indicates that it is at the 'acceptable practice' score or above in all four areas. The assessment indicates that the current and future architecture is well-defined, with the ANAO clearly documenting and understanding its current infrastructure and information requirements.

In addition, the options for the organisation are clearly outlined, which in the ANAO's case is through the business case process, which flows through to the execution of planned activities.

Below are the key points surrounding the current, future, options and implementation areas of ANAO's architecture aspects:

4.3.1 Current - Architecture

- In assessing the current ICT architecture, the ANAO's technology and application environment is clearly documented within the *ICT Strategic Plan*, giving a clear foundation of the current technology position.
- Current technologies and applications are sufficiently described in the *ICT Strategic Plan* and recently conducted reviews by Unisys have resulted in detailed documents describing the current Technology and Application environment. Between December 2009 and February 2010, Unisys has developed the review documents listed below.
  - Enterprise Architecture Review for the ANAO;
  - Enterprise Architecture Review for the ANAO (Server Architecture);
  - Enterprise Architecture Review for the ANAO (Infrastructure Architecture);
  - Enterprise Architecture Review for the ANAO (Application Architecture) and
  - Enterprise Architecture Review for the ANAO (Information Architecture).

4.3.2 Future - Architecture

- For planned / proposed technology and application implementations, the ANAO's assessment of future hardware requirements are considered low on the maturity scale. No specific technical information is documented and future application projects are outlines.

4.3.3 Options - Architecture

- In assessing the ICT Architecture options for projects, the ANAO conducts detailed evaluation processes in relation to software and hardware solutions. The evaluation process involves the Information Strategy Committee (ISC) and levels of management ranging from the Deputy Auditor-General to the Chief Information Officer.
- Resulting from this evaluation process described above, technology and application options to suit the ANAO Corporate and Business Strategy are defined and documented in the ICT Strategy Plan.

4.3.4 Implementation - Architecture

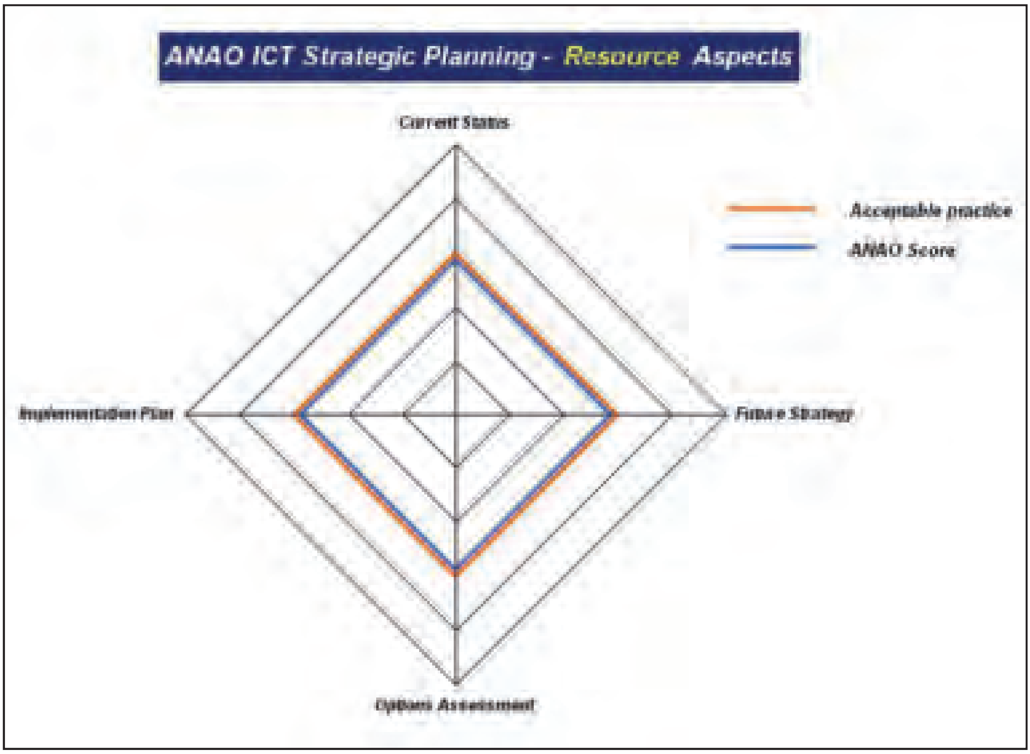
- The ICT transition / implementation of approved technology and application architecture options for future projects includes a business priority, project risk, estimated cost, percentage of annual ICT capital budget and proposed implementation year element. The ICTSP covers both infrastructure and software (application), with further detail described in the business case once a solution has been agreed.

4.4 Resources

The area of *Resources* covers both key corporate functions of finances and human resources, with an ICT focus. Primary consideration include whether appropriate financial costing have been considered in regards to the technology and application objectives and whether there are sufficient and appropriately skilled resources available to implement the plan.

Diagram 9

ANAO ICT Strategic Planning – Resource aspects.



The assessment against the COBIT® framework for the *Resource* aspect of its ICTSP indicates that it is marginally behind the 'acceptable practice' score in all four areas. The ANAO has a limited amount of in-house capability in relation to the ICT aspect of its operation, with the management of the infrastructure and systems outsourced to Unisys.

This arrangement places the ANAO in a position whereby it is to rely on the outsourcing partner for support and ICT related services. Where possible though, the ANAO in the execution of its projects endeavours to ensure it places an ANAO resource in the project management role to ensure this accountability is maintained.

Below are the key points surrounding the current, future, options and implementation areas of ANAO's Resource aspects:

4.4.1 Current - Resources

- High-level costing exist with the ICTSP for each identified project and provides an estimate of total ICT spend for the 3 year cycle. Detailed costing is developed as part of the business case process for each project.
- The current ICT support services (including infrastructure and service delivery of ICT solutions) is outsourced to Unisys. Unisys manages, administers and maintains the business as usual aspects of the ICT environment. In addition to this up to 90 percent of resources for upgrades surrounding the ICT environment, both hardware and software, are outsourced to Unisys or other third party technology service providers (this is the case for the below aspects as well).
- The Unisys contract first began in 1997 and was then market tested in 2000 and 2003. In 2007 the ANAO executed a contract extension option of 2 years and again market tested in 2009. The current contract is for 5 years with a 4-year option.
- The Unisys contract specifies Service Level Requirements (SLR) which measure key areas and target levels (which include expected and minimum targets). The previous contract had a minimum of 980 hours attendance by Unisys staff per month. The current contract is services based with only the Service Delivery Manager (SDM) required on site. Additional Unisys staff are optional depending on the demand to meet the SLR's. This is a supply / demand arrangement.

- The Unisys Service Level Requirements are broken down into seven Performance Categories[10]. These are:
    - Service Desk;
    - Incident Management;
    - Problem Management;
    - Change Management;
    - Availability Management;
    - Security management; and
    - Reporting.

Each Performance Category is further broken down into tasks which outline the requirements needed to meet each Performance Category. This includes key measurement points and expected and minimum service level targets. Each service level is measured on a calendar month base with required reporting.

4.4.2 Future - Resources

- For each future project an estimation of resources is undertaken and estimated costing determined. This high-level estimate is considered good practice and demonstrates a mature level of forward planning.

4.4.3 Options - Resources

- Costing options for future ICT applications and architecture projects are discussed during the evaluation process and then detailed as part of the business case process.

4.4.4 Implementation - Resources

- Similarly with Current, Future and Options, implementation costs are generally created at a high level.

[10] Performance Categories are sourced from Schedule 5 – Service Level Requirements of the ANAO and Unisys IT Services contract, version 3.0, 30 March 2009.

5. ANAO's Application Environment

The ANAO has a diverse set of applications within its ICT environment. These applications act as tools for the ANAO to achieve its business goals and ICT strategies. The ANAO ICT environment consists of 5 core systems. These systems are outlined in the below table:

ANAO Application	*Purpose/function*
Human Resources (PeopleSoft)	ANAO utilise the HR module of PeopleSoft for the creation of users, staff tracking and payroll.
Finance (Finance One)	Finance One is used as the corporate finance system, utilising a general ledger and account processing.
Interwoven\eHive	eHive is ANAO's content management system.
ChangePoint	ChangePoint assists in the management of end-to-end business processes. It integrates closely with PeopleSoft and Finance One.
Team Mate	Team Mate is used by ANAO to collaborate with audit documents and content.

The ANAO is not considered, from an application environment perspective, at the 'bleeding edge' of technology. The applications that are implemented into its environment follow the strategy/principle of being 'commercial off-the-shelf' (COTS) in nature. This strategy reduces ICT spend, as implemented applications require minimal software development and bespoke modification, which can be of increased cost to the organisation and increased risk to an ICT environment. It therefore relies on its vendor relationships to support this function. That said, the ANAO undertakes considerable analysis prior to the introduction of a new application, both from a 'business fit' perspective and in relation to its 'established infrastructure'.

As part of its ICT Strategic Planning Framework, the ANAO applications are reviewed on a regular basis to ensure its ICT and business objectives are being met. Two key examples are outlined below:

- A key application for the ANAO is the Team Mate product which supports the assurance business in the undertaking of financial audit activities. The ANAO, as part of the current ICTSP, had identified the need to upgrade this application to a more current version that better aligned to business activities and reflects the change to the Auditing Standards. The ANAO have decided to undertake this project in two phases, with the first phase to upgrade to a newer version of the product, but retain its current ‘audit methodology’ that supports the application. The second phase will be to review and update the audit methodology behind this application. This two phased approach will allow completion of the 2009-10 audits with the current methodology and completion of the 2010-11 audits with the updated methodology.

- A further initiative the ANAO have recently undertaken was to consolidate its range of diverse practice management systems. This was undertaken as the legacy systems were, in some cases, no longer being supported and required a complex interface arrangement for their operation. The decision was made to identify an application that can support the practice management requirements to gain efficiencies and further reduce ICT spend. This has resulted in the recent implementation of ChangePoint.

6. ANAO’s Data Security

6.1 Security Policies

The ANAO has a detailed suite of comprehensive ICT Security Policies. The Security Policies aim to provide guidance to ANAO staff in the protection of personnel, assets and related facilities.

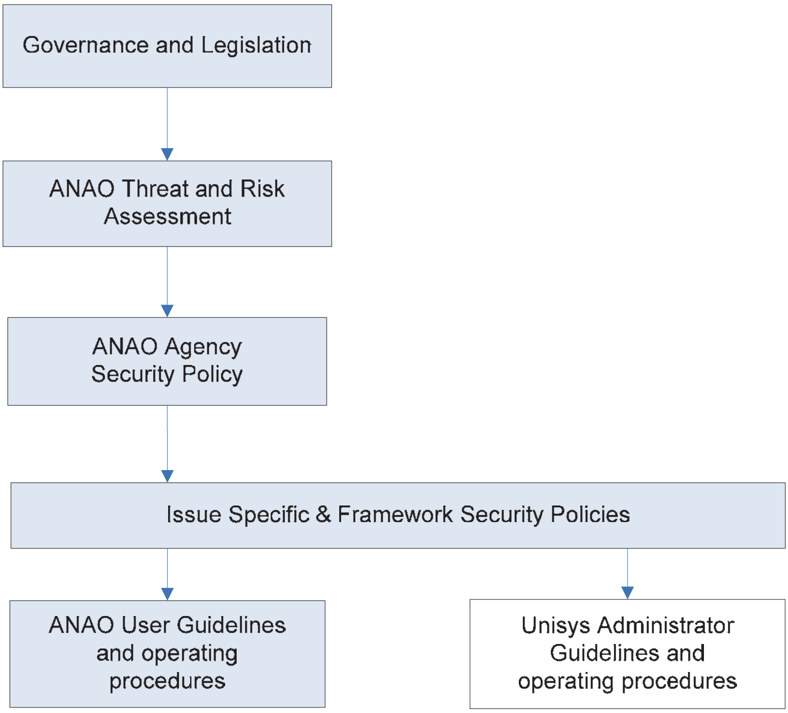
The Security Policy suite encompasses the following key components:

Key ANAO policy document	***Description***
Agency Security Policy	This policy provides guidance to ANAO staff in the protection of personnel, assets and facilities to give effect to the overall Security Plan. Sections covered include personnel security and physical security when working for the ANAO.
IT Security Policy	The IT Security Policy outlines guidance in relation to data confidentiality covering all hardware, software and devices that collectively make up the ANAO’s ICT environment. The IT Security Policy provides the framework for a number of related and system specific policy and operational documents.
Information Classification and Handling Guidelines	This guideline provides guidance to ANAO staff in classifying and protecting ANAO, client and commercially owned data and information.
Personal Computer Facilities Guidelines	This guideline provides guidance to ANAO staff in the effective usage of their personal computer facilities.
Email and Fedlink Usage Guidelines	This guideline provides guidance to ANAO staff in the effective and secure usage of email and usage of Fedlink.
Internet to the Desktop Usage Guidelines	This guideline provides guidance to ANAO staff in the effective and secure usage of the ANAO internet and staff responsibilities.
Internet Café usage Guidelines:	This guideline provides guidance to ANAO staff in the effective and secure usage of the Internet café facility located in the Information Research Centre (IRC).
Home-Based Computing and Secure Remote Access Guidelines:	This guideline provides guidance to ANAO staff that may from time to time need to work from / at home or at a client site using various electronic information processing systems, typically a Notebook and / or a fax machine.

The diagram below outlines the hierarchy of security related documents within the ANAO environment and outlines that at the highest level the Agency Security Policy is the overarching policy.

Diagram 10

Security Policy Hierarchy[11]



Governance and Legislation
ANAO Threat and Risk Assessment
ANAO Agency Security Policy
Issue Specific & Framework Security Policies
ANAO User Guidelines and operating procedures
Unisys Administrator Guidelines and operating procedures

[11] Security Policy Document Hierarchy diagram sourced from the ANAO IT Security Policy.

6.2 User Network and Application Security

The process for creating, modifying and removal of users from the network and key applications (both corporate and business applications) is well defined and documented within the ANAO environment. This includes a mature user access process flow that is neither cumbersome nor onerous on staff to complete and includes the key elements to ensure access is only granted to the network and applications on an 'as needs' basis.

Creating a user

The process for adding a user to the network (and related applications) is initiated through the commencement of employment, whereby Human Resources complete the ANAO's "*User Registration to IT Systems*" form. This form contains the relevant new user information and the required hardware, mail groups and eHive profiles that will be required. The form also contains formal sign off for a delegated ANAO manager as well as sign off from the new user acknowledging the conditions of use of the ANAO's ICT equipment and network.

The form, once signed, is passed to Unisys, where the new user details are added to the ANAO's ICT asset management and service desk system, BMC. BMC is a software tool utilised by Unisys in two ways, firstly as a Service Desk delivery system and secondly to keep track of ICT assets and their life cycle from purchase to disposal.

Once new user information is entered into BMC, it is then added to the ANAO's Microsoft Active Directory network configuration and Microsoft Exchange email. All *"User Registration to IT Systems"* forms are kept in a paper hard copy file for audit purposes.

Modifying a users access

Modifications to a user's access / security is a simple process and is generally initiated by two ways, either via a Service Desk request or the completion of a "*User Registration to IT Systems*" form. In both cases any requests for modification must be approved by the employees' manager.

Once approval is given the process for modification is similar to that of user creation where the request will be given to Unisys to make the required change. The nature of the modification will depend on the tool Unisys use to process the request, for example BMC or Microsoft Exchange.

Deleting/removing user access

For user deletions, a "*Return Authorisation*" form is triggered by Human Resources (HR). A relevant delegated ANAO manager completes and signs the form. The signed form is forwarded to Unisys for processing. In this case, processing includes the disabling of the user account from the network, a checklist is completed to ensure all pieces of ICT equipment registered with that user is returned and laptops are re-imaged.

In cases where laptops have been used to access highly sensitive data, the laptop hard drive is removed and physically destroyed to ensure no data security breaches occur.

A monthly report is generated listing users that have not logged on for 30, 60 or 90 days. No automatic disabling of user access occurs if a user account has been inactive for an extended period of time, however the ICT team do confirm with employees manager and HR as to the status of the user in question.

Application access

Access to applications outside the Standard Operating Environment (SOE), for example Finance One or ChangePoint is request via HR with manager approval.

The ANAO have a well controlled ICT network in place and have implemented port-control on all laptop and desktop computers. This essentially means that external devices (other than that approved and cleared by the ANAO) cannot be used on the network e.g. external hard drives. In addition the ANAO have implemented 'finger print" scan thumb drives to protect information and for staff to use within the network.

No computers within the network have 'administrator' rights; therefore no executable files (such as any application) can be extracted onto a user's computer. In addition to this ICT infrastructure, for example the laptop SOE, has been locked down to prevent un-authorised access and installations of un-supported applications.

User Sample Testing

As part of our investigations thirteen random ANAO "*User Registration to IT Systems*" forms and "*Return Authorisation*" forms were selected. Working with Unisys testing was conducted on each form to ensure the specific request had been carried out. The purpose of this testing is to ensure user creation and removal processes are followed.

For the "*User Registration to IT Systems*" form, each new user request was checked against the setup registered in the Windows Network Active Directory. Primarily this involved looking at the requested security access group of a new user to ensure the correct Active Directory security group has been assigned. Of each "*User Registration to IT Systems*" form selected it was found that the correct security access group has been assigned.

For the "*Return Authorisation*" form, each user removal request was checked to ensure each removal action has been followed. Removal actions include deletion of the Windows Network Active Directory account, deletion of the Windows Shared Folder and return of the users hardware, for example laptop computer. Of the samples looked at each user removal process has been completed and user access to the ANAO network has been removed.

7. ANAO's Backup and Recovery and Business Continuity

A reliable and functioning corporate ICT environment is critical to the delivery of services provided by the ANAO. An important function for ICT support is the process of backup and recovery of the ICT environment.

ANAO have a detailed documented backup and recovery procedures and business continuity plan. Key aspects of these key documents are outlined below.

7.1 Backup and Recovery

ANAO's backup and recovery services are performed and monitored by Information Technology services company Unisys. Unisys have documented the procedures that describe the process.

The backup and recovery document can be summarised as follows:

- *Overview and background* – this covers scope, intended audience, skill set required, technology and toolset required and references to related documents.
- *Backup and Recovery Procedures* – which is further broken up into the ACT and NSW operations. The ACT backup procedures cover both the production and non-production environments. The NSW backup procedures do not distinguish between a production and non-production environment as only a production environment exists for the NSW operations.

The backup procedures (for both the ACT and NSW) consist of three components being the daily, weekly and monthly processes. Each scheduled backup is clearly described and outlines the tape rotation, the type of backup (e.g. full backup) and the respective day(s) of the backup. Backups are monitored and the results, successful or otherwise, are recorded in a backup log.

The rotational backup tapes are stored off site, with the ANAO currently utilising the services of Recall to manage this process. Rotational backup tapes are returned on the next backup cycle.

The backup and recovery document briefly mentions data recovery, however very little detail is provided in terms of specific procedures for the recovery of data, even though monthly tests of data retrieval from backup tapes is carried out. We would suggest further documented detail be provided for the monthly data recovery procedures and the results from this testing be recorded. Refer to **Section 9—Audit Findings and Suggested Improvements** of this report for detail.

In February 2010 Unisys conducted an Enterprise Architecture Review a number of recommendations resulted including focus on Backup and Recovery[12]. Unisys recommended improvements in Backup and Recovery infrastructure to enhance ANAO's Backup and Recovery capability. We acknowledge this recommendation and would encourage the ANAO to consider the options given. Upon speaking with ANAO management they have indicated that the Unisys recommendation outlined was considered for financial year 2009-10, however the ANAO did not proceed as it did not align with current ICT projects and the risk / cost associated with the recommended improvements. The Unisys recommendation will be re-considered for the 2010-11 financial year.

That said, overall the backup procedures are efficient and adhere to industry standards in terms of backup schedules, the checking and logging of backups and tape rotation cycles.

[12] Backup and Recovery recommendations sourced from Section 7, Appendix B – Recommendations of the Unisys Enterprise Architecture Review for the ANAO (Server Architecture).

7.2 Business Continuity

The ANAO's Information and Technology team have prepared a Business Continuity Plan (BCP) document which outlines response procedures in the event of a disaster occurring. The BCP breaks down procedures into four phases being the:

- Response Phase (up to 24 hours);
- Resumption Phase (within five to seven days);
- Recovery Phase (up to 14 days); and
- Restoration Phase.

A separate section exists for the recovery of voice communications.

Each of the above phases contains a checklist of actions to be completed during the event of a disaster occurring. A brief summary of each section is provided below.

Response Phase

The Response Phase involves the immediate response to an incident. Actions include conducting a preliminary damage assessment; initial salvage; retrieval of off-site data.

Resumption Phase

The Resumption Phase involves resuming critical business functions: Actions include LAN services; data communications; and resuming voice communications.

Recovery Phase

The Recovery Phase has a checklist for completion, however no detailed action items. The role of the ICT team during this phase will depend on the severity of the incident that has occurred.

Restoration Phase

The Restoration Phase involves the restoration of normal business as usual operations. The time taken to restore operations is dependent on the seriousness of the incident that has occurred. Actions include liaising with the Building Facilities Team.

Voice Communications Recovery

The Voice Communications Recovery involves the actions surrounding the redirection of incoming calls and media releases during an incident.

The BCP outlines the responsibilities for the Information & Technology team. Specifically, in the event of a disaster the Information & Technology team is responsible for:

- Providing key business sections with an ICT platform as soon as possible after a disaster;
- Ensuring vital voice communication links are re-established as soon as possible;
- Recovering paper records and other information sources; and
- Ensuring all facilities are restored to pre-disaster condition.

The Business Continuity Plan discusses the important aspects required to make up a BCP. The Response Phase, Resumption Phase, Recovery Phase and Restoration Phase are discussed and described. Developed by the ANAO, the BCP is important and fits into the ANAO's overall backup and recovery strategy.

An observation made as part of this performance audit (and recognised by ANAO management) is that there are currently minimal Disaster Recovery (DR) contingencies if major ICT infrastructure was unavailable (e.g. fire damage to the data centre). Minimal DR contingencies would obviously result in a delayed recovery time for key ICT services. Management, however has indicated that this is not a high priority with the ANAO willing to accept the risk associated with this as its ICT applications are non-critical to delivering on its role within the Commonwealth.

8. Software licensing

The ANAO employs the use of a software tool called Express Meter to monitor software and licence usage. For the purpose of monitoring software and related licence usage, all applications shipped in ANAO's Standard Operating Environment (SOE) are tracked by Express Meter. Express Meter is configured to monitor non-standard applications and prevent the execution of non-standard applications should they be installed on local workstations.

Licensing conflicts, should they occur, are communicated to the end user by the Express Meter software client installed in each workstations SOE. The end user will receive a message indicating that the accessed software has exceeded its licence limit and a record of this is logged in Express Meter.

Reports can be run on an ad-hoc basis at anytime. Generally reports are run monthly listing the applications, the frequency of access, who has accessed the application and any recorded licensing conflicts.

Usage and licensing reports are reported to the Chief Information Officer (CIO). From this the CIO will assess the reports and take the necessary actions to address software licence excess or shortcomings.

Reports are generally run on a monthly basis, with key information captured, such as:

- The applications monitored;
- The frequency of access;
- Who has accessed the applications; and
- Any recorded licensing conflicts.

Identifying license excess, for example having purchased 100 licenses for an application and only ever utilising 50 concurrently, is an important end result of active monitoring of software licenses. Through this process ANAO have been able to save approximately $90,000 in license fees, this directly assists the ANAO in achieving its targets for Gershon savings.

9. Audit Findings and Suggested Improvements

It is noted that no formal recommendations were raised as part of this review, however a number of improvement opportunities were noted and as such, are outlined below.

9.1 Improvement Opportunity One – Alignment of the ANAO's Corporate ICT risks to the ICT Strategic Plan

At present there is limited discussion of key ICT risks in the ICTSP and how these risks will be managed by the organisation. Whilst there is a separate risk management process that is established within the ANAO, better practice suggests that these key risks are visible through its strategy and a clear link to the objectives is created.

Improvement Suggestion One
It is suggested that the ANAO consider, in its future consideration of the *ICT Strategic Plan*, creating a clear link from the identified ICT Corporate Risks to the ICTSP.

ANAO Comment: *Agree*

The ANAO accepts the suggestion for improvement. Clear articulation of our IT corporate risks in the *ICT Strategic Plan* will enhance our framework for deciding the priorities and areas for IT investments over the planning cycle. It is proposed that the *ICT Strategic Plan* be reviewed and risks incorporated by 30 June 2010.

9.2 Improvement Opportunity Two – Definition of Key Performance Indicators to measure the ICT Strategic Plan

Whilst the following is acknowledged:

- The ANAO has a range of KPIs and reports for its ICT activities (including monitor of ICT spend, staff surveys, Unisys service delivery reports, post implementation reviews, individual project KPIs and reporting to project boards); and
- The ANAO reviews the ICTSP on a yearly basis.

Additional benefit can be derived from the consolidation of such reports against a selection of KPIs so as to inform progress against broader strategic ICT objectives. It is suggested that the ANAO incorporate the relevant KPIs and targets into the ICTSP so as to assist the yearly deliberations of performance against the ICT strategy as a whole.

Improvement Suggestion Two
It is suggested that the ANAO incorporate the relevant KPIs and targets into the ICTSP so as to assist the yearly deliberations of performance against the ICT strategy as a whole.

ANAO Comment: *Agree*

The ANAO accepts the suggestion for improvement. Incorporation of relevant KPIs and targets into our *ICT Strategic Plan* will assist the reporting and accountability framework. It is proposed that the *ICT Strategic Plan* be reviewed and KPIs and targets incorporated by 30 June 2010.

9.3 Improvement Opportunity Three – Backup and Recovery and Business Continuity

There is minimal detail provided in the Backup and Recovery document in terms of specific procedures for the recovery of data. For clarity, procedures for recovery of data should be documented.

Improvement Suggestion Three
The backup and recovery document briefly mentions data recovery, however very little detail is provided in terms of specific procedures for the recovery of data, even though monthly tests of data retrieval from backup tapes is carried out. It is suggested that further documented detail be provided for the monthly data recovery procedures and the results from this testing be recorded.

ANAO Comment: *Agree*

The ANAO accepts the suggestion for improvement and will coordinate the development of recovery of data documentation and analysis of results of monthly testing with our IT service provider. This will also strengthen our business continuity arrangements. It is proposed that the documentation be completed by 30 June 2010.