The Auditor-General
Audit Report No.4 2006–07
Performance Audit

Tax Agent and Business Portals

Australian Taxation Office

Australian National Audit Office

© Commonwealth
of Australia 2006

ISSN 1036–7632

ISBN 0 642 80922 4

COPYRIGHT INFORMATION

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth.

Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit Barton ACT 2600

http://www.ag.gov.au/cca

Australian National
Audit Office

Canberra ACT
12 September 2006

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit in the Australian Taxation Office in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Tax Agent and Business Portals.*

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

Yours sincerely

Steve Chapman
Acting/Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office. The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits and financial statement audits of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
The Publications Manager
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Telephone: **(02) 6203 7505**
Fax: **(02) 6203 7519**
Email: **webmaster@anao.gov.au**

ANAO audit reports and information about the ANAO are available at our internet address:

http://www.anao.gov.au

Audit Team

Andrew Huey
Elisa Serje
Brenda Canning
Deborah Hope
Peter White

Contents

Abbreviations

ACSI 33	The Australian Government Information and Communications Technology Security Manual – ACSI 33
ANAO	Australian National Audit Office
ATO	Australian Taxation Office
BAS	Business Activity Statement
ECMP	Easier cheaper and more personalised change program
IT	Information technology
SSP	System Security Plan
UDMT	User Directory Management Tool

Summary and Recommendations

Summary

Background

1. The Australian Taxation Office (ATO) provides online services to tax agents and businesses through its Tax Agent and Business Portals. The Tax Agent and Business Portals provide a gateway for tax agents and businesses to access tax information and complete a range of online transactions in a secure environment 24 hours a day, seven days a week. Through the Portals tax agents and businesses can lodge business activity statements, revise previously lodged business activity statements, submit requests for private binding rulings and communicate with the ATO in a secure environment.

2. The Commissioner of Taxation launched the Tax Agent Portal on 3 October 2002. This was six weeks after the ATO made the decision to develop the initial Tax Agent Portal prototype. The ATO developed the Tax Agent Portal in response to criticism and feedback from the tax agent community. An Australian National Audit Office (ANAO) audit of the ATO's relationship with tax practitioners, around this time, concluded that the ATO's relationship with the tax agent community had not been well managed.[1] The initial release of the Tax Agent Portal was a key strategy for the ATO to make it easier for tax agents to fulfil their role within the requirements of Australia's New Tax System and improve its relationship with the tax agent community.

3. The ATO utilised the existing functionality of the Tax Agent Portal to implement a pilot of the Business Portal in June 2003. A limited release of the Business Portal was subsequently undertaken, with the ATO officially launching the Business Portal in March 2004.

Audit objective

4. The objective of the audit was to review the operation of the ATO's Tax Agent and Business Portals. In conducting the audit the ANAO examined three key areas:

- governance – the governance arrangements supporting ongoing management of the Portals;
- portals development, user satisfaction and realisation of expected benefits – the ATO's processes for involving users in developing the

[1] Audit Report No.19 2002–2003, *The Australian Taxation Office's Relationship with Tax Practitioners*.

Tax Agent and Business Portals, assessing user satisfaction, and evaluating business benefits arising from uptake of the Portals; and

- information technology (IT) security and user access controls – the ATO's IT security environment and user access controls supporting the operation of the Tax Agent and Business Portals.

Key audit findings

Governance

5. The ANAO found the ATO has established a governance framework that supports the ongoing management of the Tax Agent and Business Portals. The ATO's strategic and business planning activities supporting operation of the Portals provide clear direction and guidance for their future development. In mid-2006 the ATO commenced a review to better identify risks for its online transaction processes, including the Portals.

6. The ANAO has identified two areas where the ATO's governance arrangements supporting management of the Portals could be enhanced. These relate to the ATO documenting the roles and responsibilities of the Portals business owners and key internal stakeholders, and improving its performance measurement framework. Clearly articulating roles and responsibilities will assist the ATO to adopt a more coordinated approach to managing the Portals. Developing specific performance measures for the Portals will better inform management decision making, particularly regarding future investment in the Portals.

Portals development, user satisfaction and realisation of expected benefits

7. The ATO has been responsive to the need to improve information access for tax agents and expended a considerable effort in quickly developing the Tax Agent Portal. Overall, survey results have shown tax agents' satisfaction with and use of the Portal is high and increasing, and tax agents have experienced savings from using the Portal.

8. Uptake of the Business Portal has been slow, but has improved following the ATO's recent marketing efforts. To better understand its potential market for the Business Portal and the barriers to uptake, as well as inform its marketing and communication campaigns, the ANAO considers the ATO should assess the cost effectiveness of more comprehensively reporting

Business Portal usage and uptake, by market and industry segments. The ATO advised that it recently commenced analysing Business Portal usage by market segment and industry type. Further, the ATO's *Online services marketing communication strategy 2006–07* outlines initiatives aimed at managing businesses' expectations about online services and equipping them with the skills, confidence and support to move online.

9. The ATO advised that with the first release of the Tax Agent Portal, there was no expectation of delivering specific business benefits for the ATO. The imperative was to improve the ATO's relationship with tax agents. The ATO utilised the functionality of the Tax Agent Portal to develop the Business Portal. The ATO therefore regards the Business Portal as an add-on and any related subsequent increased use of its online services as a bonus.

10. The ANAO considers that it is now timely for the ATO to evaluate the administrative efficiencies it has achieved from introducing the Tax Agent and Business Portals. In this regard, the ATO advised that it is developing service delivery targets for each component of the online channel, of which the Portals are a key component.[2]

IT security and user access controls

11. The ATO has provided online real-time access to a number of its business systems through the Tax Agent and Business Portals. The ATO in introducing the Tax Agent Portal aimed to achieve a balance between uptake of the Portal and IT security (i.e. secure online access to taxpayer information). Access to business systems data via the Internet exposes the ATO to an increased level of risk. The ANAO considers that although the ATO has introduced a range of IT security and user access controls, these controls need to be strengthened in several areas to better protect the integrity of the ATO's business systems. Set out below is a summary of the ANAO's findings relating to the four key IT security and user access control issues examined as part of the audit.

IT security planning and architecture

12. The ANAO found in relation to the Portals the ATO requires a more systematic, directed, and comprehensive approach to IT security planning. The

[2] The Tax Agent and Business Portals are a key component of the ATO's online channel. The ATO's online channel is made up of several service delivery tools. The online channel is discussed in more detail in Chapter 1 – *Background and Context*.

ANAO considers that as part of IT security planning for the Portals, the ATO should define the roles and responsibilities of system owners and other key stakeholders. This would support a coordinated approach to future Portals IT security planning.

13. The ANAO considers the Portals' security architecture provides appropriate security over the data flows and information processed by the applications.

Application security controls

14. Appropriate internal application security controls for Portals users have been implemented. These internal application security controls restrict user access to functionality within the application.

15. With regard to external application security controls, the ANAO found that the ATO does not maintain security baselines for all key system security components. The ATO has issued security baseline guidelines for some components, but has not established a formal process for monitoring compliance with the guidelines. The ANAO considers that, without formalised security baselines for all key system security components and ongoing compliance and security enforcement measures, the ATO, through operation of its Portals, may be exposed to a higher level of IT security risk than is considered acceptable.

16. Although control mechanisms for user access to the Portals have been implemented, the ATO's practices supporting the administrator function are not well developed, particularly relating to user access. The ATO's own reviews have also identified that there were limited mechanisms in place to ensure consistency in the process for the authorisation and revocation of Portals user access, and the monitoring and review of internal user access.

IT security monitoring and reporting

17. The ATO does not have the capability for the timely production of a clear and meaningful end-to-end view of a user's actions within the Portals. The ability to trace a user's actions is required to enable the reconstruction of events and to provide an adequate audit trail of user transactions. This is particularly important when reviewing transactions performed to detect possible security breaches. The ATO is undertaking a project to establish processes that will enable a complete view of a user's actions within its systems, including the Portals.

18. The ANAO found that the reporting requirements for security of the Portals are not well defined. Several areas within the ATO and its IT provider monitor and report on security safeguards for the Tax Agent and Business Portals. However, the ATO has not specified the frequency and type of security reports to be produced, nor had it taken steps to ensure the reports were being provided to the appropriate areas. The ANAO considers that the ATO's IT reporting regime restricts the effectiveness of IT security management of the Portals. The ATO is redefining its security reporting requirements.

19. The ATO's IT security incident management process was well established, however, significant incidents were not reported to the Defence Signals Directorate as required.

IT business continuity management

20. In addition to its own business continuity requirements, the ATO is becoming increasingly aware of the dependency that external Portals users, and tax agents practices in particular, have on the online services it offers. Unavailability of the Tax Agent and Business Portals for an extended time may have an adverse impact on the business of external users. The ATO, in October 2005, implemented a disaster recovery solution for the Portals. However, this solution resulted in technical problems during peak processing periods. The ATO advised that it is working on implementing a revised disaster recovery solution.

Conclusion

21. The ATO in developing and implementing the Tax Agent and Business Portals was aiming to make its clients' experience with the taxation system easier, cheaper and more personalised. The ANAO considers that introduction of the Tax Agent and Business Portals has been a significant achievement for the ATO.

22. The ATO's governance arrangements established for the Portals support their ongoing management. The Tax Agent Portal has been well received by the tax agent community. This has assisted the ATO in improving its relationship with tax agents. The Tax Agent and Business Portals have facilitated easier access to information for both tax agents and businesses. Since the Tax Agent Portal was introduced, around 80 per cent of tax agents have accessed it. Surveys undertaken by the ATO indicate a high level of satisfaction with the Tax Agent Portal. The ANAO considers that uptake of the Business

Portal has been slow but has improved with more recent efforts by the ATO to encourage greater business use of the Portal. Around 6 per cent of businesses have accessed the Business Portal.

23. The ANAO concluded that the ATO has implemented a range of IT security and user access controls. The ANAO found that the Portals' IT security architecture provides appropriate security over the data flows and information processed and that appropriate control mechanisms have been implemented for user access. The ANAO also found that the ATO's incident management process was well established. However, the ANAO has identified several areas where the ATO needs to strengthen its IT security and user access controls around the Portals. These include: enhancing IT security planning, strengthening application security controls and user access administration, and improving IT security reporting.

Recommendations

24. The ANAO has made six recommendations. The first recommendation is aimed at strengthening the ATO's processes supporting the ongoing management of the Tax Agent and Business Portals. The remaining five recommendations are focused on improving aspects of the ATO's IT security, in order to preserve the integrity of its online channel.

25. The ATO has agreed to the implementation of the six recommendations.

Summary of agency response

26. We are pleased that the ANAO report concluded that the ATO has established a governance framework that supports the ongoing management of the Tax Agent and Business Portals. The ATO's strategic and business planning activities support the operations of the portals and provide clear direction for their future development. We are pleased with the increasing level of satisfaction reported by the tax agents and that the portal is providing savings for this important intermediary. We have made some inroads in the uptake of the Business Portal by recent marketing initiative and will continue to focus on this area. The Online Marketing Strategy developed from research of market and industry segments is expected to see an increase in uptake.

27. The Tax Office welcomes the acknowledgement from the ANAO that in introducing the portals we have aimed to achieve a balance between uptake of the portal an IT security. The Tax Office agrees with the IT Security

recommendations aimed to strengthen controls in several areas to better protect the integrity of the ATO's business systems.

28. The ATO's full response is at Appendix 1.

Recommendations

Recommendation No.1
Para. 2.24

The ANAO recommends that the ATO develop its performance measurement framework to provide assurance that the Tax Agent and Business Portals are effective and delivering business benefits for the ATO.

ATO response: Agreed

Recommendation No.2
Para. 4.11

The ANAO recommends that the ATO, in order to enhance the IT security planning function for the Tax Agent and Business Portals:

- review the IT security controls in place for existence, appropriateness and consistency; and
- clearly define the roles and responsibilities of system owners and other key stakeholders to better support systematic and coordinated cross-agency forward planning activities.

ATO response: Agreed

Recommendation No.3
Para. 4.19

The ANAO recommends that, to reduce the level of IT security risk associated with operating the Tax Agent and Business Portals, the ATO strengthen its application security controls by establishing:

- information technology security baselines for the Portals;
- a process to provide timely assurance that security baselines have been appropriately implemented and maintained; and
- ongoing compliance or enforcement mechanisms to provide assurance that application security controls are operational and effective.

ATO response: Agreed

Recommendation No.4
Para. 4.30

To strengthen user access administration for the Tax Agent and Business Portals, the ANAO recommends that the ATO:

- implement processes, which are aligned with the ATO's IT Security Policy, for the regular review of user access;
- formally endorse guidelines for the internal audit of administrator activities; and
- ensure that responsibility for auditing administrator activities and reviewing access registers is clearly understood by the relevant areas.

ATO response: Agreed

Recommendation No.5
Para. 4.49

To improve IT security reporting for the Tax Agent and Business Portals, the ANAO recommends that the ATO:

- review its IT security reporting requirements and determine how these can best be met; and
- specify the type of reports required, their content and frequency of production and distribution.

ATO response: Agreed

Recommendation No.6
Para. 4.55

To ensure compliance with Australian Government IT security incident reporting requirements and to improve the transparency of IT security incident management, the ANAO recommends that the ATO review its IT security incident reporting.

ATO response: Agreed

Audit Findings and Conclusions

1. Background and Context

This Chapter discusses development and implementation of the Australian Taxation Office's Tax Agent and Business Portals. This includes a discussion around the uptake and use of the Portals by the tax agent and business communities. The Chapter concludes by outlining the audit objective and methodology.

Background to the Portals

1.1 Introduction of Australia's New Tax System in July 2000 created a number of challenges for the Australian Taxation Office (ATO), tax practitioners and the community. The New Tax System involved major changes. These changes had a significant administrative impact on tax practitioners and specifically on tax agents. This adversely affected the relationship between the ATO and tax agents.

1.2 In reviewing the relationship between the ATO and tax agents in 2002-03, the ANAO found that the demands of tax reform had stretched the capacity of many tax agents, some to 'breaking point'. The ANAO concluded that the ATO's relationship with tax agents had not been well managed and described it as 'strained and tense'.[3]

1.3 In March 2002 the Commissioner of Taxation announced the Listening to the Community project. This involved the ATO working with the general community, including small business, industry and tax agents to identify ways to make it easier and cheaper for people to comply with their tax obligations. Through the project the ATO identified what tax agents and businesses wanted from the ATO in their dealings with them. This included easier access to information held by the ATO and the ability to transact electronically with the ATO.[4]

1.4 In response to criticism from the tax agent community, and based on feedback from tax agents consulted during the Listening to the Community project, the ATO developed an initial prototype of the Tax Agent Portal. This was part of the ATO's overall approach to improving its relationship with tax agents. The initial release of the Tax Agent Portal was a key strategy to make it easier for tax agents to fulfil their role within the requirements of Australia's

---

[3] Audit Report No.19 2002–2003, *The Australian Taxation Office's Relationship with Tax Practitioners*.

[4] Information about the ATO's Listening to the Community project is presented in the *Making it easier to comply*, *The cheaper easier and more personalised program* booklets available from the ATO's website at <http://www.ato.gov.au>.

New Tax System. The Commissioner of Taxation launched the Tax Agent Portal on 3 October 2002. This was six weeks after the ATO made the decision to develop the initial Tax Agent Portal prototype.

1.5 The ATO also developed the Business Portal in response to feedback received during the Listening to the Community project. The ATO used the existing functionality of the Tax Agent Portal to implement a pilot of the Business Portal in June 2003. A limited release of the Business Portal was subsequently undertaken, with the ATO officially launching the Business Portal in March 2004.

The Tax Agent and Business Portals

1.6 At the time of its release the Tax Agent Portal provided tax agents with access to a range of reports, registration and account balance information for their clients. This was static information which the ATO periodically updated. By December 2005 the ATO had completed nine major and two minor releases of the Tax Agent Portal.

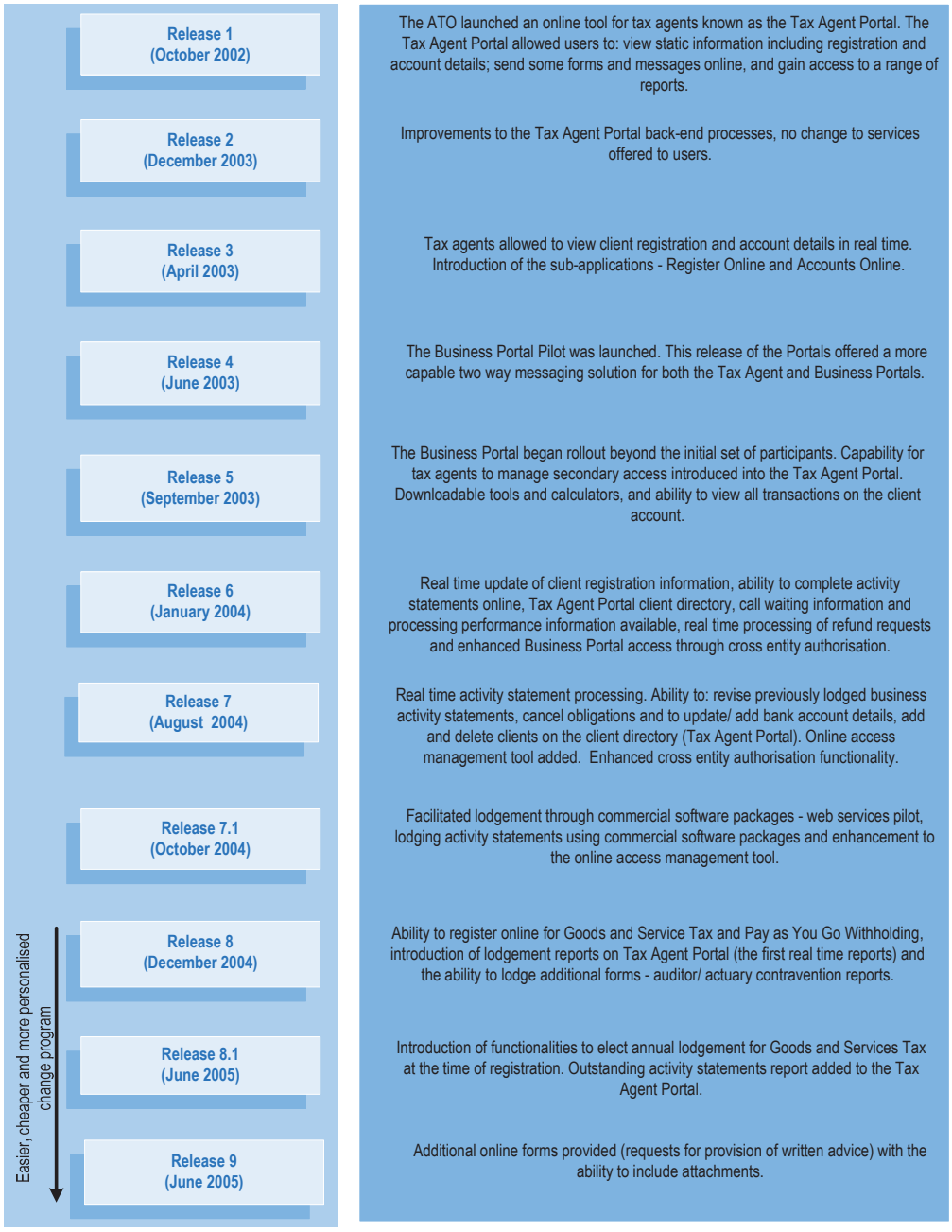
1.7 The Tax Agent Portal now provides tax agents with online real-time access to information the ATO holds. Tax agents can also complete a range of transactions with the ATO, on their clients' behalf. The Tax Agent Portal allows tax agents to lodge and revise activity statements, submit online requests for private binding rulings and request transfers between client accounts and seek refunds.

1.8 The Business Portal was developed to provide a gateway for businesses to access business tax information in a secure online environment 24 hours a day, seven days a week. The Business Portal operates as a separate application to the Tax Agent Portal, although it shares a number of functionalities. The Business Portal allows businesses to lodge and revise activity statements, view accounts, request refund balances and send messages to the ATO.

1.9 Figure 1.1 outlines the functionality introduced with each release of the Tax Agent and Business Portals. The ATO has advised that the cost of developing the Portals was around $43 million. This cost estimate includes both capital and operating costs associated with Portals development.

Figure 1.1

Tax Agent and Business Portals' releases



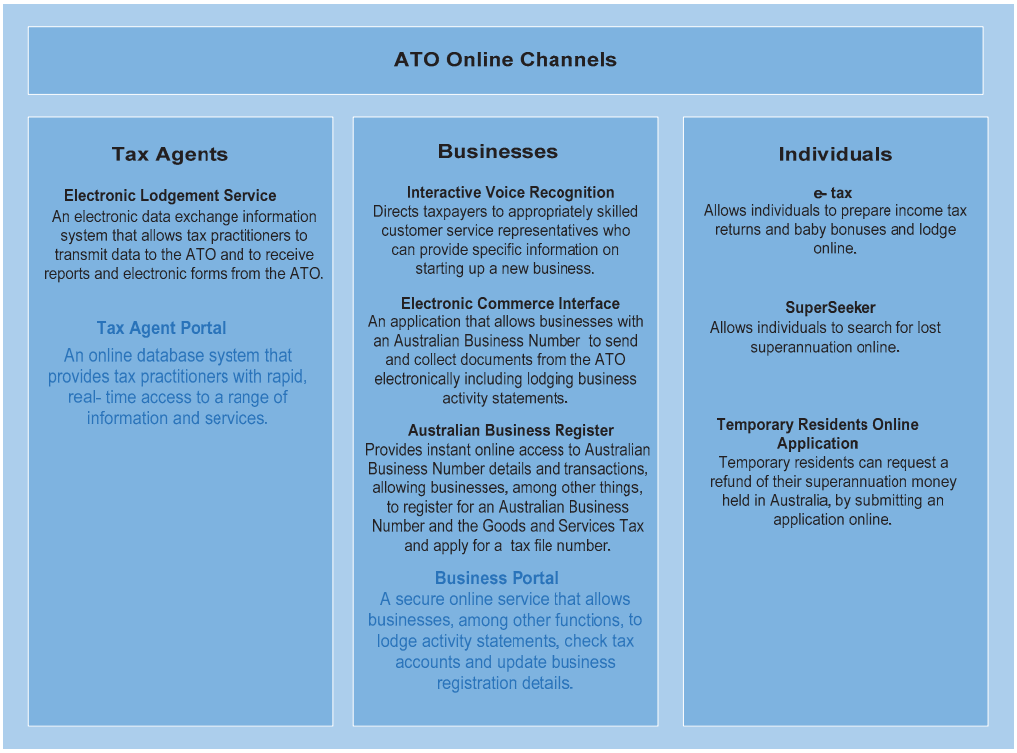
Source: ANAO analysis of ATO information

ATO online environment and uptake of the Portals

1.10 Since 1997 the Australian Government has been moving towards providing online services to the Australian public. The ATO's introduction of the Portals aligns with the Australian Government's broader e-government policy initiatives.[5] The Portals are a key component of the ATO's online channel. Other components of the ATO's online channel are the: Electronic Lodgement Service, Electronic Client Interface, and Interactive Voice Register. Other systems, such as e-tax, also form part of the ATO's approach to facilitating online interactions. Figure 1.2 broadly depicts the online services available to ATO clients.

Figure 1.2

ATO's online services



Source: ANAO analysis of ATO information

1.11 The ATO, in developing and implementing the Tax Agent and Business Portals, was aiming to make its clients' experience with the taxation system

[5] The Organisation for Economic Cooperation and Development (OECD) has defined e-government as the adoption of information and communications technology in order to improve the efficiency and effectiveness of public administration.

easier, cheaper and more personalised. The ATO's Easier, cheaper and more personalised change program (ECMP) Business Case established a number of progressive online service delivery targets. The targets are to be fully realised by 2007–08. To achieve these targets, the ATO is aiming to increase uptake of its online channel. The ATO expects that the community will progressively increase its use of the online channel during the life of the ECMP.

Uptake of the Tax Agent Portal

1.12 Uptake of the Tax Agent Portal has steadily increased since it was introduced in 2002. Between July 2005 and April 2006, approximately 75 per cent of registered active tax agents accessed the Tax Agent Portal.[6] Logins to the Tax Agent Portal have grown from around 4 million in 2003–04 to about 10 million.[7]

Uptake of the Business Portal

1.13 The total number of registered businesses in Australia participating in the taxation system is around 2.4 million.[8] As at May 2006, 133 544 businesses (about 6 per cent of businesses) had accessed the Portal. Between July 2005 and March 2006, 95 635 business logged onto the Business Portal on at least one occasion. During this period around 3 per cent of Business Activity Statements (BASs) were lodged through the Business Portal.

Managing the Portals

1.14 The ATO is a large complex public sector organisation. Underlying this is a matrix management model. In line with the ATO's matrix management model, business ownership of the ATO's Portals is shared across several ATO

---

6 The ATO defines a Tax Agent Portal user as a tax agent who has logged into the Portal on at least one occasion.

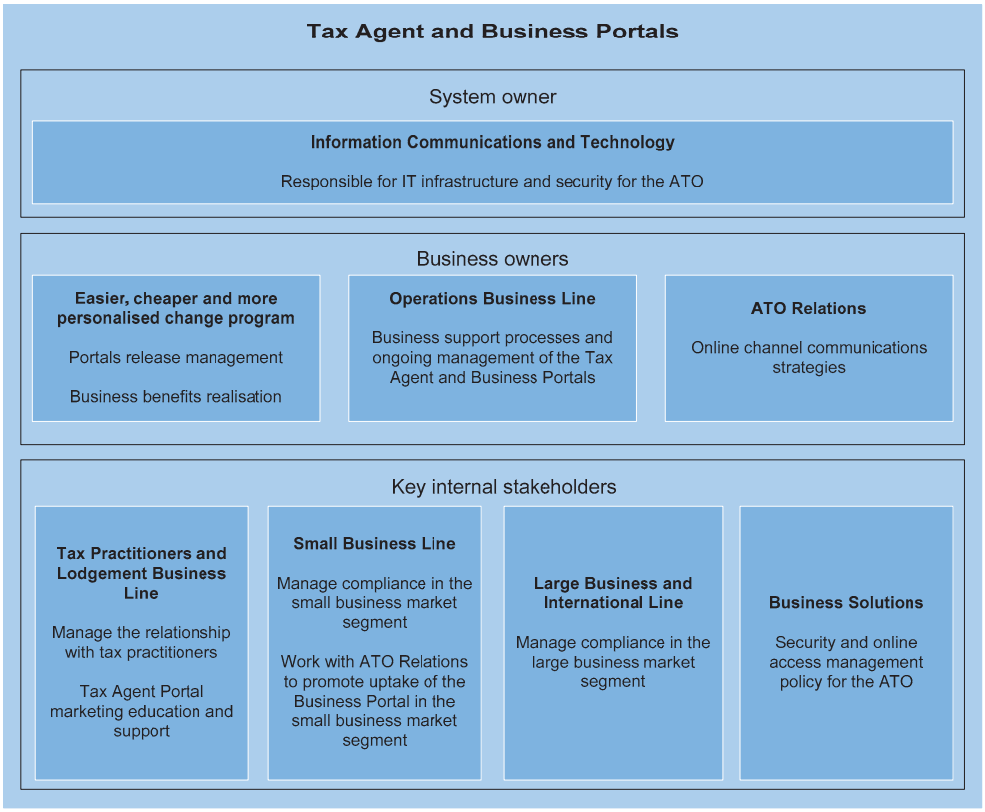
7 In measuring uptake and usage of the Tax Agent Portal the ATO has to consider the structure of the industry. Although there are around 26 000 registered tax agents, only 21 570 agents' registrations are active. The ATO has identified that the majority of tax agents have multiple registrations. Recent Australian Bureau of Statistics research indicates that there are 39 019 businesses providing accounting services in Australia. This would include a range of professional services including book keeping services. Accordingly, it is difficult to accurately determine the number of accounting practices operating in Australia.

8 The ATO has determined that approximately 2.4 million businesses are participating in the taxation system. Australian Bureau of Statistics data published in June 2004 indicates that there are about 3 million businesses in Australia. Not all registered businesses have an Australian Business Number. However the Australian Business Number is the main means of capturing information about the number of businesses operating in Australia. Corporate business structures and cross–business ownership makes a more precise calculation of the number business entities operating in the taxation system difficult.

business and/or service lines. A number of other business areas also have a strong interest in the operation of the Tax Agent and Business Portals. These key internal stakeholders have varying roles, ranging from promoting and supporting their clients in using the Portals, through to providing information technology (IT) infrastructure and services. Figure 1.3 identifies the Tax Agent and Business Portals system owner, business owners and key internal stakeholders.

Figure 1.3

Portals' ownership and business line functional responsibilities



Source: ANAO analysis of ATO information

Audit objective and methodology

Audit objective

1.15 The objective of the audit was to review the operation of the ATO's Tax Agent and Business Portals. In conducting the audit the ANAO examined three key areas:

- governance – the governance arrangements supporting ongoing management of the Portals;
- portals development, user satisfaction and realisation of expected benefits – the ATO's processes for involving users in developing the Tax Agent and Business Portals, assessing user satisfaction, and evaluating business benefits arising from uptake of the Portals; and
- IT security and user access controls – the ATO's IT security environment and user access controls supporting the operation of the Tax Agent and Business Portals.

Audit methodology

1.16 The audit included a combination of interviews with ATO business line staff and key private sector stakeholders, and an examination of the ATO's systems and processes supporting operation of the Portals. Fieldwork was undertaken at ATO offices in Adelaide, Brisbane, Canberra and Melbourne. Fieldwork involved consultation with staff from the ECMP, Tax Practitioners and Lodgement Business Line,[9] Small Business Line, Large Business and International Line, Operations Business Line, ATO Relations, Information Communication and Technology, and Business Solutions. The ANAO engaged the services of an IT consulting company to assist its IT Branch to examine aspects of the ATO's IT security environment and access controls around the Portals.

1.17 The audit was undertaken in conformance with ANAO auditing standards and cost $335 221.

Acknowledgements

1.18 The ANAO would like to thank the ATO officers who assisted in the conduct of the audit, for their time, effort and expertise. The ANAO also appreciates the co-operation and assistance of private-sector stakeholders consulted during the audit.

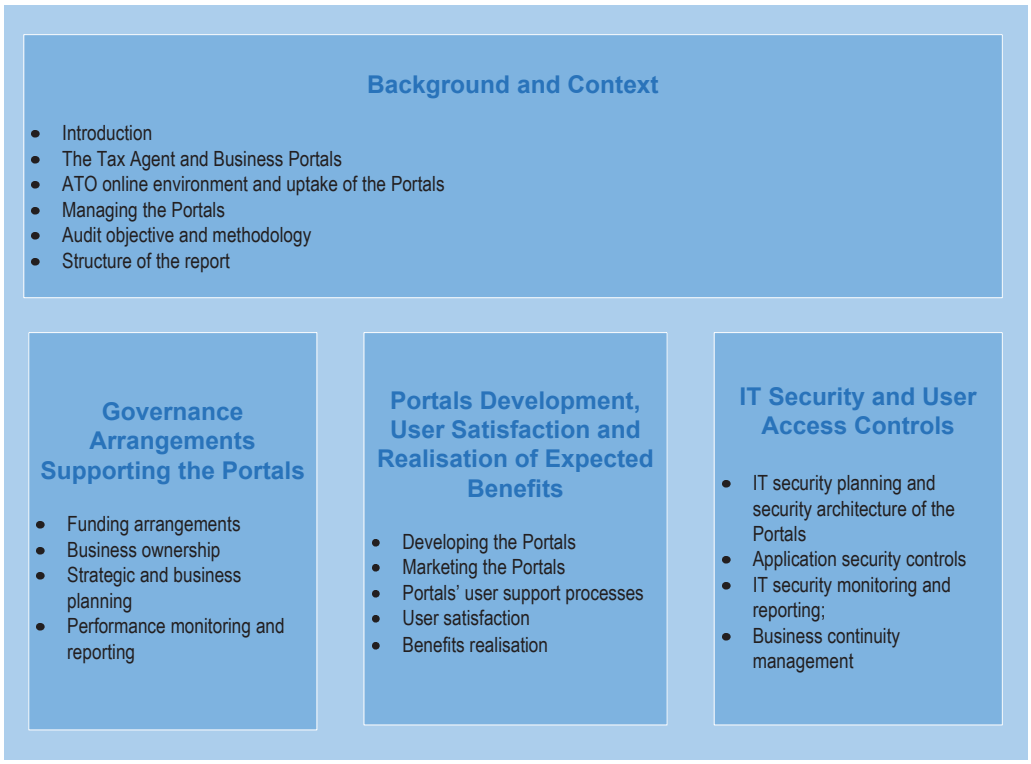
Structure of the report

1.19 Figure 1.4 depicts the structure of the report. The report is structured around the three areas examined as part of the audit.

[9] The Tax Practitioner Group of the Personal Tax Business Line was integrated into the newly formed Tax Practitioners and Lodgement Business Line in mid-2006. Fieldwork for the audit was under taken in the former Tax Practitioner Group.

Figure 1.4

Report structure



2. Governance Arrangements Supporting the Portals

This Chapter discusses the ATO's governance arrangements that support the ongoing management of the Tax Agent and Business Portals.

Introduction

2.1 Development and implementation of governance arrangements that support the effective management of agencies' IT systems, such as the ATO's Tax Agent and Business Portals, are important. These arrangements and underlying systems and processes support the ATO in making informed decisions about the most strategic use and development of its Portals.

2.2 The ANAO has examined four key governance issues in relation to the Portals:

- funding arrangements;
- business ownership, associated responsibilities and how the business owners interact;
- strategic and business planning; and
- monitoring and reporting of performance.[10]

Funding arrangements

2.3 In developing and implementing IT systems it is important for agencies to account for their investment and consider the outcomes to be derived from this investment. Development of the Tax Agent and Business Portals was included in the ECMP Business Case, with their development funded through the ECMP Sub-Plan. The ATO self-funds the ECMP through realisation of efficiencies and other business benefits. The ATO's ECMP online services business benefits are discussed in Chapter 3 – *Portals Development, User Satisfaction and Realisation of Expected Benefits*.

2.4 The Tax Agent and Business Portals are the first publicly visible output of the ATO's ECMP. The ATO advised that the cost of developing the Portals, as at 31 December 2005, was approximately $43 million. This estimate excludes

[10] For further information about public sector governance refer to the ANAO's Better Practice Guide, *Public Sector Governance*, available at <http://www.anao.gov.au>. As well, CPA Australia published a guide in 2005 entitled *IT Governance, A Practical Guide for Company Directors and Business Executives*.

general operating costs incurred in 2004–05. The ATO was unable to identify operating costs associated with Portals development during this period as general operating costs were only captured for the ECMP as a whole. The ANAO was advised that in 2005–06, the ATO amended its cost centre structure to allow costs attribution to each ECMP deliverable.

Business ownership

2.5 Good governance suggests that business and IT solutions should be supported by sound decision making and clear roles and accountabilities. The ANAO found that the responsibilities and accountabilities of the business owners of the Portals and the involvement of internal stakeholders was not documented and required clarification. The ANAO considers that documenting these roles and improving the coordination between the business owners would support more effective management of the Portals.

2.6 The ANAO noted that in late 2005, the ATO formed an Online Access Management Group. This group was formed to bring together all business areas that have accountability in relation to delivery of and changes to online access management across the ATO. The ANAO considers that formation of the group is a sound initiative and demonstrates that the ATO is adopting a more coordinated approach to managing its online services.

2.7 Overall, the ANAO considers that the ATO should continue to adopt a more coordinated approach to managing the Tax Agent and Business Portals at the business and service line level. A well-coordinated approach helps the ATO provide effective and efficient online services through the Tax Agent and Business Portals. The ANAO further considers that the ATO should define the responsibilities and accountabilities of the Portals' business owners and relevant internal stakeholders. The ATO has advised that it will do so.

Strategic and business planning

2.8 Strategic and business planning are important elements of an effective governance framework. The ATO has established a cascading model that supports strategic and business planning at several levels within the organisation. Strategic and business planning in relation to the Tax Agent and Business Portals has been successfully integrated into the ATO's broader planning framework. Due to cross-business-line responsibilities for the Portals, it is difficult in some instances to identify the outputs of the individual

business areas. This is to be expected as technical and business support processes for the Portals are part of the ATO's business-as-usual

2.9 The ECMP Sub-Plan and Business Case detail the ATO's key deliverables relating to the Portals. The ANAO considers that, overall, the ECMP Sub-Plan and Business Case provide clear direction and guidance for future development of the Portals.

Risk management

2.10 The ATO's risk and issues management process is articulated in its internal policy document, *Corporate Management Practice Statement Risk and Issues Management*. The Practice Statement details the framework within which risks and issues are to be managed. The ANAO found that risks associated with the Portals have been identified at several levels. However, the focus has largely been on managing the risks associated with a particular release of the Portals.

2.11 The ANAO found that the ATO's approach to managing risks associated with business-as-usual operation of the Portals has been somewhat reactive. The ANAO considers that as part of its planning processes, the ATO needs to identify and assess the risks associated with operating the Portals. These risks should then be managed in line with the ATO's corporate approach to risk management. The ATO commenced in mid-2006 a risk review of all transaction processes including form lodgement, registration, accounting and the relationship between these functions. The review is also expected to identify risks for each channel including the Tax Agent and Business Portals.

Fraud control planning

2.12 The *Commonwealth Fraud Control Guideline, May 2002,* require agencies to prepare complying fraud risk assessments and fraud control plans. Risk assessments must consider fraud risks to the agency, both from within the agency and from external factors.[11]

2.13 The ATO reviewed the fraud risks associated with the Tax Agent and Business Portals in late 2004. Internal fraud threats associated with ATO staff access to both the Tax Agent and Business Portals were considered. The review included Portals Releases 1 to 8 and formed part of the ATO's overall ECMP Fraud Control Plan. The ATO subsequently reviewed Release 9 and completed

[11] Attorney-General's Department, *Commonwealth Fraud Control Guidelines, May 2002*, pp. 2 and 9.

a pre-release assessment of Release 10. These reviews also focused on assessment of internal fraud risks.

2.14 Fraud incidents experienced by the ATO have highlighted the need for the ATO to identify and manage potential fraud risks and threats associated with the Portals. Failure to manage fraud risks can result in loss of Commonwealth revenue, personal information, and the community's confidence in the ATO's ability to effectively manage aspects of the taxation system. The following case study summarises the details of a fraud committed through use of the Tax Agent Portal.

Case study

Tax Agent Portal fraud

In June 2005 a financial institution advised the ATO of suspicious activity on an account containing a large refund paid by the ATO. Investigations by the ATO revealed that the refunds were issued to clients represented by 11 Victorian tax agents. The refunds arose through the fraudulent amendment of BASs for 23 tax agent clients.

The perpetrator of the fraud was a registered Victorian tax agent who obtained identity information for 23 tax agents. The agent was then able to pass the ATO's proof-of-identity tests and have the Tax Agent Portal passwords reset. This allowed the agent to change a range of client details including address, contact and bank account details.

Through revision of BASs the tax agent generated a number of refunds to fraudulent bank accounts. A total of approximately $1.5 million was paid into the fraudulent bank accounts. Once identified the ATO was able to prevent a further $9 million from being paid.

The alleged perpetrator has been charged with a variety of criminal offences and has appeared before court. The ATO anticipates it will be able to recover approximately $1.2 million.

Reparation work was still ongoing as at March 2006, with 126 cases requiring remedial action. The ATO had issued 59 new Tax File Numbers and a further 67 requests for replacement had been received.

2.15 During the course of the audit a tax agent's access information was collected by a Trojan virus[12]. This information, along with several Tax File Numbers and Australian Business Numbers, was published on an overseas website. The ATO commenced proceedings to manage the implications arising from this incident. The ANAO noted that to manage risk of this nature, the ATO has undertaken extensive user awareness in order to influence users to maintain appropriate IT security controls. These controls help users prevent fraudulent access to information either stored on or accessed through their IT systems.

[12] A Trojan virus is a program that presents to the user as being safe. However, hidden within the program is some code which can cause damage to a user's system or be of nuisance value.

Information technology threat and risk assessments

2.16 The ANAO noted that the ATO had previously commissioned several external threat and risk assessments of the Portals. These assessments have considered both internal and external threats, largely from an IT security perspective. In March 2006 the ATO commissioned a review of external threats for all ATO revenue products. The assessment is to cover business and IT risks. A key outcome of the assessment is identification of any perceived risk areas that would require mitigation in order to maintain the integrity of the ATO's refund processing. The ANAO was advised that through the ATO's risk management processes this information will feed into the ATO's revenue product fraud control plans. The fraud control plans once prepared will be passed to the Audit Committee for endorsement.

Performance monitoring and reporting

2.17 Performance management is fundamental to sound governance. Regular monitoring and reporting of performance helps management make informed decisions. Management can allocate resources, identify areas for improvement, assess the achievement of outcomes, and fulfil both internal and external accountabilities.

External reporting

2.18 External reporting in relation to the Tax Agent and Business Portals is rolled into ECMP reporting. The ATO has published two updates to its *Making it easier to comply, The easier, cheaper and more personalised program* booklet. In these documents the ATO outlines its commitments to the community and what has been delivered as part of the ECMP. Delivery of particular functionalities for the Portals has been reported as part of this process. The ANAO noted that the ATO has delivered the specified Portals functionality.

Internal reporting

2.19 As part of the audit the ANAO reviewed the measurement and reporting of the performance of the Portals to the ECMP Executive. The ECMP Executive reports to the ECMP Steering Committee, which is effectively the ATO Executive.

2.20 The ANAO observed that a range of information relating to different aspects of the Portals has been reported to the ECMP Executive monthly.[13] This has included progress against the ECMP Business Case and uptake of the Tax Agent and Business Portals. Table 2.1 summarises the ATO's expected benefits from implementing the Portals, their measures and associated targets, where stated.

Table 2.1

General and ECMP expected benefits

Benefit	Measure	Target
Increased take-up of Tax Agent and Business Portal	Logins and page hits and the impact of marketing campaigns on awareness.	No targets set.
Fewer client queries/interactions with the ATO.	Portal usage versus account-related calls (measured only for the Tax Agent Portal).	No targets set.
Client satisfied with Portals.	Measured through surveys.	No targets set.
Cost of compliance reduced.	Measured through surveys.	Qualitative measure.
Improvement in electronic lodgement of activity statements. Less manual processing by the ATO through increase in electronic lodgement of activity statements.	Electronic lodgements as a percentage of total lodgements.	2004-2005 38% 2005-2006 40% 2006-2007 43% 2007-2008 50%
Less manual processing by the ATO through increase in activity statement revisions lodged electronically.	Activity statement revisions raised as a percentage of activity statement revisions received.	By end June 2005 17% By end June 2006 41% By end June 2007 65% By October 2007 70%
Less manual error correction through reduction in activity statement exceptions.	Number of exceptions raised as a percentage of activity statements lodged.	2004-2005 8.86% 2005-2006 8.86% 2006-2007 8.44% 2007-2008 8.15% 2008-2009 7.86%
Reduction in call volumes (transactional call).	Reduction in volume of calls to the call centres due to new/improved online functionality.	5% per year for three years from July 2005.

Note: The measures shaded in grey are general measures, not ECMP Business Case business benefit measures.
Source: ANAO analysis of ATO information

2.21 The ANAO found that overall the Portals' contribution to the online service delivery targets is relatively small. For example, on average around 21 per cent of BASs lodged electronically are processed through the Portals. This equates to about 7.5 per cent of total BAS lodgements.

[13] Reporting of ECMP Business Case business benefits to the ECMP Steering Committee commenced in January 2006.

2.22 The ANAO considers that the ATO's approach to measuring the performance of its Portals could be improved. Several business lines measure and report on different aspects of the Portals' performance based on their operational requirements, but the ATO does not assess the overall effectiveness of its Portals, the associated costs and achievement of their expected benefits in a systematic or coordinated manner.

2.23 The ANAO considers that the ATO should develop and implement a performance measurement framework that supports the ongoing assessment of the ATO's Portals as part of the online channel. Development of specific performance measures for the Portals or segmentation of existing measures would support informed management decision making about investment in the Portals and/or related activities. The ATO advised that from a marketing communication perspective, it is developing clearly defined effectiveness measures for the business portal using a marketing metric framework. The framework includes online targets, channel migration plans, market and user research.

Recommendation No.1

2.24 The ANAO recommends that the ATO develop its performance measurement framework to provide assurance that the Tax Agent and Business Portals are effective and delivering business benefits for the ATO.

Agency response

2.25 Agreed.

2.26 From a marketing communication perspective the ATO is already developing clearly defined effectiveness measures for the Tax Agent and Business Portal using a marketing metric framework which includes:

- online targets;
- channel migration plans; and
- market research and user research.

3. Portals Development, User Satisfaction and Realisation of Expected Benefits

This Chapter discusses the ATO's processes for involving users in developing the Tax Agent and Business Portals, marketing the Portals, user support processes and monitoring and evaluating the benefits arising from uptake of the Portals.

Introduction

3.1 The Tax Agent and Business Portals are online services the ATO provides to make tax agents' and business entities' experience with the taxation system easier, cheaper and more personalised. As noted in Chapter 1 – *Background and Context*, the Portals have been developed through a series of releases. Sound management practice suggests that users' requirements should be considered in developing online services such as the Tax Agent and Business Portals. In developing online services there also needs to be a balance between meeting users' requirements and achieving efficiency or other business benefits.

3.2 To assess whether the Tax Agent and Business Portals have met user needs and achieved expected benefits for the ATO and users, the ANAO examined the ATO's:

- development and implementation of the Portals including its processes for consulting with tax agents and other stakeholders in the design and development of the Portals;
- approach to marketing the Portals, and communicating with and supporting its users;
- assessment of user satisfaction; and
- processes for measuring and reporting on the realisation of business benefits.

Developing the Portals

3.3 The ANAO noted that, since their initial implementation, the Tax Agent and Business Portals have been regularly updated with improved layout, navigation and additional functionality. Development of the Portals has been influenced by the ATO's findings from the Listening to the

Community project and feedback from users and key internal stakeholders. The ANAO observed that the ATO has given priority to implementing changes to the Portals in line with its published commitments[14] and then to resolving system related issues. The ECMP Executive and Steering Committee have played a key role in reviewing proposed Portals' enhancements and approving the content of the releases.

3.4 The ANAO noted that the ATO has used several existing consultative forums to collect feedback from external users; these have included the ATO Tax Practitioner Forum, Electronic Working Group, Accounting Working Group and Small Business Advisory Group. As well, users have provided feedback to the ATO through the Portals or by email. The ATO has also involved tax agents in developing the Portals through a formalised co-design process. The ATO has used this co-design process since Release 6 to engage users in developing and testing significant Portals functionality. A Simulation Centre is used to bring together end users, developers and ATO business areas.

3.5 The ANAO considers that the ATO has actively involved tax agents in developing the Tax Agent Portal. The ATO has been responsive to the need to improve information access for tax agents and expanded the functionality of the Portal through a series of rapid releases. The co-design concept has been a sound approach, which has supported Tax Agent Portal development and business process redesign.

3.6 The ATO advised that, since Release 7, investment in the Portals has been scaled back. The ATO is planning to redevelop the Portals during the later stages of the ECMP. The ATO advised tax agents in early 2006 that it is not making further significant investment or enhancements to the Portals until after 2008.

Implementation of the Business Portal

3.7 The ECMP Executive decided to develop and implement the Business Portal in the absence of a business case. The ANAO considers that at that time, the ATO did not have a sound understanding of the needs of businesses. The ATO aimed to address this issue by conducting a Business Portal pilot and evaluating a controlled release. These activities built on feedback the ATO received during the Listening to the Community project.

[14] For further information refer to the *Making it easier to comply*, *The cheaper easier and more personalised program* booklets available from the ATO's website at <http://www.ato.gov.au>.

3.8 The ATO's pilot of the Business Portal involved 20 small and 25 large businesses. Of the pilot participants, 16 could access the Business Portal, eight attempted to access the Business Portal, and six successfully logged onto the Business Portal.[15] Several pilot participants experienced technical difficulties. In September 2003 around 20 000 businesses were invited to participate in a controlled release of the Business Portal. These ATO business clients had previously indicated their willingness to deal electronically with the ATO. The ATO subsequently completed several sample-based surveys to assess participants' experience.

3.9 The ATO officially launched the Business Portal in March 2004. This was despite technical difficulties that some users experienced and the low levels of participation in the September 2003 release. The business market consists of approximately 2.4 million businesses. As at May 2006, 133 544 businesses had accessed the Business Portal.

3.10 The ANAO considers that, although the Business Portal is largely an add-on of the Tax Agent Portal, the ATO should have more actively considered businesses needs when developing it. Before investing in development of the Business Portal, the ATO should have undertaken an assessment of expected demand, business benefits and potential return on investment. This more considered approach would align with the Gateway Review Process (Gateway) the Australian Government has recently adopted.[16] The ATO advised that the cost of developing the Business Portal was minimal as it was able to use functionality developed as part of the Tax Agent Portal. The ATO views any increased use of its online services as a bonus.

Marketing the Portals

3.11 The ANAO considers that, to achieve a high level of uptake of the Tax Agent and Business Portals, the ATO needs to have in place marketing/communication, education and support strategies. These strategies should be targeted at both existing and potential users. This is particularly important as the ATO is aiming to move tax agents and business entities from its traditional paper lodgement channel to the online channel. This results in efficiencies and costs savings for the ATO and the ability to provide online

[15] The evaluation report produced by the Small Business Line for the June 2003 pilot showed that, of the 28 small businesses that participated in the pilot, only five used the Portal to perform a transaction or to interact with the ATO.

[16] Further information about the Gateway Review process can be found at: <http://www.finance.gov.au/gateway/index.html>.

services to its clients. Portal users can also access real-time information and conduct business electronically with the ATO.

3.12 Responsibility for marketing the Portals is shared between the Tax Practitioners and Lodgement Business Line[17] and ATO Relations. The Tax Practitioners and Lodgement Business Line has concentrated its efforts on marketing the Tax Agent Portal, while ATO Relations has primarily worked with the Small Business Line to market the Business Portal.

Marketing the Tax Agent Portal

3.13 The Tax Practitioners and Lodgement Business Line markets the Tax Agent Portal as part of its broader responsibilities of increasing awareness and educating tax agents about ATO products. The group uses various media including newsletters, email broadcasts, online updates and seminars to inform tax agents about Tax Agent Portal issues.

3.14 Tax practitioners consulted during the audit expressed mixed views about the quality of information disseminated about the Tax Agent Portal. Overall, tax agents were more satisfied with the information provided when the Portal was first introduced. The ANAO noted that the Tax Practitioners and Lodgement Business Line has segmented tax agents and is tailoring some of its communication activities in order to better meet its clients' needs.

3.15 The ANAO observed that, although the ATO considers that it has reached saturation point with uptake of the Tax Agent Portal, many of the Portal's functions are used on an infrequent basis. Anecdotal evidence suggests that tax agents' knowledge of the different functions that can be performed within the Portal could be enhanced. The ATO advised that it is exploring opportunities to enhance tax agents' knowledge of specific functions available within the Portal.

Marketing the Business Portal

3.16 The micro business market segment accounts for about 98 per cent of business entities operating in Australia.[18] Due to its size, this segment provides the greatest opportunity for increased use of the Business Portal. In late 2005 ATO Relations began a three-phase Online Services Marketing program

---

[17] The Tax Practitioner Group of the Personal Tax Business Line was integrated into the newly formed Tax Practitioners and Lodgement Business Line in mid-2006. Fieldwork for the audit was under taken in the former Tax Practitioner Group.

[18] Micro businesses are those businesses with a turnover of between $50 000 and $2 million per year.

(known as the 'Cookie Campaign'). The aim of the program was to encourage uptake and use of the Business Portal by small to medium enterprises and micro businesses. The campaign cost $1.5 million and, as at the end of December 2005, had resulted in 53 417 new users of the Business Portal.[19] The ANAO noted that it is too early for the ATO to evaluate the longer term impact of the Cookie Campaign. The campaign is outlined in the following case study.

Case study

Cookie Campaign

The ATO's Cookie Campaign was a three-phase program aimed at increasing the number of small to medium enterprises and micro businesses adopting the Business Portal.

The Campaign was undertaken between June 2005 and March 2006, in a staged approach. It was largely based on a creative advertising concept of a fortune cookie and conveyed the benefits of businesses going online with the ATO. The concept tested well in focus groups and involved production of a promotional compact disc (CD), which was sent to 2 million quarterly BAS self lodgers. This was supported by advertising in major metropolitan, suburban and regional newspapers, the *My Business* magazine and metropolitan and regional radio stations.

The campaign cost $1.5 million and resulted in 53 417 new users of the Business Portal. The ATO has estimated that overall it has a 65 per cent retention rate of Business Portal users.

3.17 The ATO realises efficiencies and costs savings through increased use of its online services, including the Business Portal. Through its Cookie Campaign the ATO has focused on moving business entities from paper BAS lodgement to online BAS lodgement. This results in an approximate cost saving for the ATO of $5.60 per BAS lodgement.

Future strategies for marketing the Portals

3.18 The ATO has established a Marketing, Education and Relationships Committee. The Committee has a role in connecting groups involved in managing the ATO's interaction with the community. Consistent with the Committee's role, the ATO began an integrated marketing program for online services. This was a marked departure from past marketing efforts, which were largely undertaken by separate business lines independent of each other. The ANAO considers this a positive step towards better coordinating marketing activities, and establishing a framework for monitoring and evaluating the effectiveness of the ATO's marketing strategies.

3.19 The ANAO suggests that, as part of its planning processes supporting the marketing of its online services, including the Business Portal, the ATO

[19] Since the Cookie Campaign started, in June 2005, 53 417 new users registered to access the Business Portal. This significant increase in registration has been directly attributed to the campaign.

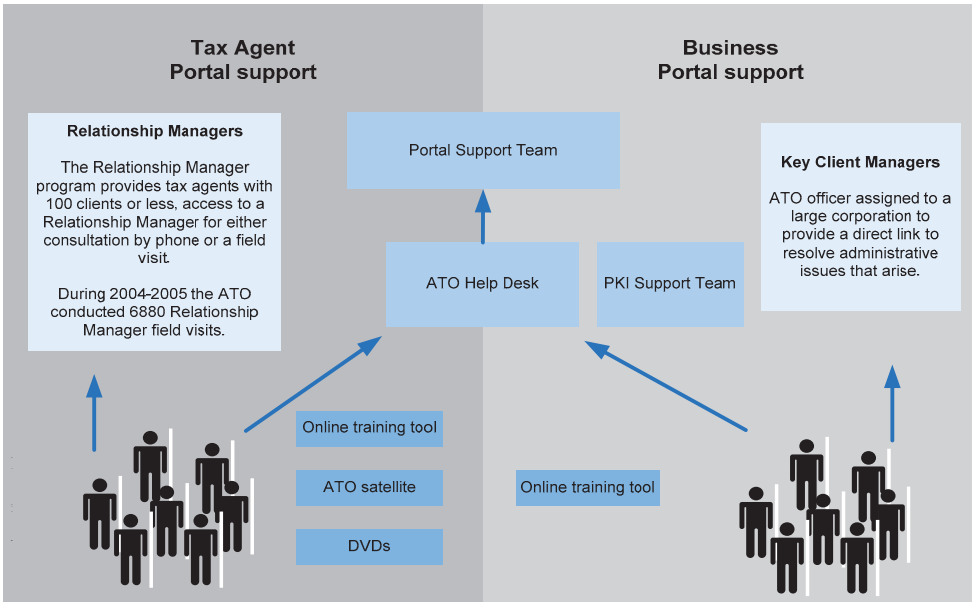
develop an evaluation model. The model should document expected benefits and focus on the longer term impact. The ATO advised that it is addressing this issue by developing a marketing metrics framework. The framework is to include business performance measures (i.e. achievements against online targets), market and user research. This will be used to develop future marketing strategies and to monitor and evaluate the return on investment of existing strategies.

Portals' user support processes

3.20 The ATO uses a combination of Portal-specific and non-Portal-specific support services, to help Portals users. Figure 3.1 provides an overview of the support services available to Portals users. The ATO Help Desk and Portals Support Team largely provide users with business-as-usual support for the Portals. Specific support issues are also addressed by the Tax Practitioners and Lodgement Business Line, the Small Business Line and the Large Business and International Line.

Figure 3.1

Tax Agent and Business Portal Support



Source: ANAO analysis of ATO information

Tax Agent Portal support

3.21 The Tax Practitioners and Lodgement Business Line provides tax agents with information about the Tax Agent Portal through is marketing and education programs. The ANAO noted that the Tax Practitioners and Lodgement Business Line has used several means to communicate information about the Tax Agent Portal to tax agents. This has included training digital versatile discs (DVDs), satellite broadcasts, email broadcast, newsletters and one-on-one support through the Relationship Manager program.[20]

3.22 Tax agents and key private sector stakeholders consulted during audit fieldwork provided the ANAO with mixed feedback about the ATO's Portal support processes. Tax agents indicated that they preferred to interact directly with the ATO in seeking support or assistance. Positive views were expressed about the ATO's satellite seminars and other forums where tax agents are able to interact in person with the ATO. A number of tax agents consulted during the audit suggested the ATO increase the frequency of the satellite seminars. The ANAO noted that knowledge and use of the Tax Agent Portal online training tool was limited.

3.23 The ANAO found that tax agents had considerably different awareness levels of the Tax Agent Portal. Those agents who used the Relationship Manager program and attended ATO forums appeared to have a greater understanding of the Portal and its functions. The ANAO considers that if the ATO reviewed the effectiveness of its existing support processes, it could improve the level of support offered to Tax Agent Portal users. Such a review would help the ATO better understand the support needs of Tax Agent Portal users, and their preferred methods of accessing support. As part of this process the ATO may need to differentiate between users on the basis of size, geographic location and other factors.

Business Portal Support

3.24 The Small Business Line, Large Business and International Line and Business Solutions provide a range of support services and products for Business Portal users. These services include a help desk, support through the

[20] The Relationship Manager program was developed in response to the Listening to the Community project findings. The program has been designed to provide tax agents with a number of specialised support and issue resolution services.

Key Client Manager program[21] and more recently ATO field visits for large businesses. The latter has been a cross-business line initiative.

3.25 Implementation and uptake of the Business Portal has been affected by technical issues and the perceived complexity of the digital certificate process. The ATO has begun promoting its help desk services to small businesses. The Help Desk can help Business Portal users resolve technical issues, including issues about digital certificate setup. The ATO is aiming to equip small businesses with the skills they need to move from the paper channel to the online channel.

3.26 The ANAO suggests that in order to improve both users' satisfaction with the Business Portal and to address barriers to uptake, the ATO continue to assess the actual and perceived support needs of Business Portal users. This information should be used to guide the further development and delivery of support services. The ATO advised that recent online marketing services research and analysis of Business Portal usage has been used to assist it in identifying the support needs of potential and current users. Further, the ATO's *Online services marketing communication strategy 2006–07* outlines initiatives aimed at managing businesses' expectations about online services and equipping them with the skills, confidence and support to move online.

User satisfaction

3.27 To measure user satisfaction, the ATO monitors uptake and usage of the Tax Agent and Business Portals and undertakes periodic user surveys. The ATO uses this information to tailor its marketing, education and support services for Portals users.

Tax agent satisfaction and uptake of the Tax Agent Portal

3.28 The Tax Practitioners and Lodgement Business Line has undertaken a series of communication, technology and Tax Agent Portal surveys. As part of this process the Tax Practitioners and Lodgement Business Line has explored tax agents' perceptions about the usefulness of the Portal. The ANAO noted that the Portal has been well accepted by the tax agent community. Around 84 per cent of tax agents surveyed used the Portal daily. In the November 2005 Tax Agent Portal Evaluation Survey, 86 per cent of respondents gave the Tax

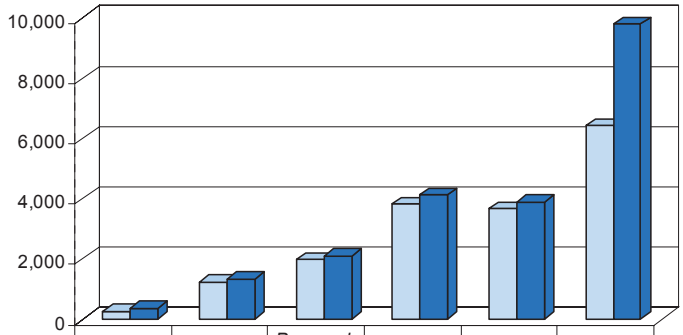
[21] Large businesses are generally assigned an ATO key client manager, thereby giving them a central contact point within the ATO. The key client manager regularly liaises with its large business clients to resolve emerging issues and facilitate provision of advice etc.

Agent Portal the highest rating possible for usefulness to their practice. Tax agents, in responding to the 2005 Tax Agent Communication Survey, nominated the Tax Agent Portal as their most frequently used method of communicating with the ATO. Overall, survey results have shown tax agents' satisfaction with and use of the Portal is high and increasing and that tax agents have made savings from using the Portal.

3.29 Uptake of the Tax Agent Portal has been substantial, with around 17 000 tax agent practices logging onto the Portal at least once since its implementation (see Figure 3.2). As of 28 May 2006 there were 21 570 active registered tax agents. During 2005–06 around 75 per cent of registered active tax agents accessed the Portal.

Figure 3.2

Tax Agent Portal uptake



	Top shelf/ 2nd tier	High bulk	Personal tax focussed	Medium	Small	Micro
Used the Tax Agent Portal at least once	274	1,226	1,980	3,823	3,667	6,439
Total number of practices in segment	380	1,326	2,111	4,130	3,897	9,810

Source: ANAO analysis of ATO data

3.30 The ANAO considers that it is now timely for the ATO to gain a better understanding of Tax Agent Portal usage. Such research should focus on understanding what Portal functions are used by tax agents and differentiate between recurrent active users and occasional users. This approach would be consistent with the findings made by the Australian Government Information Management Office in its report, *e-Government Benefits Study* published in April 2003. That study found that most agencies need to better measure adoption and take up of their online services.

Business Portal uptake and user satisfaction

3.31 The ATO monitors uptake and use of the Business Portal monthly. The ANAO found that, overall, about 6 per cent of businesses had accessed the Business Portal. In late 2005 the ATO commissioned a research project into Online Services. Since the survey was not Business Portal specific, it did not consider business satisfaction with the Portal, the frequency of use, or other user satisfaction indicators as addressed by the tax agent surveys.

3.32 The ANAO observed that the ATO reports some information on Portal usage by market segment. To better understand its potential market for the Portal and the barriers to uptake, as well as inform its marketing and communication campaigns, the ANAO considers the ATO should assess the cost effectiveness of more comprehensively reporting Business Portal usage and uptake, by market and industry segments.

Benefits realisation

3.33 Sound management practice suggests that the business benefits expected to be realised from developing and implementing IT systems, should be clearly articulated in a business case. The business benefits should be regularly measured and reported and this information used to justify further development of the systems.

3.34 The ATO advised that with the first release of the Tax Agent Portal, there was no expectation of delivering specific business benefits for the ATO. The main focus was on improving tax agents' access to information and, in turn, improving the ATO's relationship with them. The ATO first documented the business benefits to be derived from implementing the Tax Agent and Business Portals in December 2004. The business benefits were documented in the ECMP Business Case.

3.35 The ECMP Business Case identifies a number of online objectives and associated business benefits. These are expected to be realised through increased use of the ATO's online channel, including the Tax Agent and Business Portals. From July 2008, the ATO is aiming to realise financial savings of approximately $8.7 million per year. This is expected to be achieved through:

- increased online lodgement and revision of BASs;

- a reduction in BAS exceptions resulting from automated error detection during preparation;[22] and
- a reduction in calls to ATO call centres.[23]

Reporting the business benefits of the Portal

3.36 Reporting on the ECMP Business Benefits to the ECMP Executive and ECMP Steering Committee commenced in January 2006. The ATO measures and reports its cumulative performance against its online activity and associated financial savings targets, as outlined in the ECMP Business Case. The ATO is currently on or ahead of target for its three main measures. These are online BAS lodgements, online BAS revisions and a reduced number of BAS exceptions as a percentage of total BAS lodgements.

3.37 The ANAO found that the reports do not provide sufficient information to support ongoing management of the Portals. The information reported is aggregated and does not highlight the Portals' contribution to the online targets. The ANAO acknowledges that more detailed quarterly reports are prepared; however, there was no intention of reporting on the separate components of the ATO's online channel, or their individual contribution to the business benefits targets.

3.38 The ANAO considers that more informed reporting of business benefits at the channel sub-level would help ATO management better understand the online channel. In particular, this would allow management to assess the Portals' contribution to the online service delivery targets. The ATO has advised that it will develop service delivery targets for each online delivery service, including the Portals.

---

[22] The Portals' BAS preparation process includes a number of inbuilt tests to verify information prior to lodgement of the BAS. The Portals user is prompted to review the information recorded if a test is failed.

[23] Access to client account balances and other information has reduced the number of calls to ATO call centres and is expected to continue to do so.

4. IT Security and User Access Controls

This Chapter discusses the effectiveness of the ATO's IT security and user access controls supporting operation of the Tax Agent and Business Portals.

Introduction

4.1 The ATO has provided online real-time access to a number of its business systems through the Tax Agent and Business Portals. The ATO in introducing the Tax Agent Portal aimed to achieve a balance between uptake of the Portal and IT security (i.e. secure online access to taxpayer information). To this end, access to the Tax Agent Portal was initially provided through PIN/password (user ID and Password) authentication. The ATO is now moving tax agents to the more secure Public Key Infrastructure technology (digital certificate authentication).

4.2 Access to business systems data via the Internet exposes the ATO to an increased level of risk. Such exposure mandates the need for appropriate precautionary measures to be taken in order to preserve the integrity of online transactions.

4.3 IT systems such as the Tax Agent and Business Portals are made up of a number of complex components. If any of these components are compromised, this may allow an internal or external party to exploit the resulting vulnerability. Security controls and assurance activities, such as monitoring, reporting, ongoing compliance and awareness, all help to act as safeguards to reduce the risk of exposure. However, such measures will not fully mitigate all security risks, and the ATO must therefore accept and aim to manage a level of residual risk

4.4 During the audit, the ANAO examined the effectiveness of the ATO's IT security and user access controls supporting the operation of the Tax Agent and Business Portals. The specific areas of focus were:

- IT security planning and the security architecture of the Portals;
- application security controls within the Portals and supporting IT environment;
- IT security monitoring and reporting; and
- business continuity management.

IT security planning and security architecture of the Portals

IT security planning

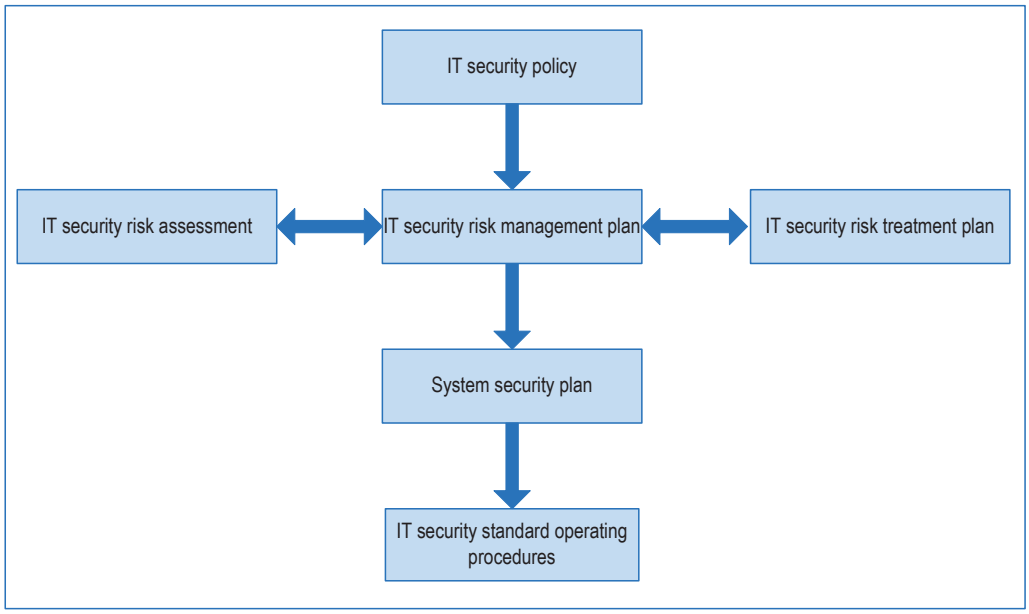
4.5 The ANAO noted that the ATO has a documented framework for IT security planning. The framework, which is supported by the ATO's IT Security Policy and the IT Security Process Handbook, has evolved over recent years to become more closely aligned with The Australian Government Information and Communications Technology Security Manual – ACSI 33, issued by the Defence Signals Directorate (ACSI 33) and the Commonwealth Protective Security Manual.[24]

4.6 ACSI 33 requires that every system is covered by a risk management plan and System Security Plan (SSP). The risk management plan comprises an IT risk assessment and IT risk treatment plan. The risk management plan should identify the risks and appropriate controls or treatments needed to meet the requirements of the agency's security policy. An SSP defines the agency's strategies for implementing the required controls in accordance with the IT security policy and risk management plan. This documentation framework is depicted in Figure 4.1.

[24] The Commonwealth Protective Security Manual (PSM), issued by the Attorney-General's Department, provides the mandatory requirements and guidelines for managing security within government agencies.

Figure 4.1

IT security documentation framework



Source: ANAO adaptation of Government guidelines[25]

4.7 The ATO's IT Security Policy requires that IT security risk assessments are performed and SSPs are developed for IT systems. IT security risk assessments at the ATO take the form of threat risk assessments that provide recommended risk treatments for significant unmitigated risks. The ANAO noted that since 2003 threat risk assessments have been performed for major upgrades to the Portals.

4.8 The ANAO found that before Portals Release 9, the ATO did not define and document the strategies needed to implement all controls identified from both the IT security policy and IT risk assessments. The ANAO noted that the ATO finalised an SSP for the Portals in October 2005.

4.9 The ANAO noted that most of the security controls and safeguards documented in the Portals SSP were those that were known or understood to have already been implemented. In some instances these controls were not fully established, for example the disaster recovery solution for the midrange

[25] Defence Signals Directorate (March 2006), *Australian Government Information and Communications Technology Security Manual* (ACSI 33), Part 1, para. 1.0.23.

platform. The midrange platform is the infrastructure that supports the client-server,[26] as distinct from the mainframe environment, and includes the Portals.

4.10 Some aspects of Portals system security, such as system security architecture, were developed through a documented and well considered process. However, in relation to the Portals, the ANAO considers that the ATO requires a more systematic, directed, and comprehensive approach to IT security planning. The ANAO further considers that as part of IT security planning, the ATO should define the roles and responsibilities of system owners and other key stakeholders. This would support a coordinated approach to future IT security planning. The ANAO notes that the recent establishment of the Online Access Management Group may go some way in addressing these concerns.

Recommendation No.2

4.11 The ANAO recommends that the ATO, in order to enhance the IT security planning function for the Tax Agent and Business Portals:

- review the IT security controls in place for existence, appropriateness and consistency; and
- clearly define the roles and responsibilities of system owners and other key stakeholders to better support systematic and coordinated cross-agency forward planning activities.

Agency response

4.12 Agreed.

4.13 The IT System Security Plan and the Audit Logging Plan were recently updated for the deployment of the Portal 10 Release. To ensure that Plans are complied with, reviews by Trusted Access Branch have been scheduled for 2006–2007. Trusted Access Branch is also close to completing necessary requirements to attain Certification and/or Accreditation of Tax Portal and Business Portal from Defence Signals Directorate or its nominated organisations or assessors.

4.14 These activities are in addition to security activities introduced for Tax Agent Portal 1 (October 2002) to mitigate risks identified in the risk management plan. This includes Threat Risk Assessments and associated risk

[26] A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to a protocol, asking for information or action, and the server responds. <http://computing-dictionary.thefreedictionary.com/client-server>

mitigation plans to address the residual risks. Threat Risk Assessments have been undertaken for each Portal release to assess the risks presented by changes to the architecture or as a result of new functionality. Threat Risk Assessments and mitigation strategies are reflected in the risk management plan to ensure it is up to date.

4.15 Roles and responsibilities of System Owners and Business Owners have been recently redefined to clarify that:

- the owners of systems have coverage for business application systems and underlying infrastructure systems; and
- there will only be one Business Owner to better support cross agency forward planning.

The roles and responsibilities for ATO Systems will be formally endorsed by the IT Executive.

Security architecture of the Tax Agent and Business Portals

4.12 Security architecture defines how a system is constructed to satisfy security requirements. This includes a detailed description of all components (hardware and software) of a system that relate to security, and the set of principles used as a basis for the overall system design. The Tax Agent and Business Portals security framework uses a seven-tier architecture model that supports the Security-in-Depth principle. This principle represents a multi-layered approach to security that mitigates the risk of failure at a single layer.

4.13 The design of the Portals provides for the separation of the public facing, processing and data storage components of the system and is well supported by the security architecture model adopted by the ATO. As part of the audit the ANAO examined the security architecture design and the specific security components established for the Portals. Overall the ANAO considers that these provide appropriate security over the data flows and information processed by the applications.

Application security controls

Internal and external application controls

4.14 Application security controls are those that restrict user access to functionality within the application (internal application controls); and the application's ability to interact with other system components within the IT environment (external application controls). The ANAO reviewed the security

design of the Tax Agent and Business Portals and the functionality of the security components that manage user access within the applications. The ANAO found that appropriate control mechanisms for user access have been implemented.

4.15 The ANAO found that the ATO has based the external application security controls for the Portals on a least privilege model. This model supports provision of a minimum set of access privileges that an application needs to interact with other systems and perform its functions. Three key elements of external application security controls are security baselines, ongoing compliance and security enforcement.

4.16 Security baselines incorporate a list of security settings that have been determined to be the minimum needed to ensure the application is able to operate within the risk level the organisation has accepted. The ANAO found that the ATO does not maintain security baselines for all key system security components.[27] The ATO has issued security baseline guidelines for some components, but has not established a formal process for monitoring compliance with the guidelines.

4.17 Ongoing compliance measures ensure that security controls, established when a system is implemented, are maintained over time in accordance with the accepted level of risk. Security enforcement is a mechanism that actively ensures security settings are maintained. The ANAO found that the ATO's approach to external application security control did not support ongoing compliance or security enforcement. The ANAO further found that no mechanisms have been established to monitor changes to the application security settings. Relevant areas of the ATO were also unaware of the application security settings for the Portals. The ANAO noted that the ATO completes security compliance checks on an infrequent basis.

4.18 The ANAO considers that without formalised security baselines and ongoing compliance and security enforcement measures, the ATO, through operation of its Portals, may be exposed to a higher level of IT security risk than is considered acceptable.

[27] Key system security components may include technologies and platforms, such as operating systems, web servers, database servers or third-party connection software.

Recommendation No.3

4.19 The ANAO recommends that, to reduce the level of IT security risk associated with operating the Tax Agent and Business Portals, the ATO strengthen its application security controls by establishing:

- information technology security baselines for the Portals;
- a process to provide timely assurance that security baselines have been appropriately implemented and maintained; and
- ongoing compliance or enforcement mechanisms to provide assurance that application security controls are operational and effective.

Agency response

4.20 Agreed.

4.21 As indicated in the ANAO report, the ATO has sufficient information security infrastructure and operating system (server level) baselines for the Portal. During 2006–2007, Trusted Access Branch will undertake additional work to establish baselines for other levels of security e.g. application level.

4.22 A review of current baselines is underway to coincide with recent changes in support roles of EDS, the external systems service provider. The review, to be undertaken in consultation with EDS and other ATO security stakeholders will ensure that the baseline documentation remains applicable, clear and relevant.

4.23 Trusted Access Branch has recently developed the Compliance Assurance Blueprint to provide a strategic focus to strengthen compliance and assurance activities. The Blueprint includes a phased implementation plan to assure that controls are operational and effective. This includes assurance of:

- certification of systems;
- user access control;
- administrative and privileged access control;
- transmission media and storage;
- Threat Risk Assessments, Penetration Testing and System Security Plans; and
- the contracts for the external systems service provider, currently EDS.

User access and administration

4.24 Users access the Portals by either PIN/password authentication or Public Key Infrastructure. Tax agents can access the Tax Agent Portal by either means. External access to the Business Portal is by Public Key Infrastructure using digital certificate authentication. Internal (ATO) users of the Portals use PIN/password authentication.

4.25 Public Key Infrastructure provides a stronger means for identifying and authenticating an individual than the PIN/password mechanism. In addition, Public Key Infrastructure provides a non-repudiation[28] security element. The use of digital certificates as part of the Public Key Infrastructure process reduces the risk of identity theft associated with PIN/password authentication.

Administration of user access

4.26 Several business lines and the ATO's IT provider share responsibility for Portals help desk support, assignment of privileged access, and administration of internal and external Portals user access. Users who access the Portals through PIN/password, including all internal users, are managed within a security administration tool called User Directory Maintenance Tool (UDMT). There are approximately 100 ATO UDMT administrators with responsibility for administering access for internal users within their local workgroups.

4.27 The ATO has a well-established devolved security administration structure for its mainframe-based applications. The ATO has determined that local administrators are best placed to verify the access needs of users in their team or workgroup. Access to the ATO's mainframe applications is supported by the regular review of user access by the IT Security area, and routine reporting to ATO governance bodies. The ATO's practices supporting the UDMT administrator function are not as well developed.

4.28 The UDMT Administrator Guidelines document responsibility for the audit of administrator activities and review of access registers. The Guidelines are based on similar procedures for the ATO's mainframe applications. The ANAO found that ATO management has not endorsed the Guidelines and that the documented responsibilities had not been accepted and actioned by the nominated areas.

[28] Non-repudiation is the ability to ensure a party cannot deny the authenticity of their actions.

4.29 Reviews completed by the ATO have identified that there were limited mechanisms in place to ensure consistency in the process for the authorisation and revocation of Portals user access, and the monitoring and review of internal user access. Where processes to allocate, change, review and remove user access for an IT system are not sufficiently formalised, there is a risk that users' access may not be appropriate. In turn, sensitive information may be accessed, viewed or modified by persons who are not authorised to do so.

Recommendation No.4

4.30 To strengthen user access administration for the Tax Agent and Business Portals, the ANAO recommends that the ATO:

- implement processes, which are aligned with the ATO's IT Security Policy, for the regular review of user access;
- formally endorse guidelines for the internal audit of administrator activities; and
- ensure that responsibility for auditing administrator activities and reviewing access registers is clearly understood by the relevant areas.

Agency response

4.31 Agreed.

4.32 ATO IT Security policy includes a requirement that the Administrator conduct 'reviews of audit trails and security logs'. Portal Administrator access is managed through the UDMT. Since December 2005, a weekly script has been run to check whether an internal user has accessed the Portal in the last 13 weeks. If they have not, their access is disabled and an email is sent to them. To strengthen user access controls the UDMT checks will be augmented by conducting more frequent 'Audit and Compliance reviews'.

4.33 Present Guidelines for the audit of administrator activities have been signed off by the Assistant Commissioner Trusted Access. ATO will seek formal endorsement of these guidelines from the ATO Security Committee.

4.34 During 2006–2007, Trusted Access has scheduled comprehensive audits of various Administrator level access to ATO systems, including for Business and Tax Agent Portals. A key part of the audit will be engaging with key stakeholders in the relevant areas to ensure there is a clear understanding of their responsibilities, including regular review of access registers.

Digital certificate migration

4.35 In introducing the Tax Agent Portal, the ATO aimed to achieve a balance between uptake of the Portal and IT security, by providing access through PIN/password authentication. The ATO recognised this type of authentication as an interim measure with the intent of moving tax agents to Public Key Infrastructure or equivalent technology in the future.

4.36 To improve security around access to the Tax Agent Portal following the fraud incident which occurred in 2005,[29] the ATO developed a strategy to migrate tax agents from PIN/password authentication to Public Key Infrastructure. This was a staged approach with the aim of migrating small and medium agents to digital certificate authentication by 31 December 2005 and large tax agents by 31 March 2006. As at 15 January 2006 approximately half of tax agent practices with access to the Tax Agent Portal had been issued with a digital certificate.

4.37 Several issues emerged during the digital certificate migration process.[30] These issues have prevented the ATO from transitioning all tax agents to digital certificate authentication by the proposed dates. In the interim, the ATO has asked tax agents to continue to migrate and those with a digital certificate to continue to use it to access the Tax Agent Portal. The ANAO noted that the ATO is progressively resolving these technical and business issues.

4.38 A further issue which may impact on the ATO's ability to migrate tax agents to digital certificate authentication is tax agents' reluctance to change if the current system is working well. PIN/password authentication is an efficient means for tax agents to access the Tax Agent Portal. The ANAO considers that migrating some tax agents to digital certificate access will therefore pose a considerable challenge for the ATO.

IT security awareness

4.39 In the current IT environment, with access to information through the Internet, it is important for agencies to ensure users have a sound understanding of their responsibilities and the need to maintain appropriate

---

[29] For further details see the Case Study in Chapter 2 – *Governance Arrangements Supporting the Portals*.

[30] Some of the issues included difficulties with the digital certificate installation process, loss of mobile access to the Tax Agent Portal, delays between applying for and the receipt of a digital certificate, and tax agents operating through an entity other than the entity registered with the relevant Tax Agents Board.

security controls. The ATO through the Tax Agent and Business Portals has provided real-time access to taxpayer information for registered users.

4.40 Tax agents are responsible for administering access for their staff. This includes providing and revoking access to client details through the Online Access Manager tool. The ATO relies on security education and awareness to manage external parties' compliance with IT security requirements and sound management practice.

4.41 The ATO, in implementing the Portals, has aimed to ensure users are aware of their obligations and the need to maintain appropriate security controls. Information about their obligations and security more generally has been provided to users through the Portals, email broadcasts, information on the ATO's website and a variety of publications. The ANAO noted that the ATO can revoke a user's access or refuse access to the Portals if that user fails to comply with ATO requirements.

4.42 When consulting with Tax Agent Portal users, the ANAO found limited awareness of IT security issues. Users did not appreciate the significant impact of a security breach on the operation of the Tax Agent Portal or on their clients. The ANAO found that the ATO's IT security awareness program has had limited effect because of users' reluctance to comply with the ATO's guidelines and requirements to maintain appropriate IT security measures. The ANAO suggests that the ATO continue to work with Tax Agent and Business Portals users to increase their understanding of IT security issues.

IT security monitoring and reporting

Logging and monitoring of user access

4.43 The ability to trace the actions of an application user is required to enable reconstruction of events and to support user accountability. This information is critical when investigating or scrutinising transactions performed and is also invaluable in detecting possible security incidents.

4.44 The tracking of user transactions within the Portals needs to be an end-to-end process. Accordingly, the ATO should have the ability to trace a user's actions across the multiple system components and applications that make up the Tax Agent and Business Portals. ACSI 33 advises of the need for

'the correlation of logged events across multiple systems'[31] in order to provide an adequate audit trail of user transactions.

4.45 The ANAO noted that the ATO produces a number of application logs for the Portals and other related system components. The ANAO found that the ATO does not have the capability for the timely production of a clear and meaningful end-to-end view of a user's actions within the Portals. The ANAO also noted that the extent of fragmentation of the monitoring function has contributed to delays and limited the effectiveness of this process.

4.46 In March 2006 the ATO implemented a new software monitoring tool that has enhanced the ATO's system monitoring capabilities. The tool also includes security monitoring functionality, which the ATO does not presently use. The ANAO observed that the ATO is also undertaking a Centralised Audit Logging Project. A key objective of this project is to establish processes that will enable a complete view of user actions within the ATO systems, including the Portals. The ANAO considers that this is a sound initiative, which is expected to significantly enhance the ATO's ability to track a user's actions within the Portals.

IT security reporting

4.47 Overall responsibility for implementing, monitoring and reporting security safeguards for the Tax Agent and Business Portals is assigned to a number of areas within the ATO and its IT provider. As part of the most recent contract extension, from July 2005, the IT provider was assigned management of the midrange platform. Where agencies rely on third-party service providers to perform some IT security functions, it is important that contractual arrangements are put in place to afford access to the information that agencies need to manage IT security.

4.48 The ANAO found that the reporting requirements for security of the Portals are not well defined. The ATO had not specified the frequency and type of security reports the IT provider was required to provide; nor had it taken steps to ensure reports received were being provided to the appropriate areas within the ATO. The ANAO considers that the ATO's IT reporting regime restricts the effectiveness of IT security management of the Portals. The ATO advised that the security reporting requirements are being redefined as part of the second phase of the IT provider contract extension.

---

[31] Defence Signals Directorate (March 2006), op cit., Part 3, para. 3.7.16.

Recommendation No.5

4.49 To improve IT security reporting for the Tax Agent and Business Portals, the ANAO recommends that the ATO:

- review its IT security reporting requirements and determine how these can best be met; and
- specify the type of reports required, their content and frequency of production and distribution.

Agency response

4.50 Agreed.

4.51 The ATO has contracted to EDS a substantial component of the IT facilities operations and support. In line with the current Compliance Assurance Blueprint, a review of reporting requirements has been undertaken. This review focussed on the roles and responsibilities for the ATO and EDS as outlined in service level agreements and how reporting, including escalation of issues, could be improved to be more consistent and effective. Reporting on Security Incidents will be by exception and based on clearly articulated and understood criteria, including when to report and to whom. The Reporting criteria will be regularly reviewed.

4.52 As indicated above the majority of security reporting will be initiated by EDS because they have coverage for the Gateway, PKI infrastructure support, and the Midrange server environments. Accordingly, the security reporting requirements are being redefined as part of the second phase of contract negotiations with EDS.

IT security incident management process

4.53 The ANAO found the ATO's IT security incident[32] management process to be well established. The process for notifying, recording, actioning and escalating IT security incidents is clearly documented and understood by those involved in the management process. It was noted, however, that the reporting of specific IT security incidents to ATO governance bodies is not a defined

[32] An IT security incident is an event that has an impact on the confidentiality, integrity or availability of a system through an act of unauthorised access, disclosure, modification, misuse, damage, loss or destruction.

process and that reports produced from the IT security incident register[33] are not standardised.

4.54 Under ACSI 33, it is a requirement that agencies report significant IT security incidents to the Defence Signals Directorate.[34] Incidents are categorised on a scale of one to four in order of severity, with categories three and four being defined as 'significant'. The ANAO noted that a small number of Portals' related IT security incidents have occurred in recent years. Although appropriate responses were given to these IT security incidents, reporting of significant incidents to the Defence Signals Directorate was not undertaken.

Recommendation No.6

4.55 To ensure compliance with Australian Government IT security incident reporting requirements and to improve the transparency of IT security incident management, the ANAO recommends that the ATO review its IT security incident reporting.

Agency response

4.56 Agreed.

4.57 The ATO already has a strong IT incident management process. This will be further strengthened by ATO wide participation in an Education and Awareness Campaign. This will ensure:

- adequate compliance with service wide obligations through a better understanding of the reporting requirements;
- incidents are correctly categorised; and
- appropriate incidents are notified to external authorities.

Business continuity management

4.58 Business continuity management aims to reduce, or mitigate, the risk of interruptions to key business resources required to support critical business activities. An IT disaster recovery plan is the component of business continuity management that is focused on the technological issues associated with

---

[33] Maintenance of an IT security register is a requirement under ACSI 33. The detailed requirements for such a register are also defined within the manual. Defence Signals Directorate (March 2006), op. cit., Part 2, para. 2.8.21.

[34] Defence Signals Directorate (March 2006), op. cit., Part 2, para. 2.8.30.

business continuity. A disaster recovery plan defines how the business will recover its IT operations in the event of a major disruption, such as a disaster or major incident. Typically, a disaster recovery plan also defines timeframes for recovery, based on the criticality of applications.

4.59 The ATO is becoming increasingly aware of the dependency that external Portals users, and tax agents practices in particular, have on the online services it offers. Unavailability of the Tax Agent and Business Portals for an extended time may have an adverse impact on the business of external users. Further, any unplanned outages have the potential to pose a significant risk to the ATO's reputation.

4.60 The ANAO noted that before late 2005, no overarching disaster recovery plan had been in place for the midrange platform that supports the Portals. In the event of a major disruption to the platform the recovery time could have extended to several weeks. The ANAO acknowledges that some measures were in place to recover from a disruption that was isolated to the Portals. This recovery strategy included use of system backup media and provided for a minimum recovery time of 24 hours.

4.61 In October 2005 the ATO implemented a disaster recovery solution for the midrange environment. The solution was based on data replication for the midrange platform and systems. This provided for recovery of Internet-facing systems including the Portals within four hours. However, it was found that the data replication process caused some technical faults during peak data processing periods for the ATO's Internet-facing systems, including the Portals. For this reason, data replication was turned off during February 2006, and turned on again in March 2006 following this peak period. The ATO advised that it is working on implementing a different data replication technology which supports high workloads for its Internet-facing systems.

Steve Chapman
Acting/Auditor-General

Canberra ACT
12 September 2006

Appendix

Appendix 1: Agency Response

Australian Government
Australian Taxation Office

SECOND COMMISSIONER OF TAXATION

Mr Ian McPhee
Auditor General
Australian National Audit Office
19 National Circuit
Barton ACT 2600

Dear Mr McPhee

Thank you for your letter of 26 July 2006, from Executive Director Peter White and the opportunity to provide comments on the proposed performance audit report on the Australian Taxation Office's administration of the Tax Agent and Business Portals.

We are pleased that the ANAO report concluded that the ATO has established a governance framework that supports the ongoing management of the Tax Agent and Business Portals. The ATO's strategic and business planning activities support the operations of the portals and provide clear direction for their future development. We are pleased with the increasing level of satisfaction reported by the tax agents and that the portal is providing savings for this important intermediary. We have made some inroads in the uptake of the Business Portal by recent marketing initiative and will continue to focus on this area. The Online Marketing Strategy developed from research of market and industry segments is expected to see an increase in uptake.

The Tax Office welcomes the acknowledgement from the ANAO that in introducing the portals we have aimed to achieve a balance between uptake of the portal and IT security. The Tax Office agrees with the IT Security recommendations aimed to strengthen controls in several areas to better protect the integrity of the ATO's business systems.

The full text of the Tax Offices response to the report's recommendations is at Appendix A.

Should you wish to discuss this matter further please contact Robert Ravanello on (02) 62166946.

Thank you for the constructive and co-operative approach to this performance audit. I would like to commend the work to you of your team, particularly Mr Andrew Huey, who were committed and thorough in their dealings with Tax Office representatives throughout the course of the audit.

Yours sincerely

Greg Farr
Second Commissioner
22 August 2006

PO BOX 900 CIVIC SQUARE ACT 2608 AUSTRALIA
ADDRESS
+61 (0)2 6216 1111
TELEPHONE
+61 (0)2 6216 2743
FACSIMILE

Appendix A

Performance Audit – Tax Agent and Business Portals – ATO Response to ANAO Recommendations

Ref.	Recommendation	ATO Response
2.24	Recommendation 1 – The ANAO recommends that the ATO develop its performance measurement framework to provide assurance that the Tax Agent and Business Portals are effective and delivering business benefit for the ATO.	**Agree.** From a marketing communication perspective the ATO is already developing clearly defined effectiveness measures for the Tax Agent and Business Portal using a marketing metric framework which includes: • online targets • channel migration plans • market research and user research.
4.11	Recommendation 2 – The ANAO recommends that the ATO, in order to enhance the IT security planning function for the Tax Agent and Business Portals: • reviews IT security controls in place for existence, appropriateness and consistency; and • clearly defines the roles and responsibilities of system owners and other key stakeholders to better support systematic and coordinated, cross agency forward planning activities.	**Agree** 1. The IT System Security Plan (SSP) and the Audit Logging Plan were recently updated for the deployment of the Portal 10 Release. To ensure that Plans are complied with, reviews by Trusted Access Branch have been scheduled for 2006-2007. Trusted Access Branch is also close to completing necessary requirements to attain Certification and/or Accreditation of Tax Portal and Business Portal from Defence Signals Directorate (DSD) or its nominated organisations or assessors. These activities are in addition to security activities introduced for Tax Agent Portal 1 (October 2002) to mitigate risks identified in the risk management plan. This includes Threat Risk Assessments (TRAs) and associated risk mitigation plans to address the residual risks. TRAs have been undertaken for each portal release to assess the risks presented by changes to the architecture or as a result of new functionality. TRAs and mitigation strategies are reflected in the risk management plan to ensure it is up to date. 2. Roles and responsibilities of System Owners and Business Owners have been recently redefined to clarify that: • The owners of systems have coverage for business application systems and underlying infrastructure systems • There will only be one Business Owner to better support cross agency forward planning The Roles and responsibilities for ATO Systems will be formally endorsed by the IT Executive.

Ref.	Recommendation	ATO Response
4.19	Recommendation 3 – The ANAO recommends that to reduce the level of IT security risk associated with operating the Tax Agent and Business Portals the ATO strengthen its application security controls by: • information security baselines for the Portals • a process to provide timely assurance that security baselines have been appropriately implemented and maintained; and • ongoing compliance enforcement mechanisms to provide assurance that application security controls are operational and effective.	**Agree.** 1. As indicated in the ANAO report, the ATO has sufficient information security infrastructure and operating system (server level) baselines for the Portal. During 2006-2007, Trusted Access Branch will undertake additional work to establish baselines for other levels of security eg application level. 2. A review of current baselines is underway to coincide with recent changes in support roles of EDS, the external systems service provider. The review, to be undertaken in consultation with EDS and other ATO security stakeholders will ensure that the baseline documentation remains applicable, clear and relevant. 3. Trusted Access Branch has recently developed the Compliance Assurance Blueprint to provide a strategic focus to strengthen compliance and assurance activities. The Blueprint includes a phased implementation plan to assure that controls are operational and effective. This includes assurance of: • Certification of systems • User access control • Administrative & privileged access control • Transmission media and storage • TRAs, Penetration Testing and System Security Plans • The contracts for the external systems service provider, currently EDS.

Ref.	Recommendation	ATO Response
4.27	Recommendation 4 – To strengthen user access administration for the Tax Agent and Business Portals, the ANAO recommends that the ATO: • implement processes that are aligned with the ATO's IT security policy, for regular review of user access; • formally endorse guidelines for the audit of administrator activities; and • ensure that responsibility for auditing administrator responsibilities and reviewing access registers is clearly understood by the relevant areas.	**Agree.** 1. ATO IT Security policy includes a requirement that the Administrator conduct "reviews of audit trails and security logs". Portal Administrator access is managed through the User Directory Management Tool (UDMT). Since December 2005, a weekly script has been run to check whether an internal user has accessed the portal in the last 13 weeks. If they have not, their access is disabled and an email is sent to them. To strengthen user access controls the UDMT checks will be augmented by conducting more frequent "Audit & Compliance reviews". 2. Present Guidelines for the audit of administrator activities have been signed off by the Assistant Commissioner Trusted Access. ATO will seek formal endorsement of these guidelines from the ATO Security Committee. 3. During 2006-2007, Trusted Access has scheduled comprehensive audits of various Administrator level access to ATO systems, including for Business and Tax Agent Portals. A key part of the audit will be engaging with key stakeholders in the relevant areas to ensure there is a clear understanding of their responsibilities, including regular review of access registers.
4.43	Recommendation 5 – To improve IT security reporting for the Tax Agent and Business Portals, the ANAO recommends that the ATO: • review IT security reporting requirements and determine how these can best be met; and • specify the type of reports required, their content and frequency of production and distribution.	**Agree** 1. The ATO has contracted to EDS a substantial component of the IT facilities operations and support. In line with the current Compliance Assurance Blueprint, a review of reporting requirements has been undertaken. This review focussed on the roles and responsibilities for ATO and EDS as outlined in service level agreements and how reporting, including escalation of issues, could be improved to be more consistent and effective. Reporting on Security Incidents will be by exception and based on clearly articulated and understood criteria, including when to report and to whom. The Reporting criteria will be regularly reviewed. 2. As indicated above the majority of security reporting will be initiated by EDS because they have coverage for the Gateway, PKI infrastructure support, and the Midrange server environments. Accordingly, the security reporting requirements are being redefined as part of the second phase of contract negotiations with EDS.

Ref.	Recommendation	ATO Response
4.47	Recommendation 6 – To ensure compliance with Australian Government incident reporting requirements and to improve the transparency of IT security incident management, the ANAO recommends that the ATO review its IT security incident reporting.	**Agree** The ATO already has a strong IT incident management process. This will be further strengthened by ATO wide participation in an Education & Awareness Campaign. This will ensure: 1. Adequate compliance with service wide obligations through a better understanding of the reporting requirements 2. Incidents are correctly categorised, and 3. Appropriate incidents are notified to external authorities.

Index

Series Titles

Audit Report No.1 Performance Audit
Administration of the Native Title Respondents Funding Scheme
Attorney-General's Department

Audit Report No.2 Performance Audit
Export Certification
Australian Quarantine and Inspection Service

Audit Report No.3 Performance Audit
Management of Army Minor Capital Equipment Procurement Projects
Department of Defence
Defence Material Organisation

Better Practice Guides

Legal Services Arrangements in Australian Government Agencies	Aug 2006
Preparation of Financial Statements by Public Sector Entities	Apr 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
AMODEL Illustrative Financial Statements 2004	May 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003
Managing Parliamentary Workflow	Apr 2003
Building Capability—A framework for managing learning and development in the APS	Apr 2003
Internal Budgeting	Feb 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Life-Cycle Costing	Dec 2001
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001
Internet Delivery Decisions	Apr 2001
Planning for the Workforce of the Future	Mar 2001
Contract Management	Feb 2001

Business Continuity Management	Jan 2000
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Managing APS Staff Reductions (in Audit Report No.49 1998–99)	June 1999
Commonwealth Agency Energy Management	June 1999
Cash Management	Mar 1999
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	July 1998
Controlling Performance and Outcomes	Dec 1997
Management of Accounts Receivable	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997
Public Sector Travel	Dec 1997
Audit Committees	July 1997
Management of Corporate Sponsorship	Apr 1997
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Asset Management Handbook	June 1996