The Auditor-General
Audit Report No.16 2000–2001
Performance Audit

Australian Taxation Office Internal Fraud Control Arrangements

Australian Taxation Office

Australian National Audit Office

ISSN 1036-7632

ISBN 0 642 44220 7

Australian National
Audit Office

Canberra ACT
29 November 2000

Dear Madam 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 this report of this audit, and the accompanying brochure, to the Parliament. The report is titled *Australian Taxation Office Internal Fraud Control Arrangements.*

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

P. J. Barrett
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.

Auditor-General reports are available from Government Info Shops. Recent titles are shown at the back of this report.

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

Telephone (02) 6203 7505
Fax (02) 6203 7798
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

Medha Kelshiker
Jon Hansen
Peter White

Contents

Abbreviations/Glossary 7

Summary and Recommendations

Summary 13
- Background 13
- Audit approach 14
- Conclusion 15

Key Findings 17
- Fraud control corporate governance mechanisms 17
- Fraud prevention 19
- Information technology systems 20
- Fraud detection 23
- Fraud investigation 23

Recommendations 25

Audit Findings and Conclusions

1. Introduction 31
   - Fraud prevention and control within the Commonwealth public sector 31
   - Australian Taxation Office 34
   - Audit objective and methodology 38
   - Report structure 40

2. Fraud Control Corporate Governance Mechanisms 42
   - Introduction 42
   - ATO fraud control policy 42
   - Organisational arrangements for internal fraud 43
   - Planning for effective fraud control 47
   - ATO performance assessment framework—internal fraud control 55
   - Conclusion 59

3. Fraud Prevention 61
   - Introduction 61
   - ATO fraud prevention strategy 62
   - Other fraud prevention initiatives 68
   - Other better practice 69
   - ATO Business Line fraud prevention practice 70
   - Conclusion 73

4. ATO Information Technology 74
   - Introduction 74
   - The ATO's information technology and security environment 76
   - IT access control 80
   - Pro-active IT controls—logging access of staff to ATO IT systems 88
   - Conclusion 91

5. Fraud Detection 93
Introduction 93
ATO pro-active fraud detection activities 94
Coordination between the Fraud Prevention and Control Section and ATO Internal Audit 96
Conclusion 98

6. Fraud Investigation 99
Introduction 99
Fraud investigations guidelines 102
Reporting and recording allegations 102
The Case Management System 103
Effectiveness of fraud investigations 106
Prosecution and other remedies 111
Conclusion 113

Appendices
Appendix 1: Relevant reports on fraud control arrangements 117
Appendix 2: Functions of the ATO Integrity Advisory Committee 118
Appendix 3: ATO fraud risk assessment methodology 119
Appendix 4: Materials provided to ATO staff as part of the ATO's Fraud Awareness Program 121
Appendix 5: ATO information technology environment 122
Appendix 6: ATO Secrecy Legislation and Information Technology Security Policy 124
Appendix 7: Senate Economics References Committee Inquiry into the Operation of the Australian Taxation Office, 6 August 1998 127
Appendix 8: Results of Fraud Prevention and Control Section Cases for 1999–2000 128

Index 129
Series Titles 131
Better Practice Guides 133

Abbreviations/Glossary

ABCI	Australian Bureau of Criminal Intelligence
ACS	Australian Customs Service
AFP	Australian Federal Police
AIC	Australian Institute of Criminology
AMT	Access Management Team. A group within the ATO IT Security Section responsible for the coordination, training and support of the Workplace Access Administrators.
ANAO	Australian National Audit Office
APS	Australian Public Service
ATO	Australian Taxation Office
ATO Extra	ATO's weekly internal publication
CAATS	Computer Assisted Audit Techniques
CD-ROM	Compact Disc-Read Only Memory. A form of optical storage, which exploits digital coding of information and laser technology to provide fast and flexible searching of large volumes of data.
CLEB	Commonwealth Law Enforcement Board
CMS	Fraud Prevention Case Management System. A computer-based system to facilitate better administrative management of fraud investigations.
Certificate of Compliance	A process involving a detailed assessment of both internal and external risks that may impact on a new ATO financial system. Once the risk assessment process has been completed, appropriate controls are installed and a Certificate of Compliance is issued for the new system.
CEI	Chief Executive Instruction
CPSU	Commonwealth Public Sector Union
DPP	Commonwealth Director of Public Prosecutions

Firecall	To facilitate the smooth operation of ATO IT systems it is necessary at times for ATO IT systems staff to make direct changes to the ATO's mainframe and Wide Area Network environments to correct system errors. To enable staff to perform these 'quick fixes' and to gain the necessary, direct access to production data in the mainframe environment, the ATO has a special access authority known as *Firecall*, which bypasses regular security controls.
Firewall	A firewall is a server that is used as a barrier to control the flow of traffic between networks (this can be either internal or external traffic). A firewall works by applying filtering techniques to block selected transactions (generally based on the entities security policies).
FMA Act	*Financial Management and Accountability Act 1997*
FP&C	Fraud Prevention and Control
GST	Goods and Services Tax
HOTSA	Health of the System Assessment. ATO's formal risk management process, which forms part of its strategic planning framework, and which has been undertaken on an annual basis across all ATO Business Lines since 1994–95.
HRMIS	Human Resources Management Information System
IAB	Internal Assurance Branch
IAC	Integrity Advisory Committee
ICAC	Independent Commission Against Corruption
IFAC	International Federation of Accountants
ISA	International Standard of Auditing
IT	Information Technology
Legacy System	An older system that must be maintained for some time before being gradually rebuilt and replaced.
LAN	Local Area Network. A collection of computers, terminals, printers and other computing devices that are connected through cable over relatively short distances (usually within a single building or office).
MoU	Memorandum of Understanding

MOSC	Management of Serious Crime Program
OCT	Official Conduct Team
Operating System	Extensive and complex set of programs that manages the operation of a computer and the applications that run on it, such as word processing on personal computers or processing of tax returns on mainframes.
PBR	Private Binding Ruling
RACF	Resource Access Control Facility. The ATO facility used to control user access to the ATO mainframe environment.
RTA	New South Wales Roads and Traffic Authority
UNIX	An Information Technology operating system
Unauthorised access	(to information) Access official information which is not based on a legitimate need to know, sanctioned by government policy or agency direction, or an entitlement under legislation.
WAN	Wide Area Network. A collection of computers, terminals, printers and other computing devices that are connected over large distances (ie. metropolitan, intercity, national and international). In the ATO, WAN enables communication between ATO offices. It is also referred by ATO as the TAXLAN. Through it, the ATO accesses various mainframe programs and provides desktop applications to enable ATO officers to perform their duties.
WAA	Workplace Access Administrators. WAAs control the access of users to ATO IT mainframe systems. They have access privileges that allows them to grant user access to particular 'IT groups' and reset passwords.
Windows NT	An Information Technology operating system

Summary and Recommendations

Summary

Background

1. The Commonwealth Government made a coordinated and systematic commitment across the Australian Public Service (APS) to protect its revenue, expenditure and property from fraudulent activity when it released *The Fraud Control Policy of the Commonwealth*[1] in 1987. Fraud is defined in this policy as:

> *…inducing a course of action or deceit involving acts or omissions or the making of false statements orally or in writing with the object of obtaining money or other benefit from, or evading liability to, the Commonwealth.*[2]

2. In 1994, the Government formed the Commonwealth Law Enforcement Board (CLEB)[3] to coordinate and develop public sector fraud control policy, as well as oversee the implementation and maintenance of this policy within Commonwealth agencies. The responsibility for the administration of fraud control, however, rests with each Commonwealth agency.

3. The requirement for a strong fraud control framework and the promotion of a strong ethical culture within the ATO, the Commonwealth's principal revenue collection agency, are essential to effective and efficient ATO operations, including the maintenance of community trust in the Office.

---

1 In the report we refer to *The Fraud Control Policy of the Commonwealth* as the 'Commonwealth Fraud Control Policy'.

2 This definition includes monetary gain and any benefit that could be gained from the Government, including 'rights' of entry to the country, documentation conferring identity, and information.

3 The functions ascribed to CLEB are now being carried out by the Attorney-General's Department.

Audit approach

4. This audit of fraud control arrangements in the ATO forms part of a series of performance audits on the management of fraud control in Commonwealth agencies. Fraud audits were completed in the then Departments of Employment, Education, Training and Youth Affairs in 1999. In 2000, similar audits were completed in the Department of Industry, Science and Resources and Health and Aged Care. Fraud-related audits are also currently under way in the Department of Defence, Department of Family Community Services and Centrelink. At the completion of these audits the ANAO plans to prepare a guide setting out practical examples, derived from its audit activities, to assist agencies to achieve better practice in fraud control.

5. To complement these audits, the ANAO conducted a survey of APS agencies to assess fraud control arrangements that had been implemented by these agencies. The Survey provided an overall view of arrangements across the APS to manage fraud.[4]

6. The objective of this audit was to assess the administration of internal fraud[5] control arrangements in the ATO and to identify areas with potential for improvement as well as identified better practice.

7. To achieve this objective, the ANAO focussed on five key areas. These were: the application of the ATO's corporate governance processes to the internal fraud control activities; the prevention of internal fraud within the ATO; the related use of information technology to minimise fraud risks; the detection of internal fraud within the ATO; and ATO fraud investigation procedures and practices.

8. In undertaking our review of internal fraud, the ANAO specifically excluded review of any current cases of alleged fraudulent activities which have been referred to the Commonwealth Director of Public Prosecutions (DPP) for investigation or which are currently being prosecuted.

---

[4] ANAO Audit Report No. 47 1999–2000 *Survey of Fraud Control Arrangements in APS Agencies.*

[5] For the purpose of this audit, internal fraud refers to fraud investigated by ATO's Fraud Prevention and Control Section. This includes all ATO employee fraud such as unauthorised access to taxpayer data, conflict of interest, a breach of the code of conduct, any fraud committed by ATO contractor staff and any cases of collusion between ATO staff and persons outside the ATO. Internal fraud excludes non-compliance by taxpayers with taxation legislation and fraud committed by non-taxpayers (eg. by, persons who have multiple tax file numbers). With regard to external fraud, the individual Business Lines are responsible for the examination of suspected cases. Each Business Line uses a variety of mechanisms to prevent and detect external/taxpayer fraud. The issue of external fraud will continue to be examined as part of discrete audits relating to the relevant Business Line or processes.

Conclusion

9. The level of alleged fraud reported in the ATO has steadily increased over the last few years (373 cases reported in 1999–2000 compared to 255 in 1994–95). The ATO attributes this increase to a significant improvement in staff awareness of fraud and ethics achieved through its conduct of a comprehensive fraud and ethics awareness program and increased staff confidence that reported matters will be handled appropriately.

10. The ATO has recognised the importance of an ethical and well controlled environment in maintaining community confidence in the taxation system and, particularly, in its revenue collection responsibilities. The ATO has demonstrated a strong commitment to comprehensive fraud control by investing significant resources in establishing and supporting fraud prevention and control capability and creating an ethical workplace culture and environment. The ATO has also implemented public sector better practice in critical areas of fraud control planning, staff education and training, and investigations.

11. The ATO has established a comprehensive fraud control policy framework. Current organisational arrangements provide for fraud prevention and control activities with the necessary independence from mainstream line areas. This development of a comprehensive Fraud Control Plan, by undertaking systematic agency-wide fraud risk assessments, is consistent with better practice.

12. The ANAO has identified areas that can be further improved to ensure that the ATO's internal fraud control framework becomes an integral part of the ATO's corporate governance framework and is consistent with better practice. In particular, there would be benefit in the ATO adopting a more holistic approach to its risk management processes by assessing and managing fraud risks in association with other business risks faced by the ATO. Similarly, any fraud control planning could be directly linked to the ATO's strategic management and business planning processes. There is also scope to further refine the performance assessment framework to enable a quantitative and qualitative assessment of the performance of ATO's internal fraud control function. The ATO advised that it is redeveloping its fraud risk assessment methodology to enable the Fraud Control Plan to become a more strategic management planning tool.

13. The ATO's Information Technology (IT) systems are an integral part of its fraud control framework. The risk to the IT systems themselves must also be adequately managed with sound planning, assessment,

treatment and monitoring given their significance to the ATO. The security of the ATO's IT systems should be an ongoing concern to the management. Since 1994–95, the ANAO has highlighted significant risks associated with ensuring the ongoing security of the ATO's IT systems. These risks relate primarily to the storage of taxpayer data on ATO's Wide Area Network[6], contrary to its IT security policy and procedures, and the granting and monitoring of access to the ATO IT systems. The ATO advised that it is in the process of introducing systems' changes and revising its policies in relation to the appropriate storage of taxpayer data and access to its IT systems.

14. The ATO's fraud prevention and control capability has been enhanced over the past five years through a program of continuous improvement in areas such as the development of: a fraud and ethics awareness program; a compliance certification process relating to the adequacy of controls in financial systems; the introduction of the investigations case management system; the issuing of a Statement of Investigations Standards; and staff training programs. We also note that external agencies, such as the Australian Federal Police, have commended the ATO on its fraud prevention and investigation practices.

15. The ANAO considers that ATO's fraud minimisation framework could be enhanced further by making greater use of internal publications and other awareness raising techniques to reinforce the role of the Fraud Prevention and Control (FP&C) Section and extending the compliance certification process to all ATO administrative systems. The assessment and treatment of risks associated with legacy systems[7] also warrants attention. The ANAO has also recommended that the ATO examine the cost/benefits of enhancing the security of its Fraud Prevention Case Management System by encrypting fraud investigation data, to ensure information held on the system is secure and cannot be altered, deleted or corrupted by the FP&C Section staff without an audit trail. Strengthening the administrative controls of its investigations function will provide further assurance that information contained in the Fraud Prevention Case Management System is accurate and timely. ATO's fraud detection capability can be further enhanced through increased pro-active detection activities.

---

[6] A Wide Area Network (WAN) is a collection of computers, terminals, printers and other computing devices that are connected over large distances (ie. metropolitan, intercity, national and international). In the ATO, WAN enables communication between ATO offices. It is also referred by ATO as the TAXLAN. Through it the ATO accesses various mainframe programs and provides desktop applications to enable ATO officers to perform their duties.

[7] A legacy system is an older system that must be maintained for some time before being gradually rebuilt and replaced.

Key Findings

Fraud control corporate governance mechanisms

ATO fraud control policy

16. The Commonwealth Fraud Control Policy forms the basis for ATO's fraud control policy. The ATO's fraud control policy expands, and further defines, aspects of the Commonwealth Fraud Control policy in relation to its application within the ATO. The ATO has demonstrated its commitment to a comprehensive fraud control environment through a number of initiatives such as:

- establishing an independent committee structure to provide advice on the strategic direction of ATO fraud control policy and operations and to give further confidence that the ATO is maintaining the highest professional standards; and
- producing a number of publications to cover aspects of the ATO's fraud policy.

Organisational arrangements

17. Coordination of internal fraud prevention and control rests with a semi-autonomous section of the ATO's Internal Assurance Branch known as the Fraud Prevention and Control (FP&C) Section. The Section reports directly to the ATO Executive, and has delegated[8] powers of access and inquiry. Although the Section has overall responsibility for investigating internal fraud matters, the ATO Business and Service Lines are equally responsible for ensuring an effective fraud control environment within the ATO.

Fraud risk assessment and planning

18. The ATO undertakes an agency-wide fraud risk assessment every two years in accordance with the Commonwealth Fraud Control Policy. The most recent fraud risk assessment was conducted in 1999 for the 1999–2001 Fraud Control Plan. The ANAO found that the methodology adopted by the ATO during the latest round of fraud risk assessment was sound and complied with the Attorney-General's Department requirements.

---

[8] The FP&C Section's authority is stated in Section 20 of the *Public Service Act 1999*, and delegated by the Commissioner for the specific purpose of receiving reports and investigating serious breaches of the code of conduct.

19. The fraud risk assessment was undertaken as a discrete process independent of the ATO's Health of the System Assessment (HOTSA) process. The HOTSA is the ATO's formal risk management process, which forms part of its strategic planning framework and has been undertaken on an annual basis across all ATO Business Lines since 1994–95. It requires each of the Business and Service Lines to address their major areas of risk and establish plans to manage those risks.

20. As part of its future approach to fraud risk management, the ANAO considers the ATO could incorporate relevant elements of its fraud risk assessment process as an explicit element of the broader ATO risk management process (that is, the HOTSA). Through adopting this more holistic approach to risk management, fraud risks could be assessed and managed in association with other business risks faced by the ATO.

21. The ANAO noted that the 1999–2001 Fraud Control Plan, developed as part of the fraud risk assessment process, also met the requirements of the Commonwealth Fraud Control Policy as assessed by the Attorney-General's Department in January 2000. The ATO had structured the monitoring and implementation process for the 1999–2001 Fraud Control Plan to overcome deficiencies in the monitoring and implementation of the previous Fraud Control Plan.

22. The ANAO acknowledges and supports these initiatives. However, the ANAO found that because of its classification status as a protected document, ATO had limited circulation of the Fraud Control Plan and appropriate access was not always provided to officers responsible for implementing action items.

23. As in the case of the fraud risk assessment process, the ANAO identified a need to link fraud control planning to ATO's strategic and business planning processes. This would increase staff awareness of fraud control issues and ensure that the Fraud Control Plan was not developed in isolation.

24. The ATO advised that with the classification of the Fraud Control Plan as a protected document in mind, the FP&C Section, in consultation with service providers has been: redeveloping the fraud risk assessment methodology to enable the Fraud Control Plan to become a more strategic planning tool; and examining ways to use e-publishing of relevant parts of the Plan to improve access to it.

Performance assessment framework

25. The ANAO found that the ATO's 1999–2000 performance assessment framework for the FP&C Section did not provide sufficient information to evaluate its performance in relation to minimisation of fraud within the ATO. As a result of the ANAO's findings, the FP&C

Section developed its 2000–2001 Business Plan based on the Commonwealth outcomes/output framework. This Business Plan demonstrates the Section's efforts to improve the measurement of its performance. However, there is scope to further refine the Business Plan in areas such as identification of outputs, targets and performance indicators (qualitative and quantitative).

26. The ATO's governance reporting process has been operating for a number of years as part of its corporate governance framework. Each Business and Service Line contributes to the corporate governance reporting process. The ANAO noted that, as part of the 1999–2000 Business Line performance and governance reporting requirements, the ATO has included an additional requirement for Business and Service Lines to report on performance against their section of the Fraud Control Plan.

Fraud prevention

27. The ANAO noted that the ATO has invested significant resources in the prevention of fraud and the creation of an ethical work environment. The Commissioner of Taxation has recognised the importance of ATO's ethical environment in maintaining community confidence in the taxation system, and its revenue collection responsibilities.

Fraud prevention strategies

28. The FP&C Section has devoted significant resources to ATO's fraud and ethics awareness training program. The program is designed to educate ATO staff about a variety of ethical and fraud-related issues applicable to the ATO. Since February 1998, 19 890 ATO staff had attended these training sessions (as at June 2000). This accounts for a high proportion of all staff currently employed by the ATO.[9]

29. The ATO has also established a framework to assess the effectiveness of its fraud and ethics awareness training program. The framework is based on regular assessment by an external consultant of ATO staff's fraud control knowledge. This is supplemented by ongoing feedback from staff on the training sessions and scrutiny by external stakeholders such as the Commonwealth Ombudsman. The ANAO noted that the external consultant's assessment found that knowledge of ATO staff's fraud control measures had increased (from 40 per cent in 1998 prior to the fraud and ethics awareness training program to 72 per cent following the program in late 1999).

---

[9] ATO was unable to provide the ANAO with the exact proportion of staff that had undergone training since February 1998 as these statistics are subject to staff departures and arrivals since 1998.

Facilitation by ATO Business Lines

30. ATO Business Lines are responsible for ensuring that ATO financial, administrative and management systems and processes are adequately protected from fraudulent activity.

31. The ATO's Financial Services Section utilises a 'Certificate of Compliance' process to provide assurance that new financial systems have controls in place to prevent and detect fraudulent activity. The ANAO considers that the compliance certification process provides a high level of assurance that system controls have been assessed to prevent fraudulent activity.

32. The ANAO noted that some systems have not undergone this process and will continue to remain in operation as 'legacy systems' for some time. The ANAO considers that controls for 'legacy systems' should also be assessed and treated for fraud-related risks as the potential for fraud increases with less scrutiny of outdated systems.

33. The ANAO also noted that the compliance certification process was limited to financial systems. As fraudulent activity can occur in both financial and non-financial systems, the ANAO considers that the ATO should also examine the certification of non-financial systems to consider the adequacy of controls to prevent and detect fraudulent activity.

Information technology systems

34. The ATO is reliant on the efficient and effective operation of its IT systems. The ANAO has noted in previous audits since 1994–95[10] that there are significant risks associated with ensuring the security of the ATO IT systems. These risks related primarily to the storage of taxpayer data on the ATO Wide Area Network and the granting and monitoring of staff access to the ATO IT systems. During this audit, the ANAO found that not only do these risks remain, but the risk factors have increased due to the outsourcing of many IT system functions. This is due to ATO contractor staff having limited exposure to ATO fraud prevention, education and awareness material and programs in comparison to ATO employees. In addition, the ATO could not provide evidence that the IT Security Section had monitored outsourced contractors' activity to ensure compliance with taxpayer data security provisions of its IT outsourcing contracts. Further, the ANAO found that FP&C Section fraud statistics show that since 1994–95, unauthorised access to taxpayer data by ATO staff has been the most common type of

---

[10] ANAO Audit Report No.6 1994-95 *Australian Taxation Office Information Technology Security*.

fraud reported for internal investigation. The ATO advised that its IT Security Section has purchased a suite of audit logging, gathering/analysis software products[11] that will improve access security by enabling the pro-active monitoring of audit logs for the WAN environment.

35. The ANAO also noted the ATO staff's practice of downloading taxpayer data on to the ATO Wide Area Network contravenes the ATO's existing security policy (which was developed in 1992). This practice increases the risk of exposing taxpayer data to unauthorised access. The ATO has advised that it intends to address this issue by reviewing the ATO's security policy regarding the appropriate storage of bulk taxpayer data outside the mainframe environment.

36. To facilitate the smooth operation of ATO IT systems it is necessary at times for ATO IT systems staff to make direct changes to ATO's mainframe environment to correct system errors. To enable staff to perform these quick fixes and to gain the necessary direct access to production data in the mainframe environment, the ATO has a special access authority known as *Firecall* to bypass security controls.

37. ATO staff requiring *Firecall* access need to obtain management and/or user approval, as it bypasses all normal system change procedures and access controls. For this reason, the ANAO considers that its use should be kept to a minimum and each use of the *Firecall* facility should be carefully reviewed.

38. The ANAO first raised concerns about the use of *Firecall* in 1994–95 and noted that many ATO staff were not only using *Firecall* for emergency situations, but also to perform their normal daily work. Since then the ANAO has noted that *Firecall* continues to be used so frequently that effective, independent review by the ATO IT Security Section is administratively unachievable. Given the concerns expressed previously by the ANAO and the findings of this report, we consider the ATO should establish more effective policy and controls for *Firecall*.

39. The ATO has advised that it is in the process of introducing systems' changes and revising its policies to restrict the use of *Firecall*. The ANAO also notes that the ATO has recently developed a draft *Firecall Usage Policy*. It is too early to say whether these developments address all of ANAO's concerns. The ATO should closely monitor these changes to ensure they remove or effectively manage the risks identified by the ANAO.

---

[11] The ATO uses these products for its Firewalls. It plans to extend the use of these products to TAXLAN (WAN) in the near future.

Pro-active information technology controls

40. Logging details of access made by ATO staff to IT systems is an important mechanism to ensure the security of ATO taxpayer and other data. Comprehensive logging of IT systems provides an audit trail to identify perpetrators of IT fraud as well as contributing to maintaining community confidence in the ATO and its staff. It also provides staff with the confidence that the ATO is in a position to defend them should they become a victim of an unjustified allegation of unauthorised accessing.[12] The ANAO noted that the ATO does not utilise a systematic approach to targeted analysis of access logs on a regular basis. Analysis is, however, undertaken by the IT security area when there is a specific purpose, such as an ATO internal audit or fraud investigation. The FP&C Section undertook two separate projects (in 1995 and 1996) to identify unauthorised access to celebrity taxpayer records. Based on the fraud statistics relating to unauthorised information access, it is likely these projects made a contribution to the reduction in the number of unauthorised information access cases reported to FP&C Section in the year immediately following the review. Since 1996 the FP&C Section has not undertaken similar projects.

41. For 1999–2000 there has been a significant increase in the number of unauthorised access to information cases reported for investigation. The ATO attributes the increase in reported cases to its fraud and ethics awareness program and raising the profile of the FP&C Section, and not to the lack of conducting projects to identify unauthorised access. However, the ANAO notes that soon after these projects were undertaken, the FP&C Section acknowledged in its briefings to the ATO Executive the value in a joint approach (by combining awareness raising with visible enforcement through unauthorised access investigations projects) to achieve a shift in the corporate culture.

42. The ANAO considers that ATO should examine the potential benefits of further targeted analysis of ATO IT system logs in the future as it is likely to prove an efficient mechanism to detect the numbers of staff who unlawfully access taxpayer information and, if well publicised, can also be an effective fraud prevention mechanism.

---

[12] ATO has advised that the audit trail system exonerates approximately 70 per cent or more of allegations reported to FP&C Section related to unauthorised access.

Fraud detection

43. Fraud detection is a key element of an agency's overall fraud control strategy. It provides staff and external stakeholders with tangible assurance that an agency's assets are protected, and perpetrators of fraudulent activity are detected and prosecuted.

Pro-active fraud detection activities

44. Use of sophisticated computer software to analyse and collect large amounts of data in an IT environment offers a new and efficient tool to detect fraudulent IT activity. Through the use of computer-assisted audit techniques and sophisticated data-mining software, fraud investigators are able to analyse, compare and compile data over numerous large databases and build profiles of fraudulent activity within an organisation.

45. The ATO has an Analytical Support Section, within the Internal Assurance Branch, which provides this support facility. The FP&C Section has made limited use of this facility. The ANAO considers that there is potential for further use of the Section's services in detecting internal fraud.

46. The ATO advised that it considers it must determine an optimal balance between conducting pro-active investigations, and responding to fraud allegations made by staff and fraud prevention training. The ATO also noted that major fraud investigations, that may require a number of investigators, draw resources away from pro-active investigations. The ANAO considers that there is benefit in conducting pro-active fraud detection even if ATO resources do not allow the investigation of all identified cases. As part of FP&C Section's risk-based approach, all cases identified in such projects would be considered for further investigation, after taking account of Section's other work priorities.

Fraud investigation

47. Fraud investigations are a significant aspect of FP&C Section's activities. The ATO has developed a Statement of Investigation Standards which covers key aspects of the investigations process. These standards are appropriately linked to several other ATO and Commonwealth policy documents and procedures and are also available on a CD-ROM. The ANAO considers this as better practice because it eliminates the need to transfer bulky documents and provides ready access to all reference material when travelling away from the office.

48. The FP&C Section has developed a Case Management System to facilitate administrative management of fraud investigations. The ANAO noted as a result of a 1998 review of the fraud prevention and control function, the Section implemented new security environment to address issues relating to logging access and restricting user access. However, the ANAO found that security of this system could be overridden. This means information contained on the Case Management System could be altered, deleted or corrupted by any staff from the FP&C Section without an audit trail. The ATO should examine the cost/benefits of enhancing the security of its Case Management System by encrypting investigation data to ensure the security of the information contained on this system.

49. Overall, we found investigations were being undertaken in accordance with documented procedures. However, there was scope to strengthen the administrative controls relating to its investigations functions. This related largely to the management of information held in the Case Management System to ensure it was accurate and timely.

Recommendations

Set out below are the ANAO's recommendations with Report paragraph references. The ANAO considers that the ATO should give priority to recommendations 1,2,3,6,7 and 8.

Recommendation No.1 Para. 2.45

The ANAO recommends that, to enable the Fraud Control Plan to be effectively implemented, the ATO develop a strategy to ensure that staff required to implement Fraud Control Plan action items are given appropriate access to the Plan, or extracts from it, and a clear indication of implementation timetables.

ATO Response: Agree

Recommendation No.2 Para. 2.51

The ANAO recommends that the ATO adopt a more holistic approach to risk management and planning processes by:

- incorporating relevant aspects of its fraud risk assessment process as an explicit element of the broader ATO risk management processes to enable fraud risks to be assessed and managed in association with other business risks faced by the ATO; and
- linking fraud control planning to its strategic management and business planning processes as part of its corporate governance framework.

ATO Response: Agree

Recommendation No.3 Para. 2.65

The ANAO recommends that the ATO further refine the performance assessment framework to enable quantitative and qualitative assessment of its internal fraud control function.

ATO Response: Agree

Recommendation No.4 Para. 3.32

The ANAO recommends that, as an important element of the fraud education process, the ATO make greater use of its internal publication, *ATO Extra*, and other awareness raising techniques in publicising case studies and results of investigations conducted by its Fraud Prevention and Control Section.

ATO Response: Agree

Recommendation No.5 Para. 3.42

The ANAO recommends that, to further protect its financial, administrative and management systems and processes from fraudulent activity, the ATO:

- conduct certificate of compliance checks on 'legacy systems' to provide assurance that adequate controls are in place to prevent and detect fraudulent activity; and
- extend its 'Certificate of Compliance' process to non-financial systems.

ATO Response: Agree

Recommendation No.6 Para. 4.21

The ANAO recommends that the ATO:

- develop standards and guidelines for inclusion in the ATO Security Policy which address the risks of storing bulk taxpayer data outside the mainframe control environment; and
- introduce a program of internal checking to ensure adherence to these standards.

ATO Response: Agree

Recommendation No.7 Para. 4.53

The ANAO recommends that, to achieve the required level of security and to promote consistency in access approval processes, the ATO:

- investigate the cost effectiveness of automating the access approval process by linking mainframe access privileges to the ATO's Human Resources Management System;
- implement consistent accountability controls for all Workplace Access Administrators and the Access Management Team so that special access privileges are used correctly; and
- ensure the legitimate use of *Firecall*, by monitoring and analysing all accesses using *Firecall*, and finalise its detailed security policy outlining the guidelines for controlling *Firecall* access.

ATO Response: Agree

Recommendation No.8 Para. 4.64

The ANAO recommends that to minimise exposure to fraudulent activity, the ATO IT Security Section and, where necessary the Fraud Prevention and Control Section, undertake regular targeted reviews of ATO IT system logs to detect and deter unauthorised access to taxpayer data.

ATO Response: Agree

Recommendation No.9 Para. 5.19

The ANAO recommends that, to improve the efficiency and effectiveness of its internal fraud detection strategy, the:

- Fraud Prevention and Control Section make further use of the Analytical Support Section to identify potential fraud-related cases and assess the further investigation of these cases against other work priorities; and
- ATO strengthen the coordination between the Internal Audit Section and the Fraud Prevention Control Section to improve the development of risk mitigation strategies.

ATO Response: Agree

Recommendation No.10 Para. 6.21

The ANAO recommends that the ATO examine the cost/benefits of enhancing the security of its Fraud Prevention Case Management System with encryption to ensure information held on the system is secure and cannot be altered, deleted or corrupted by the Fraud Prevention and Control Section staff without an audit trail.

ATO Response: Agree

Recommendation No.11 Para. 6.39

The ANAO recommends that the ATO strengthen the administrative controls associated with the Fraud Prevention Case Management System to ensure that the information contained in the system is accurate and timely.

ATO Response: Agree

Audit Findings and Conclusions

1. Introduction

This chapter provides an overview of fraud prevention and control within the Commonwealth public sector, the ATO's fraud control environment and the framework and methodology ANAO used to assess ATO's internal fraud control arrangements.

Fraud prevention and control within the Commonwealth public sector

1.1 The prevention and detection of fraud within the Commonwealth public sector is not only important to protect Commonwealth revenue, expenditure and property, but also to maintain the Parliament's and community's confidence in the staff and operations of public sector agencies.

1.2 The Commonwealth Government first made a coordinated and systematic commitment to the prevention of fraud across the Australian Public Service (APS) in 1987 when the government released *The Fraud Control Policy of the Commonwealth*.[13] Fraud is defined in this policy as:

> *…inducing a course of action or deceit involving acts or omissions or the making of false statements orally or in writing with the object of obtaining money or other benefit from, or evading liability to, the Commonwealth.*[14]

1.3 In 1994, the Government formed the Commonwealth Law Enforcement Board (CLEB)[15] to ensure that all Commonwealth agencies with law enforcement responsibilities were able to adapt to the changing criminal environment and work together to pursue the Government's law enforcement interests. As part of its mission, CLEB had responsibility for the coordination and development of public sector fraud control policy, as well as overseeing the implementation and maintenance of this policy within Commonwealth agencies.

---

[13] Throughout the report we refer to *The Fraud Control Policy of the Commonwealth* as the 'Commonwealth Fraud Control Policy'.

[14] This definition includes monetary gain and any benefit that could be gained from the Government, including 'rights' of entry to the country, documentation conferring identity, and information.

[15] The functions ascribed to CLEB are now being carried out by the Attorney-General's Department and the Australian Federal Police.

1.4 The Commonwealth Fraud Control Policy was developed further in 1994. The objectives of the Commonwealth Fraud Control Policy are to:

- protect public money and property;
- protect the integrity, security and reputation of public institutions; and
- to maintain high levels of service to the community consistent with the good Government of the Commonwealth.

1.5 The Attorney-General's Department is continuing the development of these objectives in three main areas. These are:

- the reduction of losses through fraud by the rigorous implementation of fraud prevention procedures;
- a commitment to a policy of detection, investigation and prosecution of individual cases of fraud; and
- respect for the civil rights of all citizens.

1.6 A recent review by the Attorney-General's Department of the Commonwealth Fraud Control Policy led to the release of a *Consultation Draft* in 1999.[16] The new *Consultation Draft* is a more principles-based policy that is designed to:

- encourage agencies to manage fraud risks alongside other risks they face;
- assist agencies to better deal with both the existing and new risks of fraud facing the public sector; and
- provide agencies with greater flexibility to choose and develop the fraud control arrangements best suited to them.

Accountability of Chief Executive Officers

1.7 Although the Attorney-General's Department oversees the development of Commonwealth Fraud Control Policy, the Government has outlined in this policy that responsibility for its implementation and the administration of fraud control rests with each Commonwealth agency and, more particularly, the Chief Executives of those agencies.

1.8 In addition to the prescriptive requirements of the Commonwealth Fraud Control Policy, Commonwealth Chief Executive Officers also have a legislative requirement under the *Financial Management and Accountability Act 1997* (the FMA Act) to:

- manage the affairs of the agency in a way that promotes proper use[17]

---

[16] The Fraud Control Policy of the Commonwealth, Consultation Draft No.1 (21 June 1999).

[17] Section 44(3) defines 'proper use' as efficient, effective and ethical use.

of Commonwealth resources for which the Chief Executive is responsible;[18] and

- implement a Fraud Control Plan for their agency.[19]

1.9 An agency's Fraud Control Plan should contain procedures for implementing the Government's requirements in relation to: fraud prevention; detection; investigation; prosecution; and recovery and civil rights privacy processes.[20]

1.10 The Commonwealth Fraud Control Policy outlines that individual Chief Executive Officers are to be fully accountable to their respective Ministers for the implementation of fraud control policy in their agency. The principal mechanism for Chief Executives to provide this accountability is the preparation of a fraud control report[21] for the relevant Minister, as outlined under the FMA Act (*Financial Management Accountability Orders*).

1.11 Agencies are also required to provide the Attorney-General's Department with a report outlining fraud that has occurred within the agency. A summary report combining fraud statistics from all Commonwealth agencies is then provided to the Minister for Justice and Customs.

1.12 The desired outcome of the Commonwealth Fraud Control Policy and legislation is the elimination of cases of fraud on Commonwealth programs involving public sector employees and elimination, by all possible efforts, of fraud against Commonwealth programs generally.

1.13 This audit of fraud control arrangements in the ATO forms part of a series of performance audits on the management of fraud control in Commonwealth agencies. Fraud audits were completed in the then Department of Employment, Education, Training and Youth Affairs in 1999. In 2000 similar audits were completed in the Department of Industry, Science and Resources and Health and Aged Care. Fraud-related audits are also currently under way in the Department of Defence, Department of Family Community Services and Centrelink. At the completion of these audits the ANAO plans to prepare a guide setting out practical examples to assist agencies to achieve better practice in fraud control.

---

[18] Section 44 (1) of the *Financial Management and Accountability Act 1997*. Those Commonwealth agencies not bound by the FMA Act have similar responsibilities under the *Commonwealth Authorities and Companies Act 1997* (CAC Act).

[19] The mandatory use of a Fraud Control Plan by an agency CEO is outlined under section 45 of the FMA Act.

[20] These requirements are specified in the Commonwealth Fraud Control Policy.

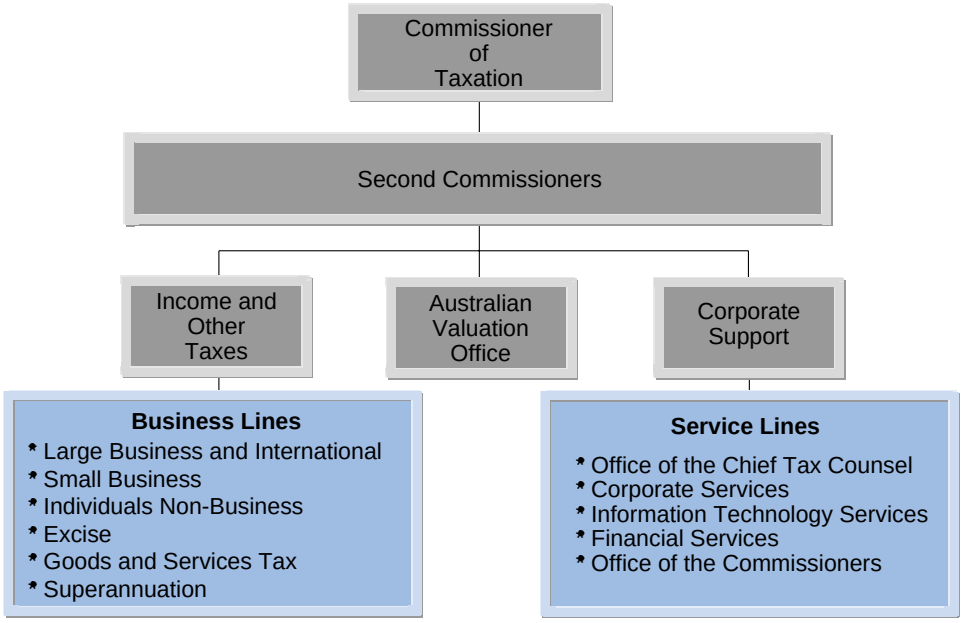
[21] The report must contain the following documentation: an assessment of fraud risks relevant to that agency; if a Fraud Control Plan has been previously prepared, an assessment of that previous Fraud Control Plan; and a current Fraud Control Plan. (Financial Management and Accountability Orders—Consolidated as in force on October 1999).

1.14 To complement these audits, the ANAO conducted a survey of APS agencies to assess fraud control arrangements that had been implemented by these agencies. The Survey provided an overall view of arrangements across the APS to manage fraud.

Australian Taxation Office

1.15 The Australian Taxation Office (ATO) is the Commonwealth's principal revenue collection agency. In 1999–2000, the ATO's taxation revenue totalled $151 billion. The ATO is structured into Business and Service lines as shown in Figure 1.

Figure 1
Structure of the Australian Taxation Office



1.16 Due to the amount of revenue collected and the number of staff it employs (19 131 as at 30 June 2000), the requirement for a strong fraud control framework, and the promotion of a strong ethical culture within the ATO, is essential to effective and efficient operations within the ATO and to maintaining community trust.

1.17 The Commissioner of Taxation recognises and has emphasised the need for a strong fraud control environment in the ATO. In 1998 he stated that:

> *It is unremarkable – and totally predictable – that in an organisation of nearly 17,000 staff there will be some who act illegally… What is important is that the ATO has effective measures in place to both minimise the potential for such fraud and misconduct, and to identify and hold to account those who engage in it.* [22]

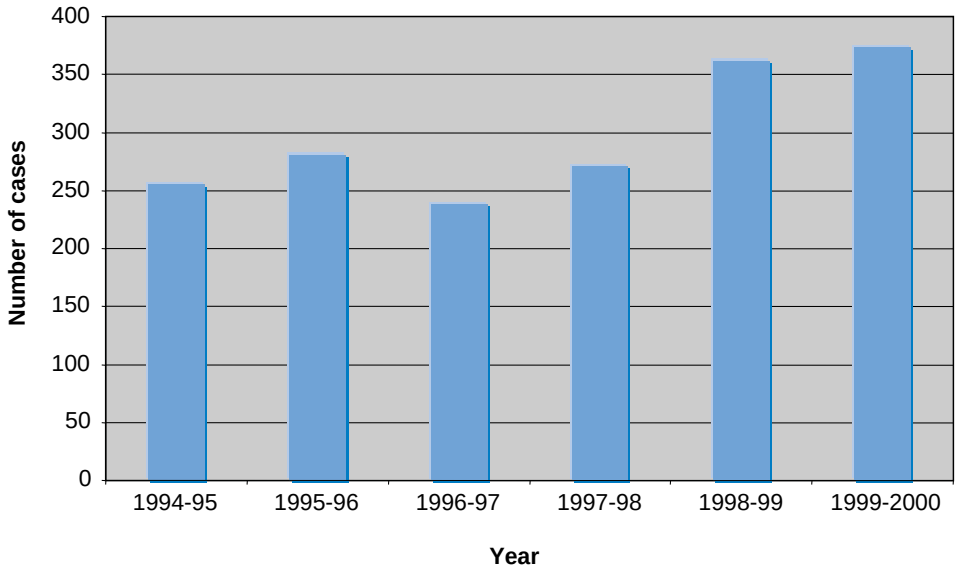
ATO's operational framework for fraud prevention and control

1.18 Coordination of internal fraud[23] prevention and control rests with a semi-autonomous section of the ATO's Internal Assurance Branch (IAB)[24] known as the Fraud Prevention and Control (FP&C) Section. The objective of the Section is to maintain community confidence in the ATO through the minimisation of fraud and misconduct.

1.19 Figure 2 illustrates the number of allegations received by the ATO's FP&C Section since 1994–95.

Figure 2

Number of allegations received by the Fraud Prevention and Control Section since 1994–95



Source: ATO data

---

[22] ATO Media Release—Nat 98/55, *Fraud Prevention and Control in the Tax Office*, 16 September 1998.

[23] The ANAO defines internal fraud in paragraph 1.27.

[24] The ATO Internal Assurance Branch is part of the Corporate Support Service Line.

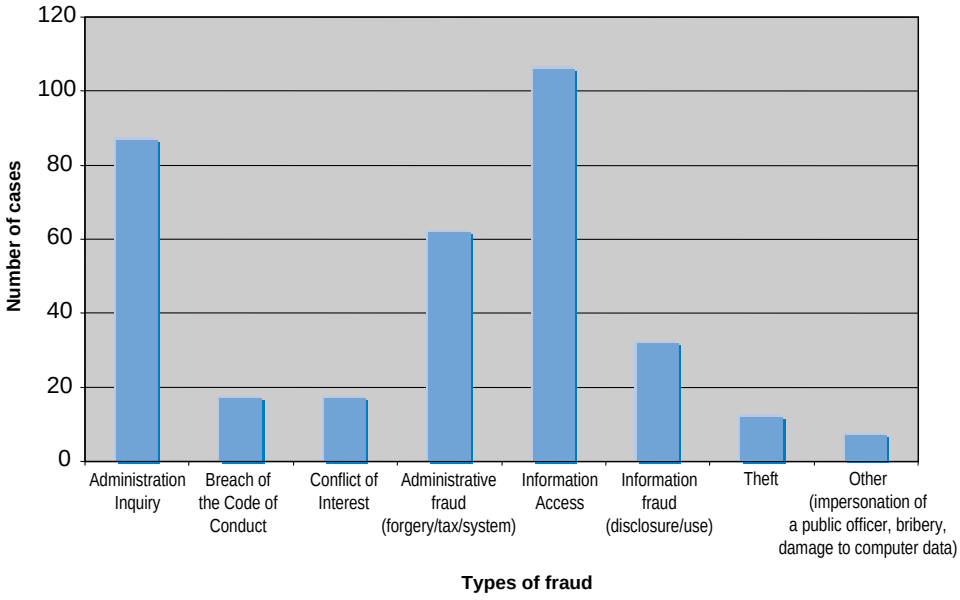
1.20 The figure shows that the level of alleged fraud reported in the ATO has steadily increased over the last few years (373 cases reported in 1999–2000 compared to 255 cases reported in 1994–95). The ATO attributes this steady increase to: significant improvement in staff awareness of fraud and ethics achieved through its comprehensive fraud and ethics awareness program; increased staff confidence that a reported matter will receive attention; and increased confidence that the interests and well being of staff who report wrongdoing by other staff will be protected.

1.21 The dollar value of reported internal fraud within the ATO is not readily available. Prior to 1998–99, the FP&C Section estimated the value of assets lost to internal fraud and the dollar amount recovered. However, the ATO has advised that it now considers that these figures were indicative, cannot be substantiated and are of minimal relevance. For the ATO, maintaining community confidence and minimising fraud were the driving factors rather than the amount of the fraud.

1.22 Figure 3 illustrates the types of fraud cases received by the FP&C Section in 1999–2000. Unauthorised access to taxpayer data by ATO staff remains the most common type of fraud perpetrated in the ATO.

Figure 3

Cases received by the Fraud Prevention and Control Section for 1999–2000 by fraud type



Source: ATO data

1.23 Aside from the FP&C Section, there are number of other areas that provide assistance in implementing fraud control policy within the ATO. These include:

- Protective Security Section: responsible for managing matters of physical security within the ATO;
- Official Conduct Team (OCT): responsible for providing expert advice on enforceable standards of conduct, options for dealing with apparent misconduct, and the proper application of policy corporate values and precedents;
- ATO Business and Service Lines: responsible for applicable ATO system controls;
- ATO Concern: responsible for helping ATO staff with issues and concerns they may have with the administration of the ATO;
- Employee Protection and Reporting Policy and Program: responsible for assuring employees that their wellbeing and interests will be protected against victimisation and discrimination when they report fraud or misconduct. It includes the Employee Assistance Program, a confidential counselling service set up to assist ATO employees and their families with personal problems;
- Information Technology Security Section: responsible for maintaining the information technology control environment; and
- Financial Services Section: responsible for assuring the effectiveness of controls over ATO financial systems.

ATO internal fraud control policy

1.24 In response to the requirement to have effective measures in place to minimise the potential for fraud and misconduct, the ATO has devised a fraud control policy. The ATO fraud control policy expands, and further defines, aspects of the Commonwealth's Fraud Control Policy in relation to its application within the ATO. Figure 4 illustrates the elements that comprise the ATO fraud control policy.

Figure 4
Elements comprising ATO fraud control policy

Audit objective and methodology

1.25 The objective of the audit was to assess the administration of internal fraud[25] control arrangements in the ATO and to identify areas with potential for improvement as well as identified better practice.

1.26 To achieve this objective the ANAO examined five key areas. These were:

- the application of the ATO's corporate governance process to the internal fraud control activities;
- the prevention of internal fraud within the ATO;
- the related use of information technology to minimise fraud risks;
- the detection of internal fraud within the ATO; and
- ATO fraud investigation procedures and practices.

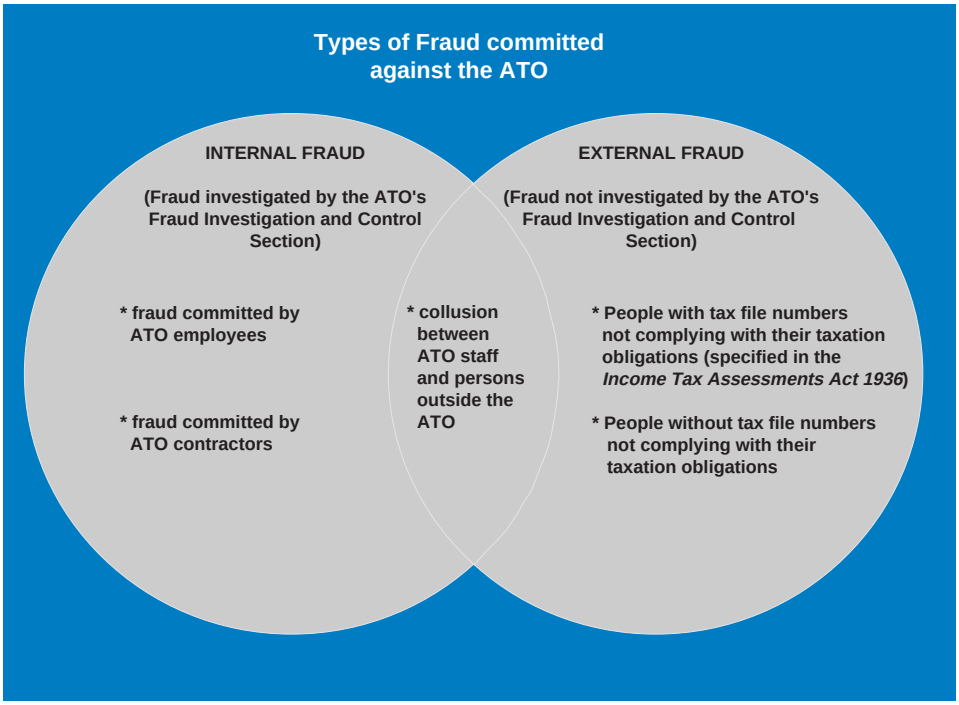
[25] The ANAO defines internal fraud in paragraph 1.27.

Audit scope

1.27 The audit focused on the ATO's internal fraud prevention and control arrangements. In particular, the audit centred on the activities of the FP&C Section, corporate governance processes (including risk management) and ATO Business Line involvement in preventing and detecting internal fraud. We also considered cases of suspected collusion between ATO staff and external parties where FP&C Section investigated those cases. Figure 5 illustrates the ATO's distinction between internal and external fraud and also the scope of the audit.

Figure 5

Categories of fraud committed against the ATO



1.28 The individual Business Lines are responsible for the examination of suspected cases of external fraud. Each Business Line uses a variety of mechanisms to prevent and detect external/taxpayer fraud. External fraud will continue to be examined as part of discrete audits relevant to each Business Line or processes.

1.29 In undertaking our review of internal fraud the ANAO specifically excluded review of any current cases of alleged fraudulent activities which have been referred to the Commonwealth Director of Public Prosecutions (DPP) for investigation or which are currently being prosecuted.

Audit methodology

1.30 Audit fieldwork was conducted between April and June 2000. In addition to document and file review, interviews with key ATO staff were undertaken at ATO National Office in Canberra and six Regional Offices.[26] The principal purpose of these visits was to determine whether there was consistency in ATO fraud control practices throughout ATO Regional Offices. Key staff, integral to the effective implementation of fraud prevention and control policy, were also located in these regions. Fieldwork included an analysis of case data stored on the FP&C Section's Case Management System as well as associated physical files.

1.31 The ANAO consulted a selected range of agencies with expertise in fraud prevention and control including the Attorney-General's Department, the Australian Federal Police, the Australian Bureau of Criminal Intelligence (ABCI), the DPP, the New South Wales (NSW) Audit Office, NSW Roads and Traffic Authority (RTA) and the NSW Independent Commission Against Corruption (ICAC). These agencies provided the ANAO with information on current fraud control methodology and research.

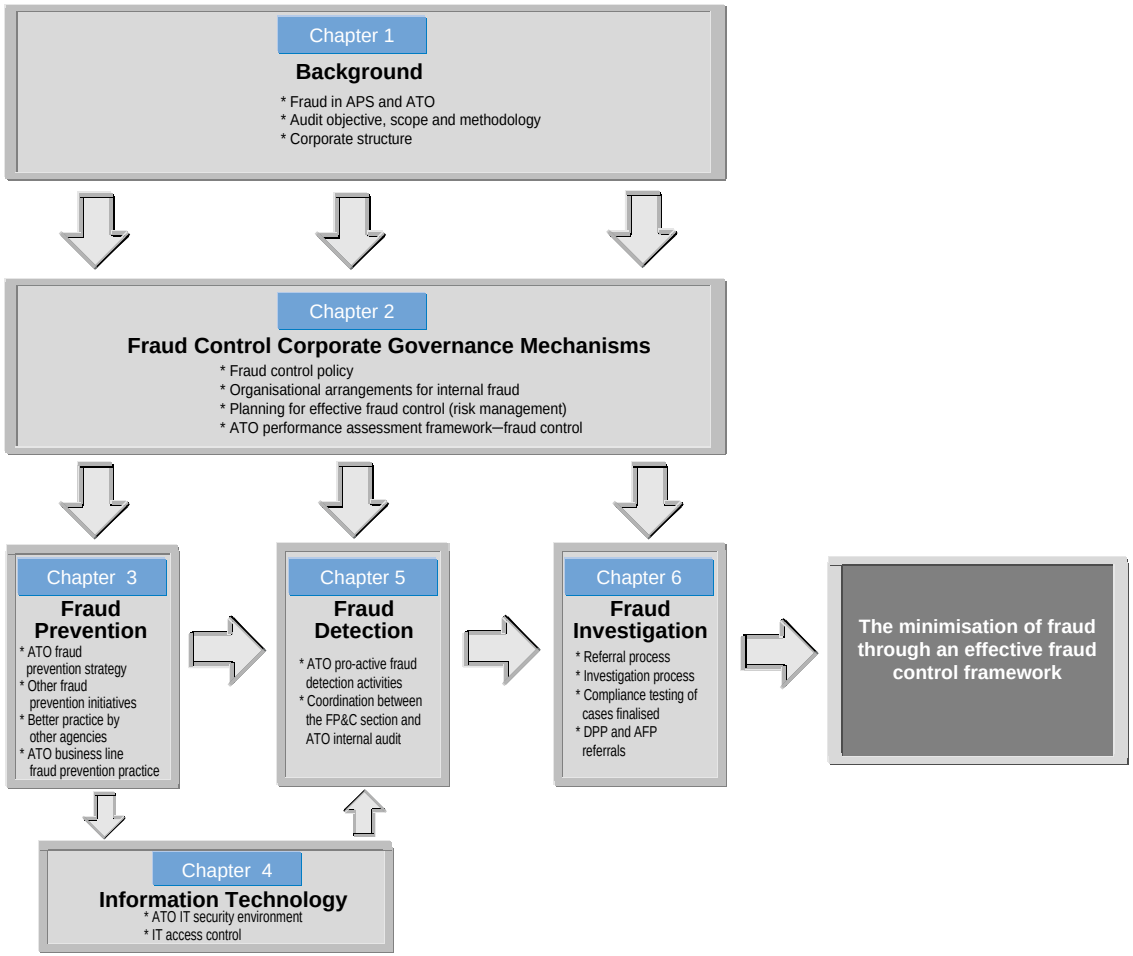
1.32 The audit had regard to recent ANAO and external reviews on fraud control. Further information on these reviews is provided at Appendix 1. The audit was conducted in conformance with ANAO auditing standards at a cost of $245 000.

Report structure

1.33 Figure 6 illustrates the framework the ANAO used to analyse ATO fraud control arrangements. This framework formed the basis for the structure of the report.

[26] ATO Regional Offices visited were: Sydney CBD, Parramatta, Penrith, Box Hill, Casselden Place, Moonee Ponds and Hobart.

Figure 6
ANAO report structure



2. Fraud Control Corporate Governance Mechanisms

This chapter reviews the ATO's fraud control framework as a key element of an effective corporate governance strategy. In assessing the corporate governance of internal fraud control, the ANAO examined the ATO's fraud control policy, fraud risk assessment and planning processes, and relevant aspects of the ATO's performance assessment framework.

Introduction

2.1 An effective fraud control strategy is a key element of a sound corporate governance framework. To assess the fraud control mechanisms used by the ATO as part of its corporate governance process, the ANAO reviewed:

- the ATO's fraud control policy;
- organisational arrangements;
- the ATO's Fraud Control Plan, and associated development, implementation and monitoring processes; and
- the ATO's performance assessment framework and accountability arrangements.

ATO fraud control policy

2.2 As noted in Chapter 1, the Commonwealth Fraud Control Policy forms the basis for ATO's fraud control policy. The ATO developed its fraud control framework based on Attorney-General Department Guidelines.[27] These Guidelines are based on the Commonwealth Fraud Control Policy and state that:

> *…Chief Executives are responsible for fostering an environment within their agencies which makes active fraud control a major responsibility for all public sector staff, for articulating clear standards and procedures to encourage minimisation and deterrence of fraud, and for the detection and prosecution of offences should they occur.*

[27] Better Practice Guide for Fraud Control, CLEB 1994.

2.3 The Commissioner has issued a Chief Executive Instruction (CEI) which specifies responsibility for the development, implementation and review of the ATO's Fraud Control Plan.[28] The Commissioner also demonstrated his strong commitment to a comprehensive fraud control environment through the following initiatives:

- establishing a semi-autonomous FP&C Section with delegated powers of access and inquiry. The Section has the authority to directly refer cases for prosecution to the DPP;
- establishing an independent committee structure to provide advice on the strategic direction of ATO fraud control policy and operations and to give further confidence that the ATO is maintaining the highest professional standards;
- making it mandatory for all existing and new ATO staff to attend fraud awareness training seminars presented by the FP&C Section (further discussed in Chapter 3); and
- producing a number of publications, to cover aspects of the ATO's fraud control policy.

Organisational arrangements for internal fraud

2.4 The current ATO Fraud Control Plan specifies that external fraud control is largely devolved to each ATO Business and Service Line (Figure 1 illustrates the ATO's Business and Service Line structure.) Although the FP&C Section (which is part of ATO Corporate) has overall responsibility for investigating internal fraud matters, the ATO Business and Service Lines are equally responsible for ensuring an effective fraud control environment within the ATO.

2.5 Chapter 1 identified a number of additional areas that contribute to the ATO's operational fraud control framework (paragraph 1.23). The ANAO focused primarily on the principal areas responsible for the operational and strategic direction of internal fraud control within the ATO. These areas are the:

- the FP&C Section; and
- the Integrity Advisory Committee and the ATO Audit Committee.

---

[28] The CEI on Fraud Control Plan was first issued in 1997. It has since been revised and re-issued in July 2000.

Role of Fraud Prevention and Control Section

2.6 To ensure impartiality in decision making and to maintain independence from other areas of the ATO's operations, the ANAO considers that the fraud prevention and control area of an agency should operate semi-autonomously. That is, it should have a direct reporting relationship with senior executive management.

2.7 The ANAO considers that the current lines of reporting provide FP&C Section with an acceptable degree of autonomy. Although part of ATO Corporate, the Section reports directly to the ATO Executive.

2.8 The ATO's FP&C Section located within the Internal Assurance Branch (IAB) is responsible for the prevention, detection and investigation of internal fraud and fraud-related issues. Figure 6 provides an overview of the organisational and reporting arrangements for internal fraud within ATO from the FP&C Section perspective.

2.9 The FP&C Section underwent a significant restructure in 1995. It contains two Units whose functions are shown in Table 1.

Table1

Functions of the FP&C Section

Fraud Prevention and Education	Investigations
• Fraud control planning within ATO; • Developing and presenting fraud and ethics awareness programs, including induction programs and internal communication strategies; • Developing fraud impact statements on new and revised policies; • Undertaking probity reporting; and • Providing fraud prevention consultative services. The Investigations Services forms part of this Unit and is responsible for: • Managing investigations referred to the FP&C Section; • Providing secretariat services for the Integrity Advisory Committee (discussed in paragraphs 2.12 to 2.18); • Monitoring the implementation of the Fraud Control Plan within ATO and • Administering of the FP&C Case Management System.	• Investigating potential and actual internal frauds; • Monitoring the progress of investigations; • Determining when internal fraud will be referred to the Australian Federal Police (AFP) for investigation or Commonwealth Director of Public Prosecutions (DPP) for prosecution; • Identifying corporate risks and 'control issues'; and • Investigating and assessing liability on safe custody of public money and public property. The Fraud Investigation Services for the Child Support Agency are also the responsibility of this Unit. The Unit is responsible for providing fraud prevention and internal investigation services to the Child Support Agency under a contractual arrangement and a service agreement.

2.10 The separation of fraud prevention and investigation functions demonstrates a structured approach to fraud control. The current structure has enabled FP&C Section to implement a full scale fraud awareness training program (discussed in Chapter 3) without compromising its investigation activities. The further segregation of the investigation referral function from the investigations areas emphasises the commitment to timely and independent investigations.

2.11 The Section is predominantly staffed with ex-AFP officers who have extensive investigations experience. As at June 2000 the FP&C Section had 30 staff, of whom 15 were responsible for undertaking internal investigations. The Section's budget allocation for 1999–2000 was $2.9 million.

Integrity Advisory Committee and ATO Audit Committee

2.12 Until 1998 the FP&C Section reported through the Internal Assurance Branch to the ATO Audit Committee.[29] On particularly sensitive matters they could report directly to the Commissioner of Taxation.

2.13 In October 1998, the Public Service and Merit Protection Commissioner, the Commonwealth Ombudsman and the Commissioner of the AFP accepted an invitation from the Commissioner of Taxation to provide representatives of their organisations to form an ATO Fraud Committee (subsequently re-named Integrity Advisory Committee—IAC). The Committee was to advise and provide assurance on the management and operations of the FP&C Section.[30]

2.14 In October 1999, during hearings of the Senate Economic References Committee Inquiry into the *Operations of the ATO*, the ATO advised that the Fraud Committee provided an overseeing role for the work of the FP&C Section.

2.15 Since then, the Fraud Committee (now referred to as the IAC) has considered its role, and does not wish to be involved in overseeing operational aspects of ATO's fraud prevention and control function. In discussions with the ANAO the IAC indicated that it perceives its role to be as an adviser, rather than as part of the ATO management structure. The IAC views the ATO Audit Committee having responsibility for overseeing fraud control because of its statutory role under the FMA Act.

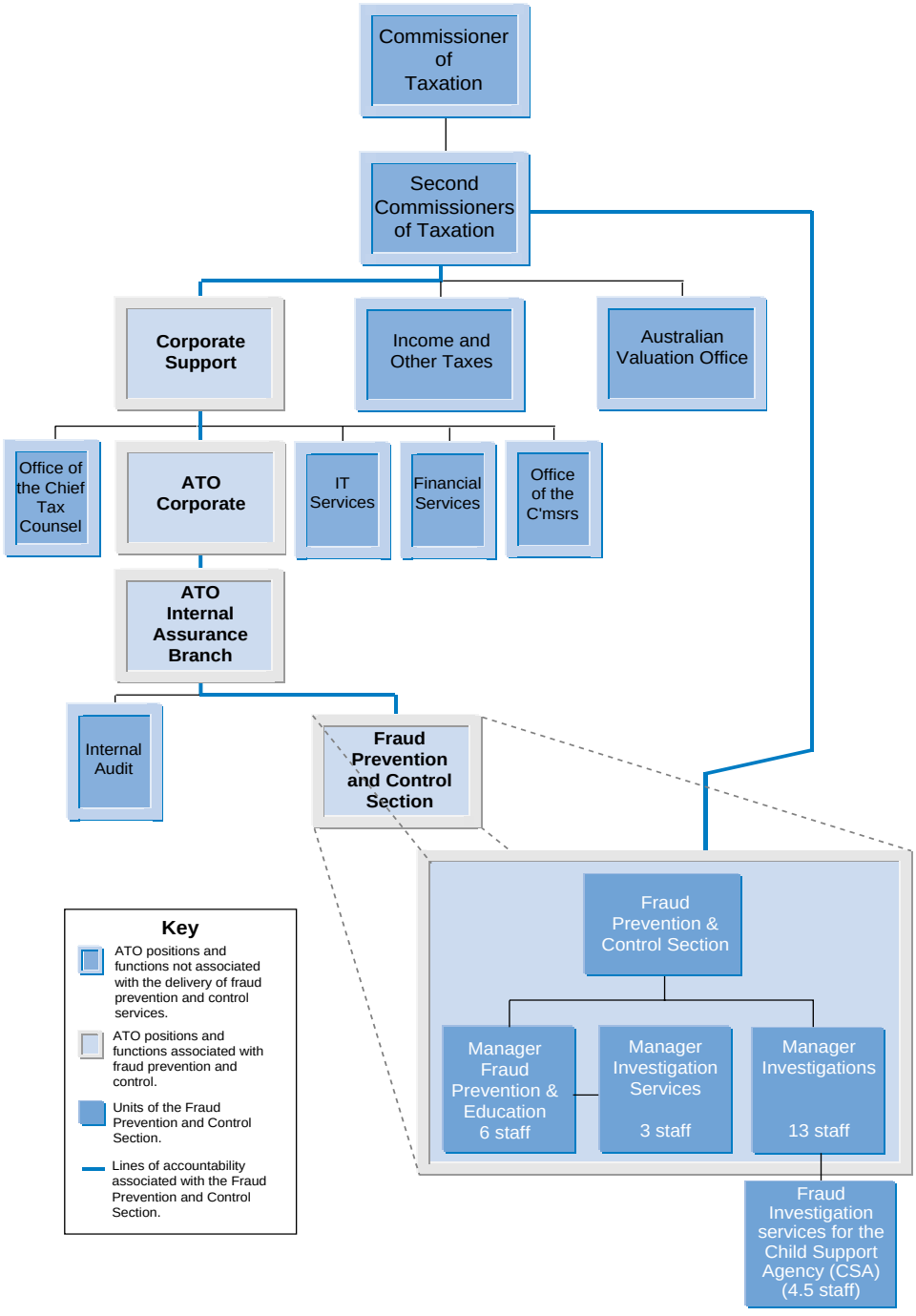
---

[29] Under section 46 of the FMA Act, a Chief Executive must establish and maintain an audit committee for the Agency, with the functions and responsibilities required by the Finance Minister's orders.

[30] The Fraud Committee would be chaired by a member of the ATO Executive (Second Commissioner of Taxation). Other ATO members of the Committee are: Assistant Commissioner Internal Assurance Branch and Deputy Commissioner ATO Corporate.

Figure 7

Organisational and reporting arrangements for internal fraud within ATO



2.16 In addition, external members of the IAC emphasised that their focus is on matters relating to internal fraud and the conduct of the ATO staff, as opposed to taxpayer or external fraud issues. In April 2000, a Memorandum of Understanding (MoU) was signed by the Chair of the IAC (an ATO Second Commissioner) on behalf of both the Committee and the Commissioner of Taxation. The MoU sets out the broad terms of reference of the IAC that include providing advice on ethics and on issues concerned with enhancing community confidence in the integrity of the ATO (see Appendix 2 for details). The MoU reflects the current thinking of IAC members.

2.17 The ANAO considers that the formation of the IAC demonstrates the ATO's commitment to promoting an effective fraud control environment. We support the ATO's initiative in establishing a mechanism for external input to ensure its approaches and attitudes are not insular. Expanding the role of the IAC to cover integrity matters recognises the overlap between ethics and fraud, given that fostering an ethical organisational culture is associated with fraud minimisation.

2.18 However, we also consider that there needs to be a clear understanding, within the ATO and by external stakeholders, of the delineation of roles and responsibilities between the Audit Committee and the Integrity Advisory Committee, especially in view of the change in functions of the IAC noted above.

Planning for effective fraud control

2.19 A comprehensive planning regime based on appropriate risk assessment processes is a key element of a corporate governance framework. The Commonwealth Fraud Control Policy requires a fraud risk assessment to be conducted as part of the development of a Fraud Control Plan, and fraud control arrangements to be reviewed every two years. The Commonwealth Fraud Control Policy Guidelines specify that plans developed as a result of the fraud risk assessment should include both a Fraud Control Plan for the agency as a whole and specific action plans for those areas which have been identified as having a medium to high level of risk.

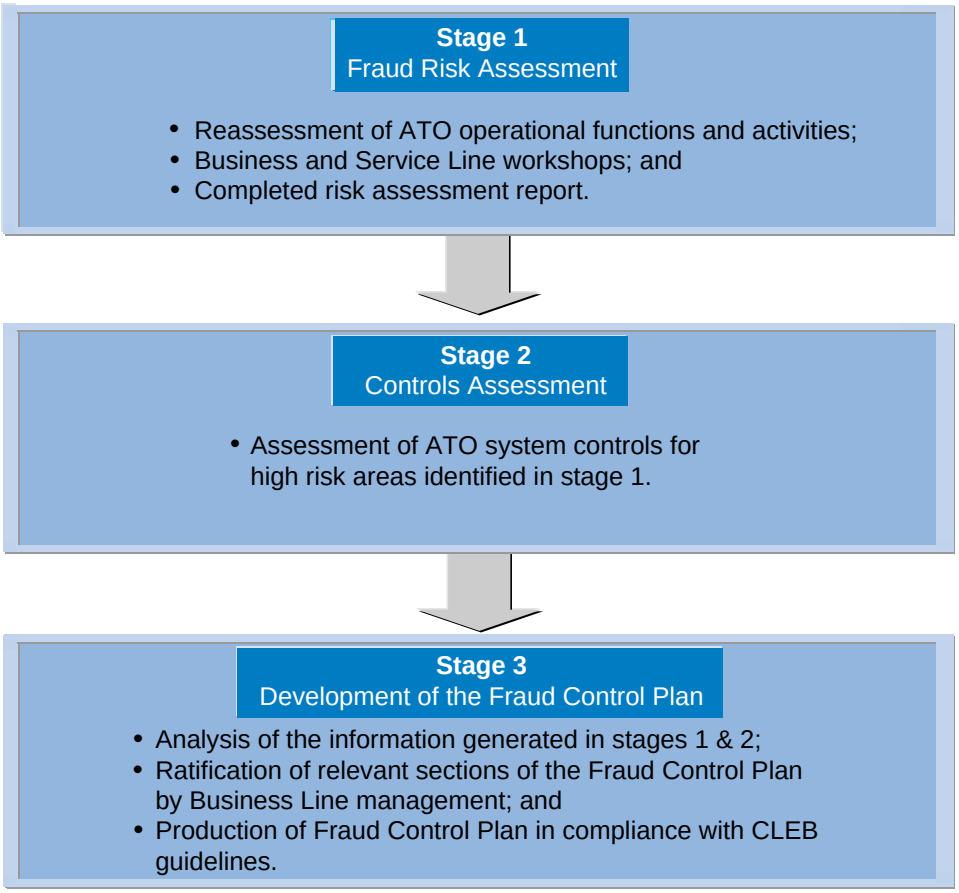
2.20 The ANAO considers that a Fraud Control Plan should contain appropriate links to the broader objectives and directions of an agency as outlined in the agency's corporate plan and the activities specified in the business and operational plans of the relevant work areas.

Fraud risk assessment

2.21 The ATO undertakes an agency-wide fraud risk assessment every two years in accordance with the Commonwealth Fraud Control Policy. The 1999–2001 fraud risk assessment was undertaken as a discrete process independent of the ATO's Health of the System Assessment (HOTSA) process. The HOTSA is the ATO's formal risk management process, which forms part of its strategic planning framework, and which has been undertaken on an annual basis across all ATO Business Lines since 1994–95. It requires each of the Business and Service Lines to address their major areas of risk and establish plans to manage those risks. [31]

Figure 8

Fraud control plan methodology



[31] ANAO Audit Report No.37 1996-97 focused on broad strategic issues relevant to risk management in the ATO as a whole, and aimed to assist the agency to focus better on the implementation of risk management principles.

2.22 The most recent fraud risk assessment (separate from the HOTSA process) was conducted between February and June 1999 for the 1999–2001 Fraud Control Plan. The ATO engaged consultants to assist with the development of the fraud risk assessment and Fraud Control Plan. Figure 8 illustrates the methodology used to develop the ATO's fraud control plan. Fraud risk assessment is used in this process.

2.23 As part of stage one, a reassessment of all functions and activities was undertaken. This involved holding several workshops with representatives nominated by Business and Service Lines to assess the fraud risk for all ATO functions and activities against an agreed set of criteria. Where functions had recently undergone changes, and processes were in transition, the risk assessment recognised that the ATO would need to address the risks in the new environment at a later stage, for example, the ATO outsourcing its information technology infrastructure and support systems, and the inclusion of Excise as an ATO Business Line since February 1999. The fraud risk assessment methodology used in 1999 is outlined in detail at Appendix 3.

2.24 As part of the second stage, high risk[32] areas were assessed to determine what controls were in place to prevent, detect or deter fraudulent activity. The ATO has indicated that this assessment does not provide a full audit of controls and relies on a range of evidence including interviews, reviews of manuals and observations to determine the controls which are in place. The ATO has acknowledged that it has not tested the systems or controls to determine the extent of compliance with the procedures.

[32] The ATO acknowledges that the determination of activities considered to have a higher risk of fraud is to a large extent subjective. In reaching this determination the Inherent Risk and Residual Risk ratings (see Appendix 3) were used to identify the higher risk functions and activities.

2.25 The development of the current (1999–2001) ATO Fraud Control Plan was the third stage of this process. The Plan describes the controls in place to prevent, detect and deter fraud in the high-risk activities identified in the first stage. The ANAO found that the methodology adopted by the ATO during the latest round of risk assessments was sound and that it complied with the Attorney-General's Department requirements. In particular:

- the methodology was capable of being consistently applied across all the ATO Business and Service Lines;
- the methodology was capable of 'green fields'[33] measurement of fraud risk;
- staff from Business Lines with an operational knowledge of the processes were involved in the workshops to gather risk assessment data; and
- Business Line management were involved in the review and ratification of the risk assessment data generated from the workshops.

ATO approach to the tax reform projects

2.26 The approach to fraud risk assessment outlined above was negotiated with the ATO Executive and the Attorney-General's Department in the context of major tax reform being undertaken between 1998–2000. It was agreed that the ATO would not undertake risk analysis on processes that were no longer relevant following the implementation of tax reform policy in July 2000. Due to the constant changes in the areas undergoing tax reform, a decision was made to conduct formal fraud risk assessment of all activities covered by tax reform when the systems and procedures were ready for implementation.

2.27 In May 2000, the ATO commenced the formal risk assessment process for a number of Goods and Services Tax (GST) projects. The results of fraud risk assessments are to be incorporated into the ATO's fraud control planning processes as they were finalised. As an interim measure, the Internal Assurance Branch asked ATO Project Managers (those responsible for managing individual reform projects) to be aware of their responsibilities to identify and address project, fraud and business risks for particular processes.

2.28 The ANAO considers the approach to fraud risk assessment in relation to reform projects to be appropriate.

---

[33] This involves the measurement of the risk of internal and external fraud in the absence of any system of internal control to prevent or detect the occurrence of the fraudulent activity.

Future approach to fraud risk assessment

2.29 The ATO has recognised the need for an ongoing program of fraud risk assessments. The ATO has proposed to the Attorney-General's Department that it will undertake a rolling program of fraud risk assessments as functions and new systems become operative.

2.30 The ANAO supports this approach and considers that the ATO should move towards incorporating relevant aspects of the fraud risk assessment process as an explicit element of the broader ATO risk management processes (that is, the HOTSA, referred to in paragraph 2.21). Through adopting this more holistic approach to risk management, fraud risks could be assessed and managed in association with other business risks faced by the ATO. This approach would be consistent with the preferred policy direction in a revised Commonwealth Fraud Control Policy currently being developed.[34]

Fraud Control Plan

2.31 In Chapter 1 we outlined that a Fraud Control Plan is a specific requirement of both the Commonwealth Fraud Control Policy and the FMA Act. The Fraud Control Plan provides a mechanism for outlining an agency's overall approach to fraud control and should:[35]

- reflect the risks identified in the fraud risk assessment;
- present strategies to rectify shortcomings identified in the risk assessment;
- provide a timetable for implementation of the strategies; and
- nominate action areas responsible for implementing each strategy.

2.32 The ANAO noted that the ATO's 1999–2001 Fraud Control Plan met the requirements of the Commonwealth Fraud Control Policy as assessed by the Attorney-General's Department in January 2000. The Fraud Control Plan includes matters that are specific to Business and Service Lines and others of a more general or strategic nature. For each of the high risk functions, the Plan summarises the process, identifies potential fraud threats, undertakes a control assessment (that is, identifies controls in place to prevent, detect and deter fraud) and presents an overall assessment.

---

[34] *Consultation Draft No. 1.*

[35] *Better Practice Guide for Fraud Control, CLEB 1994.*

2.33 Where an overall assessment identifies a need to improve controls to reduce the risk of fraud, recommendations have been included to rectify the deficiencies. The recommendations are considered to be 'action items' when accepted by the relevant ATO operational area. The Plan also includes timeframes for action items to be implemented. The timeframe is specified as short, medium and long-term, as opposed to specific dates. The ANAO notes, however, that the Fraud Control Plan does not provide any guidance on what is meant by short, medium and long-term. This becomes important when monitoring the implementation of the action items.

2.34 The ANAO considers that a more explicit timetable for action item implementation could be used to better facilitate on-going monitoring.

Monitoring and implementation of the Fraud Control Plan

2.35 Each Business Line determines whether to accept the recommended action items (to address the area of weakness) or introduce another solution to improve the control environment and thereby reduce the risk of fraud. Following agreement to Fraud Control Plan action items, the Business Lines have the responsibility to ensure that these items are implemented effectively. The FP&C Section is responsible for monitoring and coordinating the process and reporting to the ATO Executive on the implementation of the Fraud Control Plan.

2.36 The ATO experienced problems with the implementation of the 1997–99 ATO Fraud Control Plan. Governance reports from Business and Service Lines to the ATO Executive were the primary mechanism for advice on the implementation of, or decisions to vary, action items in the Fraud Control Plan. The FP&C Section stated that it had adopted a passive approach to monitor the Fraud Control Plan, relying on Business Lines to report variations to the Fraud Control Plan through the corporate governance reporting process. However, the reporting process did not reveal the action items that were not implemented or other improvements substituted.

2.37 In recognition of the problems experienced with monitoring and implementing the 1997–99 Fraud Control Plan, the ATO has improved the monitoring process for the 1999–2001 Fraud Control Plan.

2.38 A small team of staff has been established within the FP&C Section to monitor implementation of the Fraud Control Plan on a full time basis. Their duties include:

- regularly monitoring action items to ensure they are implemented in a timely manner;

- identifying changes to systems, or the introduction of new systems and conducting a fraud risk assessment of these systems;
- performing control reviews of those activities assessed as high risk and developing additional controls as appropriate; and
- reporting to the Audit Committee and the IAC on the implementation of the Fraud Control Plan.

2.39 A revised CEI on the Fraud Control Plan was also issued on 1 July 2000 to clearly specify the responsibility of the FP&C Section and the Business Lines. The revised implementation and monitoring strategy also requires all Business Lines to report as part of the corporate governance process on the status of their responsible action items in the 1999–2001 Fraud Control Plan.

2.40 The FP&C Section had also established a Fraud Control Liaison Officers Network, which comprises representatives from ATO Business and Service Lines. Staff of the FP&C Section chair meetings (proposed to be held twice a year) to discuss progress on implementation of the action items.

2.41 The ANAO acknowledges and supports these initiatives. However, to ensure effective implementation of the Fraud Control Plan, the staff responsible should also have access to sections of the Fraud Control Plan relevant to their area of operation. ANAO's discussions with a number of staff in different Business Lines indicated that staff were either unaware of an ATO Fraud Control Plan or, if they were aware, they had no access to it.

2.42 Because of its classification status as 'Protected', the ATO had limited circulation of the Fraud Control Plan. However, to ensure effective implementation of action items, operational staff need to understand the context and the reasons for implementing the action items.

2.43 To overcome the issue of limited circulation of the Fraud Control Plan, one Business Line developed its own Fraud Control Plan. This Fraud Control Plan reflected relevant sections from the ATO Fraud Control Plan and was circulated to appropriate staff within the Business Line to ensure effective implementation of action items.

2.44 The ATO advised that, with the classification of the Fraud Control Plan as a protected document in mind, the FP&C Section, in consultation with service providers has been: redeveloping the fraud risk assessment methodology to enable the Fraud Control Plan to become a more strategic planning tool; and examining ways to use e-publishing of relevant parts of the Plan to improve access to it.

Recommendation No.1

2.45 The ANAO recommends that, to enable the Fraud Control Plan to be effectively implemented, the ATO develop a strategy to ensure that staff required to implement Fraud Control Plan action items are given appropriate access to the Plan, or extracts from it, and a clear indication of implementation timetables.

ATO Response

Agree.

Links to Corporate Plan and other business/operational plans

2.46 To ensure effective internal fraud control arrangements, agencies need to promote a coordinated approach to fraud control planning. The ATO Fraud Control Plan should be clearly linked to the ATO's Corporate Plan. In addition, the business/strategic plans for the various ATO Business Lines should be linked to these higher level documents.

2.47 The ANAO found that through its fraud control function the ATO has provided some links to its Corporate Plan. The Fraud Control Plan was indirectly linked to ATO's Corporate Plan through the identification of the majority of processes and mechanisms to manage ATO fraud control arrangements. However, the ANAO considers that this link could be strengthened if the Fraud Control Plan includes a reference to its contribution in achieving agency objectives.

2.48 The ANAO examined the Business Plan for the FP&C Section, as well as those for two ATO Business Lines (referred to as Strategic Plans) to establish whether these were appropriately linked.

2.49 We found that closer links between the FP&C Section Business Plan (1999–2000) and the Fraud Control Plan would ensure the activities of the Section align better with the action items identified in the Fraud Control Plan. During the course of the audit, the FP&C Section finalised the 2000–2001 Business Plan that develops these links.

2.50 However, the Business Lines' Strategic Plans (for 1999–2002), examined for two ATO Business Lines, did not show direct links to the Fraud Control Plan nor include reference to the risks established through the fraud risk assessment process. The ANAO recognises that Business Line Strategic Plans are high level documents which focus predominantly on ATO clients. However, reference in these planning documents to the Fraud Control Plan would increase staff awareness of fraud control issues and ensure that the Fraud Control Plan is not developed in isolation.

Recommendation No.2

2.51 The ANAO recommends that the ATO adopt a more holistic approach to risk management and planning processes by:

- incorporating relevant aspects of its fraud risk assessment process as an explicit element of the broader ATO risk management processes to enable fraud risks to be assessed and managed in association with other business risks faced by the ATO; and
- linking fraud control planning to its strategic management and business planning processes as part of its corporate governance framework.

ATO Response

Agree.

ATO performance assessment framework—internal fraud control

2.52 Performance assessment of internal fraud control activities is vital to assess the effectiveness of an agency's fraud control arrangements. It also forms part of an agency's accountability to its key stakeholders such as the Parliament, the community and clients.

2.53 The ANAO examined the ATO's performance assessment framework for internal fraud in terms of:

- operation of the fraud control function; and
- the ATO Business and Service lines.

Operation of the fraud control function

2.54 Until 1998–99, the Internal Assurance Branch (IAB) operated on the basis of a Service Agreement with the ATO Audit Committee. This Agreement covered the operations of the IAB's Internal Audit Section and the FP&C Section. The performance indicators specified in the Service Agreement in relation to fraud control function were:

- a high level of satisfaction among both the Commissioners and the Audit Committee in regard to the Section's internal investigations and its fraud control functions;
- the extent to which fraud impact statements were included in ATO policy proposals;
- a high rate of acceptance of prosecution of cases referred to the DPP; and
- a reduction in the average time taken from commencement to completion of an investigation.[36]

[36] This data was computed manually and was based on the number of investigators working each quarter and the number of investigation cases finalised.

2.55 The Service Agreement expired at the end of June 1999 and has not been renewed. The FP&C Section indicated that it was awaiting resolution of its operating arrangements, especially with regard to the Integrity Advisory Committee (that is, whether the Section would have a separate service agreement with the Integrity Advisory Committee). The Section was also of the view that more meaningful performance indicators were required.

2.56 The Section's 1999–2000 performance assessment framework included:

- an FP&C Section Business Plan;
- individual staff performance agreements; and
- governance reporting processes.

2.57 On analysing these elements, the ANAO found that the 1999–2000 performance assessment framework did not provide sufficient information to assess and evaluate adequately the performance of the fraud control function on an ongoing basis.

2.58 The FP&C Section Business Plan was seen as an activity statement which identified various activities to be undertaken within the Section in relation to fraud prevention, fraud investigations, administration and staff development. It also detailed the positions responsible for undertaking these activities and a timetable. While the statement of activity was useful in guiding and directing the work of the Section, with the timetable providing some measure of the milestones to be achieved, it did not include any performance information to allow its performance to be measured qualitatively or quantitatively.

2.59 The ANAO noted that individual staff performance agreements were linked to the FP&C Section Business Plan. However, these agreements did not include any specific performance measures. They referred to performance indicators in the service agreement between FP&C Section and the Integrity Advisory Committee (IAC). As mentioned earlier the IAC has adopted an advisory role and no longer operates on the basis of a service agreement.

2.60 As a result of the ANAO's findings, the FP&C Section developed its 2000–2001 Business Plan based on the Commonwealth outcomes/output framework. The current Business Plan demonstrates the Section's effort to improve the measurement of its performance. However, there is scope to further refine the Business Plan in areas such as identification of outputs, targets and performance indicators (qualitative and quantitative).

2.61 As part of the governance reporting process, the FP&C Section prepares monthly and six monthly governance/accountability reports.[37] These are submitted through the IAB to the Corporate Assurer's Group.[38] The FP&C Section reports to the Audit Committee on a quarterly basis (focusing on statistical information and administrative issues). It also provides quarterly executive briefings through IAB to the ATO Executive on the status of FP&C Section activities in relation to fraud prevention and investigation. Such briefs include sensitive information, and quarterly case statistics such as reporting rate, case completion rate compared to previous years, and case workload trends.

2.62 The ANAO noted that these briefings address the performance indicators specified in the 1998–99 service agreement (which has now expired). Often these briefings include summarised cases of interest, including operational information on significant cases and identifying control issues. The briefings also refer to progress on development of the Fraud Control Plan but do not address implementation aspects of the Fraud Control Plan. The ATO advised that, when the corporate governance and assurance processes were implemented within the ATO, a decision was made earlier this year to restrict the briefings to the status of significant investigations and associated control issues as all other information, including the status of fraud control planning and fraud awareness programs, were reported through the corporate governance process.

2.63 In May 1998 the IAB undertook projects on benchmarking and contestability in relation to Internal Audit and Fraud Prevention and Control. As part of the contestability study the structure and classification profiles of the internal investigation area were compared to those of a number of State and Commonwealth agencies. However, the study did not undertake quantitative comparisons with other agencies relating to case loads, time taken and costs of finalised investigations, fraud prevention and detection capability. ATO advised that the lack of quantitative data greatly impeded this exercise.

---

[37] The monthly reports include information on an exception basis. The six monthly report includes information relating to: proportion of ATO staff participation in internal fraud awareness seminars; reporting rates of matters for internal investigation and trends in investigation workload; financial position of the Section; and any significant issues.

[38] This Group is responsible for providing overview reports on aspects such as finance, security, information technology, internal audit and human resources.

2.64 The ANAO acknowledges the FP&C Section efforts to report on its performance through the various governance reporting processes, but considers that this should be linked to an agreed assessment framework which includes qualitative and quantitative measures. As well, establishing targets and benchmarks for performance indicators where possible would make the process more transparent and increase the Section's accountability. The ANAO considers that the development of a Business Plan based on an output/outcomes framework would provide an appropriate basis for performance reporting.

Recommendation No.3

2.65 The ANAO recommends that the ATO further refine the performance assessment framework to enable quantitative and qualitative assessment of its internal fraud control function.

ATO Response

Agree.

ATO Business and Service Lines

2.66 As mentioned in Chapter 1, fraud control reports are the principal mechanism for Chief Executive Officers to provide assurance to their respective Ministers that they have fulfilled their legislative requirements with respect to fraud control arrangements. The ATO advised that it has fulfilled these requirements through the annual reporting process. However, the ANAO notes that the ATO has not submitted a separate fraud control report to its Minister in accordance with the FMA Act.[39]

2.67 The Commonwealth Fraud Control policy also requires agencies to submit fraud control information annually to Attorney-General's Department, including reporting on losses and overpayments. The ATO has acknowledged in its 1999–2001 Fraud Control Plan that it has not done so, pending the revision of the current Commonwealth Fraud Control Policy.[40] However, the Attorney-General's Department has advised the ANAO that until such time as a revised policy is introduced, the Commonwealth Fraud Control Policy (1994) remains in force, including its annual reporting requirements.

2.68 The ATO's governance reporting process has been operating for a number of years. The governance reporting process forms part of the corporate governance framework. Each Business Line and members of the Corporate Assurer's Group provide these reports.

---

[39] 22.1, Part 2, *Financial Management and Accountability Orders 1997*.

[40] The Attorney-General's Department advised that the ATO had been fulfilling this requirement until 1997–98.

2.69 Each Business Line is also required to complete a corporate governance questionnaire to provide the Commissioner with an assurance that environmental and financial controls are operating efficiently, effectively and ethically within their respective Business Line. The Chief Finance Officer collects and reviews these questionnaires annually on behalf of the Commissioner.

2.70 The corporate governance questionnaire includes reference to the existence of management controls and requires certification by Business Lines on areas such as negligence, misconduct and fraud.[41]

2.71 The ANAO notes that, as part of its 1999–2000 Business Line performance and governance reporting requirements (issued in May/June 2000), the ATO has included an additional requirement for Business Lines to report on performance against their section of the Fraud Control Plan. It states that '*IAB Fraud Control Unit will work with Line Fraud Control Plan representatives*[42] *to prepare a corporate performance report for the Commissioners. Individual Lines will then be able to add their Line specific information to their governance report….*'. The corporate governance questionnaire now incorporates a sign off on implementation of the Fraud Control Plan.

Conclusion

2.72 The ATO is progressing towards incorporating aspects of fraud control reporting as part of its corporate governance framework. The ATO has established a comprehensive fraud control policy framework and, through a number of mechanisms, has demonstrated a commitment to a comprehensive fraud control environment. Current organisational arrangements provide the necessary independence from mainstream Line areas. The development of a comprehensive Fraud Control Plan, based on systematic agency-wide fraud risk assessments is consistent with better practice and complies with the Attorney-General Department requirements. The ATO has also incorporated the implementation of the Fraud Control Plan into its overall performance assessment framework.

---

[41] Business Lines have to certify that all cases of fraud in their Business Line were properly dealt with and disclosed to the Chief Finance Officer.

[42] These are the Business Line Fraud Prevention and Control Liaison Officers responsible for coordinating fraud prevention and control activities within their Business Line.

2.73 To ensure that the ATO's internal fraud control framework becomes an integral part of the corporate governance framework there are a number of areas which require attention. These include:

- adopting a more holistic approach to risk management and planning processes to enable fraud risks to be assessed and managed in association with other business risks faced by the ATO;
- linking the fraud control planning process to its overall strategic management and business planning process so that it forms part of the strategic management and corporate governance framework; and
- further refining its performance assessment framework to enable quantitative and qualitative assessment of the performance of ATO's internal fraud control function.

3. Fraud Prevention

This chapter discusses fraud prevention and the initiatives and controls utilised by the ATO to prevent internal fraud. In particular it examines the measures undertaken by the Fraud Prevention and Control Section to inform and educate ATO staff about fraud; and the initiatives undertaken by ATO Business Lines to ensure ATO system controls address fraud control issues, including quality assurance.

Introduction

3.1 The formulation of a robust control environment based on ethical practices, comprehensive training programs and strict adherence to Commonwealth policies and procedures is an effective method for Commonwealth agencies to prevent fraud. Although many Commonwealth agencies have well-established administrative fraud prevention controls,[43] a highly effective fraud prevention strategy also requires specific fraud prevention programs such as fraud prevention training. The combination of both robust system controls and targeted fraud prevention training programs underpin a coordinated and effective fraud prevention strategy.

3.2 Since 1987, Australian Governments have emphasised the importance of Commonwealth agencies preventing fraud through the implementation of an effective fraud prevention strategy. This emphasis was strengthened in the 1994 Commonwealth Fraud Control Policy, which notes that:

> *Fraud flourishes in an administrative environment where opportunities exist for waste, abuse and mismanagement. The Government is convinced that its emphasis on fraud prevention as part of its financial management and law enforcement policies will reduce these opportunities for waste, abuse and mismanagement.*[44]

---

[43] An example of a common control used to prevent fraud is the segregation of duties. This control is particularly important for positions that require the receipting and payment of money.

[44] Commonwealth Law Enforcement Board, *Best Practice for Fraud Control—Fraud Control Policy of the Commonwealth*, 1994, paragraph 39, p25.

3.3 The development of a comprehensive fraud prevention strategy consumes considerable resources and may not produce immediate, apparent or tangible results. However, agencies can obtain significant benefits from a comprehensive strategy through:

- the retention of information, assets and resources that may have otherwise been lost to fraudulent activity;
- cost savings associated with a reduction in expensive fraud investigations and prosecutions; and
- a public and staff perception that an agency has a high level of integrity regarding the protection of public assets.

ATO fraud prevention strategy

3.4 The principal influence on organisational culture is ethical conduct by management, and in particular by the Chief Executive Officer (CEO). Studies conducted on the impact of management behaviour on the attitudes of staff showed that staff were more likely to do what they see their supervisor doing, than adhere to ethics policy.[45] Other research conducted into the impact of CEO opinions on ethical behaviour showed that:

> *Statements from the CEO on his or her stance on ethics have more impact on staff decision making than do the staff's own ethical goals or beliefs.*[46]

3.5 The ATO, and in particular the Commissioner of Taxation, has recognised the importance of the ATO's ethical environment in maintaining community confidence in the taxation system, and in its revenue collection responsibilities. In a 1998 media release, the Commissioner of Taxation stated:

> *The community has a right to expect the ATO to administer the tax system in an ethical and responsible manner.*[47]

3.6 To determine whether the ATO was committed to promoting an organisational culture of high ethical standards and minimising fraud, the ANAO examined: the ATO fraud prevention strategy; the ATO fraud

---

[45] Soutar, G., McNeil, M.M., & Molster, C. (1994) *The Impact of the Work Environment on Ethical Decision Making: Some Australian Evidence*. Journal of Business Ethics,13(5), pp. 327-339.

[46] Hegarty, W.H., & Sims Jr. H.P. (1979) *Organizational Philosophy, policies and objectives related to unethical decision behaviour: A Laboratory Experiment,* Journal of Applied Psychology, 64, No.3, pp. 331-338.

[47] *Fraud Prevention in the ATO—Judge For Yourself*, Australian Taxation Office Media release Nat98/67, 15 December 1998.

program review methodology; other ATO fraud prevention initiatives; better practice by other agencies; and the facilitation of fraud prevention by ATO Business Lines.

ATO fraud awareness program

3.7 In 1997, the FP&C Section began to shift its emphasis from traditional reactive fraud control strategies to a pro-active fraud preventative strategy. This pro-active strategy has focused on the development and implementation of fraud awareness training programs and is complemented by a number of other initiatives.

3.8 In December 1998, the Minister for Justice and Customs and the Commissioner of Taxation launched a new fraud awareness training program known as *Judge For Yourself*.[48] The *Judge for Yourself* program is conducted in a workshop format allowing interaction between the FP&C Section presenters and ATO staff. A significant feature of these workshops is the use of an innovative interactive CD-ROM computer program that encourages staff participation. Since February 1998, 19 890 ATO staff had attended this workshop (as at June 2000). This accounts for a high proportion of all staff currently employed by the ATO.[49]

3.9 Although fraud prevention is the predominant theme of the *Judge For Yourself* program, it also covers other important issues, such as:

- ATO ethics;
- the procedures and mechanisms available to staff to report fraud to the FP&C Section;
- employee protection (for example victimisation of staff in the workplace); and
- the impact of the ATO Taxpayer's Charter on the ethics of the ATO.

3.10 At the completion of the workshop, participants are provided with a range of FP&C Section products to reinforce the information contained in the workshop (see Appendix 4 for the materials provided).[50] The *Judge for Yourself* CD-ROM is also distributed to Line areas throughout the ATO and is constructed so that it can be used as a stand-alone central fraud education and future reference tool.

---

[48] Other fraud awareness training modules cover areas such as ethics, APS Values and Codes of Conduct for managers and staff.

[49] ATO was unable to provide the ANAO with the exact proportion of staff that had undergone fraud awareness training since February 1998, as these statistics are subject to staff departures and arrivals since 1998.

[50] Other products include computer mouse mats with FP&C Section information.

3.11 The *Judge for Yourself* program has been complemented by a second program, *Play it Again Sam*, which is also presented in a workshop format and utilises CD-ROM technology. *Play it Again Sam*, like its predecessor, is designed to make staff aware of issues in relation to fraud, however it has a heavier emphasis on 'conflict of interest' issues.

3.12 Aside from educating existing ATO staff, the *Judge for Yourself* and *Play it Again Sam* training packages form part of a larger induction program for new staff. Induction training covers both the ATO graduate program as well as new ATO staff at all levels.

3.13 The FP&C Section has also developed a training package to educate ATO managers about the roles and responsibilities of the Fraud Prevention and Control Section.[51] Since 1997, in excess of 3000 senior level ATO staff have undertaken the training package. In addition, Commonwealth Public Sector Union (CPSU) representatives have also undertaken this training. The ATO considers that this has clarified the FP&C Section's role and responsibilities with the CPSU and fostered a sound working relationship.

3.14 The ANAO acknowledges that the ATO's fraud awareness training is an innovative and effective mechanism to teach and reinforce ATO ethics and fraud awareness. The ANAO also notes the emphasis placed on the *Judge For Yourself* and *Play it Again Sam* programs by the Commissioner of Taxation, who has issued an instruction for all ATO staff, including executive staff, to attend the programs. The ANAO considers that other Commonwealth agencies should consider the use of such material as part of their fraud prevention training.

ATO fraud program review methodology

3.15 Prior to the introduction of the *Judge for Yourself* program in December 1998, the FP&C Section commissioned a consultant to report on ATO staff awareness of fraud issues. The results of the consultant's examination were to serve two purposes. Firstly, the results of the examination were to form the basis for the development of the ATO fraud awareness program through the identification of fraud related topics that required explanation or further clarification. Secondly, the criteria used in the examination would be used to assess the effectiveness of the fraud awareness program at a later date.

---

[51] This training package outlines the methodology behind FP&C Section investigations, the rights of ATO staff involved in investigations, and investigation procedures.

3.16 In February 1998, the consultant completed a report on ATO staff awareness of fraud-related issues. The principal findings contained in the consultant's report were: many ATO staff had a less than adequate knowledge of fraud control and what constitutes fraud; and a comprehensive fraud awareness campaign would be strongly supported by staff.

3.17 In December 1999 (one year after the launch of the *Judge for Yourself* program), the FP&C Section commissioned the consultant to reassess the ATO Staff's knowledge of fraud-related issues. The major findings of this report were: that staff knowledge of ATO fraud control measures had increased;[52] staff difficulty in understanding fraud had decreased; [53] and staff were satisfied with the content of the FP&C Section training course.[54] The ATO also attributes the significant increase in the fraud-reporting rate by staff to this program. The ATO has advised that reviews of the ATO's fraud awareness program will continue in the future.

Feedback on the ATO fraud awareness program

3.18 Although the content of ATO fraud training programs relies predominantly on consultant evaluations, two other factors have a significant bearing on the content of the ATO fraud awareness program. These are:

- staff surveys conducted at the end of fraud awareness training (for example *Judge for Yourself*); and
- advice proffered by external ATO stakeholders, such as the Commonwealth Ombudsman.

---

[52] ATO staff awareness of ATO fraud control measures operated by the ATO for outside persons or organisations against the ATO increased (from 40 per cent awareness in 1998 prior to the fraud awareness campaign) to 72 per cent awareness following the campaign in late 1999.

ATO staff awareness of ATO fraud control measures operated by the ATO relevant to protecting the ATO from fraud by its staff increased (from 54 per cent awareness in 1998 prior to the ATO fraud awareness campaign) to 89 per cent following the campaign in late 1999.

[53] Staff not understanding what constitutes fraud by ATO staff fell from 21 per cent in 1998 to 13 per cent in 1999.

[54] Ninety-six per cent of staff supported the staff awareness program. Ninety-one per cent were satisfied with the content of the program.

3.19 In March 1998, the Commonwealth Ombudsman identified that ATO staff did not appear to have a comprehensive understanding of 'conflict of interest' issues. An evaluation of staff surveys by an external consultant in May 1999 confirmed that additional fraud training was required in this area. As a result the ATO developed the *Play it Again Sam* program, which, as noted above, specifically addresses 'conflict of interest' issues. The FP&C Section advised the ANAO that it intends to determine the success of the *Play it Again Sam* program when 80 per cent of all ATO employees have undertaken the program.

3.20 Based on the feedback provided by ATO staff, the reviews completed by an external consultant, and the establishment of comprehensive program review and development mechanisms, the ANAO considers that the ATO has developed an effective fraud awareness program that utilises innovative training methodology and techniques. Fraud awareness programs of this kind represent Australian Public Service better practice.

3.21 The ANAO conducted interviews with a sample of ATO staff throughout NSW, Victoria and Tasmania. We noted that the ATO staff interviewed had a good awareness of ATO fraud policy and were aware of their ethical responsibilities in relation to reporting fraudulent activity. They were made aware also of the standards of probity and ethics expected by the Commissioner of Taxation to undertake their duties. All staff interviewed indicated their understanding of these issues was influenced significantly by the ATO's fraud awareness training as well as internal circulars and minutes.

3.22 The ANAO noted that there is a strong awareness by ATO stakeholders that the Commissioner of Taxation and ATO staff have a strong commitment to the minimisation of fraud and the maintenance of high levels of ethics. In his 1999–2000 Annual Report the Commonwealth Ombudsman observed:

> *In my opinion, the Commissioner is genuinely concerned to ensure that ATO procedures and operations meet the professional and ethical expectations of the community and that he has the benefit of outside experience in designing strategies and approaches.*[55]

---

[55] *Commonwealth Ombudsman Annual Report 1998-99*, Commonwealth Ombudsman's Office, Canberra. p. 40.

3.23 Other external observers who have commented positively on the ATO's fraud prevention strategies have included the Australian Federal Police, Community and Public Sector Union, and the Public Service and Merit Protection Commission.

3.24 In response to concerns expressed by the Commonwealth Ombudsman in 1998 about ATO staff's understanding of conflict of interest issues, the FP&C Section developed a strategy for the avoidance of conflict of interest within the ATO. As part of this strategy, the Commissioner of Taxation has undertaken to appoint an Ethics Counsellor for the ATO.[56]

External scrutiny of ATO fraud and ethics processes

3.25 As mentioned in Chapter 2, the Commonwealth Ombudsman, the AFP and Public Service and Merit Protection Commission, as members of the IAC, can provide valuable contributions when observing and discussing ATO ethics and fraud control practices.

3.26 In August 1998, the Senate Economics References Committee began an inquiry into, amongst other things, allegations of internal corruption and organised crime within the ATO.[57] The Committee found that although no organisation can be fully protected from individuals with criminal intent, the ATO has:

> *…developed and implemented a comprehensive range of fraud prevention and control procedures and has subjected these procedures to external review.*[58]

3.27 The Committee praised the ATO for its commitment to preventing fraudulent practices in relation to the collection of taxation revenue and also noted that there was no credible evidence to suggest infiltration by organised crime.

---

[56] The role of the Ethics Counsellor will be to preserve the reputation of the ATO and its staff by undertaking a series of measures.

[57] The Senate Economics References Committee: *Operation of the Australian Taxation Office*, 6 August 1998. The terms of reference for the Committee can be found in Appendix 7.

[58] Senate Economics and References Committee, *Operation of the Australian Taxation Office*, 9 March 2000. p. xv.

Other fraud prevention initiatives

3.28 In addition to its fraud awareness program the FP&C Section is implementing a fraud control communications strategy throughout the ATO. This involves the dissemination of fraud prevention information, statistics, lessons learnt and case information throughout the ATO. Measures currently under consideration for the strategy include the establishment of an FP&C Section website, as well as the strengthening of existing contributions to the ATO's internal weekly publication *ATO Extra*.[59]

3.29 A highly effective method of establishing acceptable ethical behaviour, advocated by the NSW ICAC, is the distribution of information relating to the prosecution of fraudulent conduct. The ICAC noted that:

> *Making staff aware of the repercussions of corrupt conduct is considered to be a useful part of the education process. Publicising what happens to those who fail to comply with the rules was considered a positive way of communicating that the organisation is serious about corruption prevention.*[60]

3.30 The ANAO noted that the NSW Roads and Traffic Authority (RTA) exhibits better practice in this area.[61] It regularly publicises significant case studies to make staff aware of the types of fraudulent practices occurring in the RTA, and the consequences of fraudulent activities when detected. For example:

Case study 1

Putting the Horse Before Your Job

One of our fellow workers was a very keen punter – too keen in fact. She was responsible for handling some RTA money but from time to time she used part of it to place her bets. It all seemed pretty easy; bet with the RTA money; pocket the winnings; then replace the original money. Any shortfall from a loss was made up with her own money. Having more money to bet, the winnings were greater, but eventually so too were the losses. The use of RTA money for gambling continued for a period of six months before too many losses brought her undone. The

---

[59] *ATO Extra* is distributed to all ATO employees.

[60] ICAC research publications: *Tips from the Top: Senior NSW public sector managers discuss the challenges of preventing corruption*, 1/04/99.

[61] The RTA has been recognised as exhibiting better practice in the area of fraud prevention in the NSW Public Sector. It has received a number of awards for fraud awareness, including the *1999 NSW Premier's Public Sector Award for Ethics*.

employee was subsequently dismissed and later appeared in court. The employee is now serving a prison sentence and has repaid the stolen public money.

Some of her friends had noticed how stressed she had been for several months, but they did not feel confident to raise their concerns with her.

Point to remember:

Personal trust cannot be regarded as suitable control over RTA cash and assets. Managers must ensure appropriate controls are always in place.

Source: RTA Publication: *Audit Investigation Case Studies – We Are Almost There*

3.31 The FP&C Section use of *ATO Extra* could be an effective method of publicising the prosecution of fraudulent practices within the ATO. However, the ANAO notes that the FP&C Section's use of *ATO Extra* has been infrequent and considers that the FP&C Section could better utilise this publication as a means of disseminating case study information to assist in preventing fraud within the ATO.

Recommendation No.4

3.32 The ANAO recommends that, as an important element of the fraud education process, the ATO make greater use of its internal publication, *ATO Extra*, and other awareness raising techniques in publicising case studies and results of investigations conducted by its Fraud Prevention and Control Section.

ATO Response

Agree.

Other better practice

3.33 Although the FP&C Section has implemented and is a leader in a number of fraud prevention strategies that constitute better practice within the APS, the ANAO considers that it should continue to examine mechanisms used by other Government and private sector agencies, both nationally and internationally to minimise fraud.

3.34 The ANAO notes that the RTA is developing a computer-based ethical decision-making model for RTA staff. The model is designed to assist RTA staff in making ethical decisions when confronted with ethical problems. It utilises a computer program to guide the user through a series of questions that should ultimately determine whether the decision made by the user is ethical. Once the questionnaire is completed, a computer printout is generated illustrating the process undertaken to arrive at an ethical conclusion.

3.35 The ANAO considers that documentation of this type clearly outlining the reasoning behind a decision-making process is highly desirable, as it provides a clear audit trail and lines of accountability.

ATO Business Line fraud prevention practice

3.36 The prevention of fraud and the promotion of high ethical standards throughout the ATO is not limited to the programs and material produced by the FP&C Section. The ATO Business Lines are also responsible for successfully preventing fraudulent activity by ATO officers.

3.37 Unlike the FP&C Section that has a role to educate ATO staff on fraud control issues, the Business Lines are responsible for ensuring that ATO financial, administrative and management systems and processes are adequately protected from fraudulent activity. This is accomplished through the assessment, maintenance and review of the ATO system controls. In this context, the ANAO examined the performance of the two principal areas responsible for fraud control assurance (the Financial Services Section and the ATO Business Lines), in monitoring the Fraud Control Plan to prevent fraud and in implementing quality assurance processes.

Financial Services Section

3.38 The ATO's Financial Services Section[62] is responsible for the preparation of the ATO's financial statements and the provision of other financial services to ATO Business Lines. This includes the review and maintenance of ATO system controls relating to the efficacy of ATO financial management.

3.39 The ATO's Financial Services Section utilises a 'Certificate of Compliance' process to provide assurance that new financial systems[63] have controls in place to prevent and detect fraudulent activity. The Certificate of Compliance process involves a detailed assessment of both internal and external risks that may impact on a new ATO financial system. Once the risk assessment process has been completed, and appropriate controls are installed, a Certificate of Compliance is issued for the new system. A new ATO system is not allowed to go on-line until it receives a Certificate of Compliance. The ANAO considers that the Certificate of Compliance process provides a high level of assurance that system controls have been assessed to prevent fraudulent activity.

---

[62] The ATO's Financial Services Section is located within the ATO's Corporate Service Line.

[63] An example of an ATO financial system is the SAP R/3 system. This system is used for aspects of ATO financial administration including accounting, asset management, managing appropriations, budgeting and financial planning.

3.40 The ANAO noted that there were existing ATO systems that had not undergone a Certificate of Compliance process. The ANAO acknowledges that many of these systems were due for replacement soon after 30 June 2000. However, some of these systems will continue to operate as 'legacy systems'[64] after this date. The ANAO considers that controls for 'legacy systems' should be assessed and treated for fraud-related risks as the potential for fraud increases with less scrutiny of outdated systems.

3.41 The ANAO also noted that the Certificate of Compliance process was limited to financial systems.[65] As fraudulent activity can occur in both financial and non-financial[66] systems, the ANAO considers that the ATO should consider the certification of non-financial systems to ensure the adequacy of controls to prevent and detect fraudulent activity.

Recommendation No.5

3.42 The ANAO recommends that, to further protect its financial, administrative and management systems and processes from fraudulent activity, the ATO:

- conduct certificate of compliance checks on 'legacy systems' to provide assurance that adequate controls are in place to prevent and detect fraudulent activity; and
- extend its 'Certificate of Compliance' process to non-financial systems.

ATO Response

Agree.

Business Line Fraud Control Liaison Officers

3.43 As discussed in Chapter 2, the ATO has produced a comprehensive Fraud Control Plan to identify fraud control risks, and to develop action items to address those risks. The ANAO considers that the monitoring of fraud risks and the implementation of the action items identified in the Fraud Control Plan are important fraud prevention controls.

---

64 A legacy system is an older system that must be maintained for some time before being gradually rebuilt and replaced.

65 Systems that have undergone the certificate of compliance process include Australian Taxation Office Integrated System, National Taxpayer System, Super Guarantee System, Child Support Agency system; and numerous new GST systems.

66 A non-financial system is one that is not used to manage the financial resources of the ATO. For example the ATO's Electronic Lodgement System.

3.44 The ATO officers responsible for coordinating fraud-related issues within each Business Line are known as Fraud Control Liaison Officers. These officers are responsible for:

- the compilation of information used in the development of the Fraud Control Plan;
- the monitoring of, and reporting on, applicable action items and fraud controls identified in the Fraud Control Plan to the FP&C Section;
- Business Line liaison contact with the FP&C Section; and
- advice to the FP&C Section of changes to the Fraud Control Plan.

3.45 The ANAO notes that although the fraud control liaison officers are responsible for monitoring the Fraud Control Plan for their respective Business Lines, there has been no detailed or formal feedback provided to the FP&C Section on the Business Line's progress in relation to Fraud Control Plan action items. During the audit, the ATO revised the CEI's (see paragraph 2.3), which specify Business Line reporting responsibilities relating to the Fraud Control Plan.

3.46 However, it is important that Business Lines (through the work of the Fraud Control Liaison Officers) are held accountable for measuring Business Line progress against Fraud Control Plan action items, and for providing assurance that Business Line fraud controls are operating efficiently and effectively.

3.47 Gathering the information needed to determine Business Line performance against the Fraud Control Plan, requires that Fraud Control Liaison Officers have appropriate skill levels and experience commensurate with the responsibilities of the position. We noted that the seniority and experience of Fraud Control Liaison Officers varied markedly between Business Lines.

Business Line fraud prevention through quality assurance

3.48 The primary function of quality assurance processes is to provide key stakeholders with assurance that ATO systems produce reliable information, as well as information to continuously improve internal processes. An implicit feature of an effective quality assurance process is that it can also provide stakeholders with a degree of assurance that fraudulent activity has not occurred within that system.

3.49 ATO Business Lines have developed a variety of quality assurance processes to ensure the quality of information that ATO systems produce is appropriate. Although the ATO's quality assurance processes are not designed specifically to detect or prevent fraud,[67] these processes have the potential to support fraud control depending on the integrity of:

- the ATO systems; and
- the nature of the quality assurance processes (with respect to sampling rules and design to ensure conformance to internationally recognised quality standards).

3.50 The ANAO considers that, subject to the factors identified above, the ATO could assess its current quality assurance practices as an effective fraud prevention and detection mechanism and take appropriate action, as necessary to enhance their effectiveness.

Conclusion

3.51 The ATO has invested significant resources in the prevention of fraud and the creation of an ethical work environment. Through the creation of an ethical workplace culture and environment (which has been driven by the actions of the Commissioner of Taxation and the use of a vigorous fraud prevention training program), the ATO has established a sound platform for fraud control. As demonstrated by other leading fraud control agencies, a heavy emphasis on fraud prevention exhibits public sector better practice.

3.52 The ANAO considers that the ATO has implemented public sector better practice in relation to the critical areas of fraud control education and training. However, to further improve on the sound basis of the ATO's fraud prevention strategies, the ATO should further develop the:

- use of internal ATO publications to deter fraudulent activity;
- assessment and treatment of risks associated with 'legacy systems'; and
- use of the ATO's Certificate of Compliance processes for non-financial systems.

3.53 Improvements in these areas will complement the strong fraud prevention practices already exhibited by the ATO.

---

[67] The ANAO recognises there are other system controls that are not part of formal quality assurance processes but which contribute to fraud minimisation (for example, fraud awareness training as discussed in this chapter).

4 ATO Information Technology

This chapter examines ATO Information Technology security prevention and detection mechanisms. The ATO is reliant on its Information Technology to administer effectively and efficiently the collection of taxation revenue. In particular, we examined Information Technology security measures to prevent unauthorised access and manipulation of taxpayer information as well as the use of pro-active IT controls to detect fraud.

Introduction

4.1 Over the last two decades, both the public and private sectors have become increasingly reliant on IT systems for the performance of their core business functions. Although there are significant efficiencies generated through IT systems in areas such as data processing, data collection, and communications,[68] protection of the information contained in these IT systems has become increasingly difficult.[69]

4.2 Research undertaken in Australia and overseas shows that the growing use of new technology had significantly expanded the potential for fraud.[70] For example, a survey conducted by the United States Federal Bureau of Investigation into 600 organisations found financial crime committed in 1998–99 involving the use of information technology had doubled from the previous year to approximately US$266 million.[71] Likewise, a survey of 11 Australian Government agencies found that 36 per cent had reported misuse of their computer systems and 45 per cent reported external attacks through remote-access computer systems.[72]

4.3 In practice, the Australian Institute of Criminology (AIC) found that criminals were more frequently using computer-perpetrated fraud to misappropriate government property and funds. The AIC noted that Government agencies relying heavily on computer systems, and in particular e-commerce, will need to develop appropriate security measures to prevent the abuse of Government funds and property.[73]

---

68 For example, e-mail.

69 Factors that influence the security of information contained on IT systems include:
- rapid changes in technology;
- the increasing number of functions performed in an IT environment; and
- the complexity and size of IT networks.

70 Australian Financial Review, *Technology Helps Breed Fraud In Government Bodies*, p. 61, 11 May 2000.

71 The Arizona Republic, Business and Money, *Cybercrime Continues Swift Rise*, p. D1 27 March 2000.

72 Australian Financial Review loc. cit.

73 Australian Financial Review loc. cit.

4.4 The Office of Strategic Crime Assessments (Australia) also noted that, although the types of fraud perpetrated may not have changed, new technologies may encourage redistribution within the categories of fraud currently under investigation.[74] In particular, the use of computer technology:

> *…offered relative anonymity, made it easier to disguise the intent of your scheme, and the complexity of the network made the task of monitoring and detecting cyber-fraud extremely difficult.*[75]

4.5 Case study 2 illustrates the large-scale frauds that have been perpetrated through the misuse of IT facilities.

Case study 2

$1.4 million computer fraud against the Commonwealth

In June 1995 a contractor working for a Commonwealth agency was convicted of defrauding the Commonwealth of $1.4 million.

The contractor was to provide IT support for a major system in a Commonwealth agency. While performing his regular duties which involved the maintenance of the system's information technology, the contractor was able to access and alter system data. More particularly, he was able to change the status of rebate claims from 'paid' to 'unpaid' on this system, and transfer bogus rebate payments into his own account. The contractor was then able to delete the record of the illegal transaction and return the 'paid' status and dates to their original state.

The Commonwealth agency was not able to detect the fraud initially, as there were a number of programs kept on the system that enabled the direct change of system data without the production of an audit trail.

It was later found that the project leader of the application team responsible for the System did not know the specific system access rights his team needed (including the contractor) and how system security was supposed to be controlled.

---

[74] Canberra Times, *Our worst crime: Fraud to "explode with information revolution"*, p. 17 22 September 1999.

[75] Canberra Times loc. cit.

The ATO's information technology and security environment

4.6 The ATO is reliant on its IT systems for recording information and for supporting its revenue collection systems. Failure of crucial ATO IT systems would seriously disrupt ATO operations.

4.7 The ATO IT network, although complex, can be broadly categorised into two main areas:

1. ATO mainframe environment: This environment is used as a repository for all taxpayer information collected by the ATO and contains the software used to compile and control taxpayer information. ATO IT Services is responsible for controlling and maintaining the data contained on the ATO mainframe, as well as user access to mainframe data. A private sector contractor is responsible for providing and supplying administrative services and platforms for the ATO mainframe environment.
2. Wide Area Network (WAN) environment:[76] This environment comprises a number of linked local area networks (LANs)[77] and uses the Microsoft Windows NT operating system. A private sector contractor provides the administrative services and platform to support the WAN, including software and hardware.

4.8 A further explanation of the ATO IT network can be found in Appendix 5.

ATO IT Security Section

4.9 The responsibility for providing day-to-day advice, implementation and monitoring of IT security lies with the ATO's IT Security Section.[78] The principal functions of the IT Security Section are:

- IT security policy and awareness;
- LAN environment security;
- audit and assurance;
- access management; and
- mainframe access control.

---

[76] A wide area network is a collection of computers, terminals, printers and other computing devices that are connected over large distances (ie. metropolitan, intercity, national and international). The ATO WAN enables communication between ATO offices. It is also referred by ATO as the TAXLAN. Through it, the ATO accesses various mainframe programs and provides desktop applications to enable ATO officers to perform their duties.

[77] A local area network is a collection of computers, terminals, printers, and other computing devices that are connected through cable over relatively short distances (usually within a single building or office).

[78] The IT Security Section is part of the ATO's Information Technology Services Group.

4.10 The ATO IT Security Section controls the security of taxpayer and tax return data located on the ATO mainframe.[79] This involves primarily the administration and maintenance of user profiles,[80] and the monitoring of user access to the mainframe.[81] ATO IT security staff are also responsible for the administration of security issues relating to the WAN environment. As mentioned in paragraph 4.7, in July 1999, the ATO outsourced its administration of the WAN to a private sector contractor.[82]

4.11 Although a contactor may have taken over responsibility for the delivery of some IT services to the ATO, the ATO remains fully accountable for the delivery of an efficient and effective taxation system. The Commonwealth Attorney General's Department stated that it:

> *…believes that there is not and should not be any lessening of accountability for government services as a consequence of contracting out the provision of these services*.[83]

4.12 The ANAO considers that to ensure the effective delivery of IT services, the ATO needs to ensure that there is an adequate level of monitoring of the contractor activity to ensure compliance with contracts and to provide assurance that ATO IT systems are secure and taxpayer information is protected.

ATO mainframe environment controls

4.13 The ANAO examined the ATO's mainframe environment to determine whether controls were in place to minimise the occurrence of fraudulent activity relating to the security of taxpayer information. In particular, we focused on three main areas:

- the control of mainframe (taxpayer) information;
- access control: includes the security control in place to provide assurance that staff access to the mainframe environment is secure; and
- pro-active IT controls: projects or activities undertaken specifically to detect fraudulent activity. For example a review of logged information relating to access of a particular system.

---

[79] ATO IT security is also responsible for the ATO LAN gateway. The main function of the LAN gateway is to screen electronic incoming and outgoing material (eg. e-mail) before it enters or leaves the ATO LAN system.

[80] An ATO user profile is the list of systems and applications to which an ATO staff member has access. It is the principal mechanism used by the ATO to restrict access to ATO systems.

[81] The ANAO notes that an ATO contractor indirectly administers access to the mainframe in emergency situations through the use of *Firecall. Firecall* is discussed further in Appendix 5.

[82] A contractor is responsible for providing and maintaining WAN software and hardware. The contractor is also responsible for granting approved ATO access rights to users. The ATO IT Security section is responsible for setting, applying and enforcing ATO security policy.

[83] Senate Standing Orders, 1997, SO 26 (2).

Control of information contained on the ATO mainframe environment

4.14 The ATO IT security policy (June 1992) specifies the requirement for all taxpayer data to be kept on the ATO's secure mainframe environment where it is protected by the Resource Access Control Facility (RACF).[84] Failure to ensure that taxpayer data is kept on the mainframe environment (which is protected by RACF), could result in unauthorised access to sensitive taxpayer information.[85]

4.15 In its audit of Information Technology Security conducted in 1994–95,[86] the ANAO found that there were a number of instances where taxpayer data is stored outside the mainframe environment. This data was stored in bulk, on branch office and UNIX computers. The report recommend that: ATO review the circumstances where taxpayer data is stored away from the mainframe; and where it is determined that taxpayer data is allowed on the WAN, the ATO develop policy for the storage and internal checking of this data.[87]

4.16 Since 1994–95 the ANAO, through its Financial Statement Application Access Management Reports, has raised similar concerns about the security of taxpayer data located outside the ATO mainframe environment. During this audit, we noted that ATO staff continue to download taxpayer data from the ATO mainframe to a WAN environment that does not provide similar levels of security to the ATO mainframe.[88] This contravenes the ATO's existing security policy as well as increasing the risk of exposing taxpayer data to unauthorised access.

4.17 The ANAO recognises that there are various applications available in the WAN environment that allow ATO staff to efficiently analyse and process taxpayer data.[89] These applications are not available in the ATO mainframe environment. Since 1992 the ATO's reliance on WAN

---

84 RACF is the ATO facility used to control user access to the ATO mainframe environment. A further explanation of the RACF can be found in Appendix 5.

85 The ATO mainframe is protected by RACF which provides stringent access protection to mainframe data. The ANAO notes that the ATO does have mechanisms to prevent unauthorised access to the WAN. However, the WAN does not have a robust protection mechanism similar to RACF to restrict access to data by users. The ATO has determined that RACF provides the level of security required to ensure the security of taxapayer data.

86 ANAO Audit Report No. 6 1994-95 *Information Technology Security* Australian Taxation Office. Australian Government Publishing Service, November 1994.

87 Recommendation No. 13. ANAO Audit Report No. 6 1994-95 *Information Technology Security* Australian Taxation Office. Australian Government Publishing Service, November 1994.

88 The WAN environment uses the Windows NT operating system. The ANAO notes that the Windows NT operating system does not afford taxpayer data the same level of security as does the ATO mainframe environment.

89 For example Microsoft Excel, Access and Word.

applications has increased. However, the ATO has not updated its procedures, guidelines or policy to ensure the protection of data located on the WAN. The ANAO considers it is important that the ATO resolve the issues first raised by the ANAO in 1994–95 regarding the security of taxpayer data on the WAN environment.

4.18 The ATO acknowledges that its existing policies have not kept pace with initiatives to exploit the potential of new technology available. This technology allows ATO staff to efficiently analyse and process taxpayer data. The ATO has indicated that it intends to address this issue by:

- reviewing the ATO's security policy regarding the appropriate storage of bulk taxpayer data outside the mainframe environment;[90] and
- engaging a consultant to advise on the most appropriate way to risk manage access to data outside the mainframe environment. The advice will consider network usage in other agencies and the fact that LAN is the ATO's common work platform.

4.19 Since introducing its outsourcing arrangements in July 1999, the ATO could not provide evidence to confirm that the IT Security Section had monitored IT contractor activity to ensure compliance with taxpayer data security provisions of its IT outsourcing contracts. As a result, the ATO faces an increased risk of compromising the confidentiality and integrity of taxpayer data by not providing assurance on authorised contractor staff access to taxpayer data.

4.20 The ATO advised that its IT Security Section has purchased a suite of audit logging, gathering/analysis software products[91] that will enable the pro-active monitoring of audit logs for the WAN environment.

Recommendation No.6

4.21 The ANAO recommends that the ATO:

- develop standards and guidelines for inclusion in the ATO Security Policy which address the risks of storing bulk taxpayer data outside the mainframe control environment; and
- introduce a program of internal checking to ensure adherence to these standards.

ATO Response

Agree.

---

[90] The ATO advised that its IT Security Policy will be re-revised in accordance with the Commonwealth Protective Security Manual.

[91] The ATO uses these products for its Firewalls. It plans to extend the use of these products to TAXLAN (WAN) in the near future.

IT access control

4.22 As noted in Chapter 1, since 1994–95, unauthorised access to taxpayer data by ATO staff remains the most common type of fraud perpetrated in the ATO and therefore consumes the highest amount of fraud investigation resources. Figure 3 (Chapter 1) illustrates the high number of alleged unauthorised information access cases received by the FP&C Section in 1999–2000 compared with other allegation types. In 1999–2000 there were 106 unauthorised information access cases reported to the FP&C Section. Most of these cases of unauthorised information access relate to accessing taxpayer data on ATO's mainframe applications.

4.23 The implication of inappropriate access to ATO mainframe applications is serious. It could potentially result in unauthorised changes being made to taxpayer data, including the processing of fraudulent transactions. The ANAO recognises that the majority of unauthorised access by staff to taxpayer data does not involve a 'dollar value' and may result from 'curiosity' by ATO staff. However we also note the legislative responsibility the ATO has regarding the security and privacy of taxpayer information, and the potential penalties for breaching this legislation. Appendix 6 provides the relevant extracts of the *Income Tax Assessment Act 1936* and ATO internal policy regarding the improper use of ATO IT facilities.

ATO information technology access management practices

4.24 Although the ATO IT Security Section is ultimately responsible for the control of the ATO mainframe security environment, the certification of user access to the mainframe environment has been devolved to ATO Business Line management. That is, Business Line managers are responsible for certifying that ATO staff require certain IT access rights because of the positions they hold. The factors that Business Line managers should consider prior to granting mainframe access include:

- access is in accordance with approved user profiles;
- user profiles are current and reflect those privileges commensurate with user duties;
- valid access is only granted to authorised staff;
- user access is removed when a user is no longer required to perform a specific job or function; and
- approvals are adequately documented (ie. they have a clear audit trail).

4.25 The documentation that Business Line management uses to provide assurance that accesses are genuine is the ATO IT access matrix.[92] The primary function of the matrix is to review and certify that staff IT access is commensurate with their employment positions and work responsibilities.[93] Under ATO IT security policy, access matrices should be completed every three months, or whenever staff require changes to their access status by Workplace Access Administrators (WAAs).[94]

4.26 Once complete, access matrices are reviewed by the ATO's Access Management Team (AMT),[95] who also have the responsibility of implementing changes to staff access specified in the access matrices. Specifically, this entails:

- adding new users to the mainframe environment;
- changing access rights to reflect the promotion of staff and staff temporarily performing higher duties; and
- the deletion of staff access rights when they leave work areas.

4.27 Through an efficiency audit in 1994–95[96] and a series of Application Access Management Reports, the ANAO has analysed the ATO mainframe and WAN environments over a number of years. The findings outlined in these reports relating to access control involved:

- management of the IT access Matrix;
- WAA and AMT access to the ATO IT mainframe environment; and
- management of *Firecall* access.

4.28 These are discussed below.

---

92 The ATO IT access matrix defines user (staff) employment positions and access privileges under Resource Access Control Facility (RACF).

93 The access rights, as specified in the access matrices, relate solely to the ATO mainframe system (not the LAN).

94 WAA's control the access of users to ATO IT mainframe Systems. Each WAA is responsible for access control for a discrete ATO work group. For example the ATO's Penrith Branch Office has work groups from the Small Business and Individuals Non-Business Business Lines and hence several WAAs to manage access control for those groups.

95 The AMT is a group within the ATO IT Security Section consisting of five people who are responsible for the coordination, training and support of the WAAs. The AMT has been provided with an access level known as *System Special Access* that allows access to all mainframe systems. The Access Management Team also reviews and determines the special access privileges of the WAAs.

96 ANAO Audit Report No. 6 1994-95 *Information Technology Security* Australian Taxation Office.

Management of the ATO IT access matrix

4.29 Since 1994–95, ANAO has identified weaknesses in the ATO's IT access matrix process. These weaknesses related to the:

- inconsistent matrix approval practices by Business Line management;
- non-retention of previous matrix documentation;
- matrices not being maintained to ensure compliance with business system control objectives; and
- matrix information not detailed enough to provide assurance that users have correct levels of access.

4.30 The fieldwork undertaken as part of this audit supports these findings. Although management and staff interviewed found the current matrix system to be an effective control in preventing unauthorised access to IT systems, ATO management practices regarding the timeliness and completeness of the matrices varied markedly between ATO teams. For instance, some ATO team managers completed their matrices on a monthly basis, others on a three monthly basis (as required under ATO policy), and a number of team managers completed them less frequently.

4.31 The ATO has advised that during the audit, considerable work has been done to ensure that access matrices are checked by the AMT on a three monthly basis. The ATO stated that this has resulted in estimated compliance of around 90 per cent for the period ended June 2000.

4.32 The ANAO considers that the application of a consistent approach to the documenting and timely reporting of access matrices is essential for ensuring consistent access approval practices. A better practice approach to ensure access approval consistency is to automate the approval process by connecting staff employment positions to access privileges. This could be achieved by linking the ATO's Human Resource Management System (HRMS) to access privileges.

4.33 The ANAO notes that the ATO is investigating the use of its HRMS to manage staff IT system access privileges. The ATO advised the ANAO that the use of the HRMS for this purpose will be subject to financial considerations.

Workplace Access Administrators and the Access Management Team

4.34 As noted in paragraphs 4.25 and 4.26, WAAs and the AMT manage access to the ATO's mainframe environment. This requires that the AMT and WAAs have special access functions that allow them to manage access to the ATO mainframe environment. For example AMT staff have access privileges that allow them to add new users, delete existing users and

change the existing users' access privileges to the ATO mainframe. Likewise, WAAs have access privileges that allows them to grant user access to particular 'IT groups', and reset office passwords. These privileges are contained within the security category known as *Group Special*. *Group Special*[97] not only allows the AMT and WAAs to grant user access to aspects of the ATO mainframe environment, but also provides them with a full range of access privileges to specified databases (or groups) within the mainframe environment.[98]

4.35 Given the range of access privileges available to users with *Group Special* access it is essential that *Group Special* access is only granted to those ATO staff that need it.

4.36 In 1998–1999, the ATO had approximately 1200 WAAs with *Group Special* access. This means that one in 14 ATO staff could grant access to other ATO employees. In 1999–2000 there were 975 WAAs with *Group Special* access, meaning that one in 18 staff can grant access to other ATO employees. This decrease in the number of WAAs shows that the ATO is seeking to rationalise the number of staff with *Group Special* access. Rationalisation of *Group Special* access is being achieved through centralising access management administration in the ATO's National Office.

4.37 Although the AMT provides WAAs with access to *Group Special* and are required to monitor its use to ensure that the privilege is used correctly, the ANAO has noted that the monitoring of WAAs by the AMT was not occurring in most of the cases reviewed by the ANAO. It was observed that there were a number of instances where WAAs were not properly trained, were not aware of their responsibilities, and were given inadequate administrative support.[99]

4.38 Given the high proportion of ATO WAAs with *Group Special* access, the ATO requires a structured system to monitor their access, and ensure that it is only used for the purpose for which it was intended.

---

97 *Group Special* access only extends to all access privileges associated with a particular group or database within the mainframe. Access to all privileges contained within RACF is outlined under System Special access.

98 For example, a user within the ATO Integrated System group, with *Group Special* access could have the ability to approve, provide refunds, reconcile income tax returns.

99 The ANAO notes that during the Audit, the ATO has instituted a half day training program for all new WAA's.

4.39 The ATO has advised that it is continuing the work to further review and, where possible, reduce the number of WAAs and also plans to review the WAA access rights and activity at a rate of 10 per cent per month starting from November 2000.[100]

4.40 The ANAO found also, that the ATO does not have formal procedures in place to monitor the activities of the AMT. Although there are fewer staff in the AMT (five as at July 2000) than WAAs, the access powers of the AMT are significantly greater (see paragraph 4.34).

4.41 The ANAO considers that the ATO should develop a comprehensive access management system to monitor WAA and the AMT special mainframe environment accesses to ensure these privileges are used correctly.

Firecall

4.42 To facilitate the smooth operation of ATO IT systems it is necessary at times for ATO IT systems staff to make direct changes to the ATO's mainframe and WAN environments to correct system errors. To enable staff to perform these 'quick fixes' and to gain the necessary direct access to production data in the mainframe environment, the ATO has a special access authority known as *Firecall* to bypass regular RACF controls (see Appendix 5).

4.43 ATO staff requiring *Firecall* access need to obtain management and/or user approval, as it bypasses all normal system change procedures and access controls. For this reason, the ANAO considers that its use should be kept to a minimum and each use of the *Firecall* facility should be carefully reviewed.

4.44 The ANAO first raised concerns about the use of *Firecall* in its performance audit of Information Technology Security in 1994–95, which noted that many ATO staff were not only using *Firecall* for emergency situations, but also to perform their normal daily work.

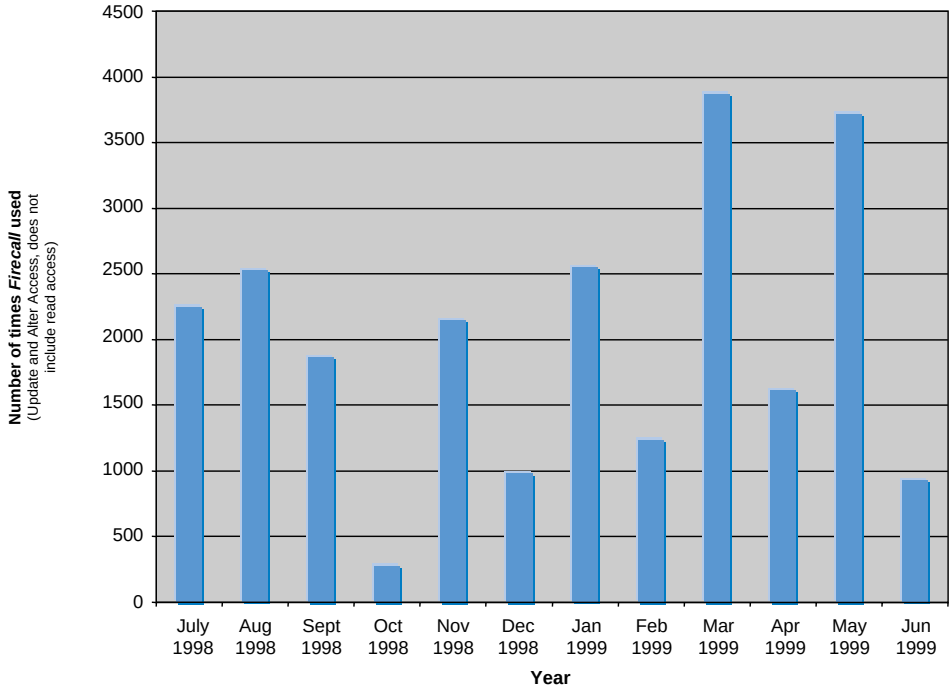
---

[100] From November 2000, on a weekly basis, the ATO plans to deactivate accounts not used for three months and suspend those not used for 30 days.

4.45 As part of its ATO Applications Access Management Report 1998–99, the ANAO found that *Firecall* continued to be used excessively. Analysis contained in this report shows that *Firecall* is being used so frequently that effective independent review by the ATO IT Security Section is administratively unachievable. Figure 9 illustrates the high usage of *Firecall* between 1 July 1998–30 June 1999.[101]

Figure 9

ATO *Firecall* usage between July 1998 and June 1999.



Source: ATO Data

4.46 During this audit we conducted further analysis of ATO *Firecall* use between August 1999 and August 2000. The following figure illustrates *Firecall* usage for this period. This figure includes *Firecall* Read as well as Alter and Update access statistics. Read access statistics are also relevant because a *Firecall* user may perpetrate a fraud by unlawfully accessing mainframe data using *Firecall*'s Read Access capability.

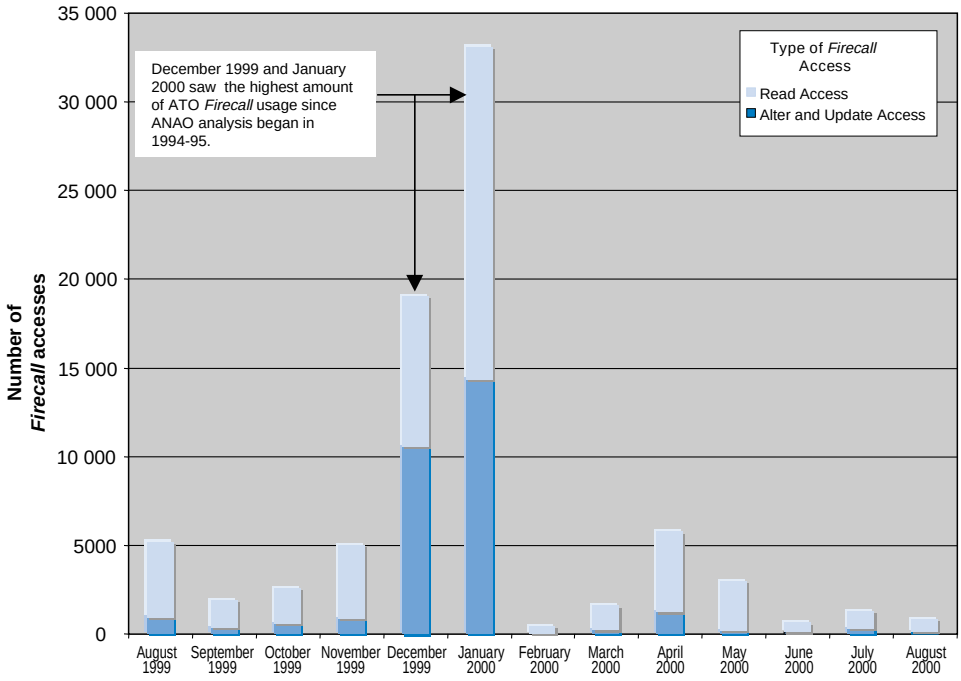
---

[101] The ATO has three groups of *Firecall* Access. These are:
- Alter: allows the user of *Firecall* to read, update and delete data from the ATO mainframe;
- Update: allows the user of *Firecall* to read and update mainframe data;
- Read: allows the user of *Firecall* to read mainframe data.

The ANAO was only able to obtain Alter and Update *Firecall* statistics for 1998-99. However, *Firecall* Read access statistics are also relevant, as a *Firecall* user may also perpetrate a fraud by unlawfully accessing mainframe data using Firecall's Read Access capability.

Figure 10

ATO *Firecall* usage between August 1999 and August 2000.



Source: ATO Data

* The ATO was unable to provide the ANAO with complete Firecall statistics for February 2000 (only one week of data provided) and June 2000 (only three weeks provided).

4.47 A comparison between *Firecall* Alter and Update usage in 1998–99, and usage between August 1999–August 2000 indicates usage increased, particularly in December 1999 and January 2000. When combined, the *Firecall* Alter and Update usage in these two months (24 911) was greater than the total *Firecall* Alter and Update usage in 1998–99 (23 966). The ANAO notes that since January 2000, the ATO has implemented a strategy to decrease the use of *Firecall*.[102] However, *Firecall* use needs to be reduced further for the ATO to undertake effective monitoring of all *Firecall* accesses.

[102] Note that *Firecall* statistics for February 2000 (only one week of data provided) and June 2000 (only three weeks provided) are not complete.

4.48 The ATO stated that the dramatic increase in *Firecall* usage in December 1999 and January 2000 was due to significant changes made to ATO IT systems as part of its tax reform program and these changes required the use of *Firecall*. However, the ATO has acknowledged that inappropriate use of the *Firecall* facility has also been a contributing factor.

4.49 The ANAO is concerned that *Firecall* is being used as an alternative access method to enter ATO IT systems. If staff require the level of access provided by *Firecall* to undertake their daily duties, then their RACF access profiles should be changed to reflect these requirements.

4.50 Given the ANAO's concerns expressed in previous reports since 1994–95, we consider that the ATO should have established more effective policy and controls for the provision of the *Firecall* facility. The ANAO noted also with some concern the increasing use of *Firecall* by ATO IT contractor staff. Contractors undergo similar security checks to those undertaken by ATO staff and under the contract only have access to taxpayer data for the purpose of supplying services to the ATO as specified in the contract.[103]

4.51 However, in January 2000 alone, contractor staff used *Firecall* Update and Alter access 14 228 times. The use of *Firecall* by contractor staff poses a significant risk to the security of taxpayer data as the majority of these accesses were not reviewed by the ATO's IT Security Section. The ANAO considers that *Firecall* use by contractor staff should be carefully controlled and scrutinised by the ATO's IT Security Section, with regular reports provided to management outlining the nature and reasons for *Firecall* use.

4.52 The ATO advised that it is in the process of introducing systems changes and revising its policies to restrict the use of *Firecall*. The ANAO also notes that the ATO has recently developed a draft *Firecall Usage Policy*. It is too early to say whether these developments address all of ANAO's concerns. The ATO should closely monitor these changes to ensure they remove or effectively manage the risks identified by the ANAO.

---

[103] Services Agreement for IT&T Services and Industry Development between the Australian Taxation Office and the Contractor, 31 March 1999.

Recommendation No.7

4.53 The ANAO recommends that, to achieve the required level of security and to promote consistency in access approval processes, the ATO:

- investigate the cost effectiveness of automating the access approval process by linking mainframe access privileges to the ATO's Human Resources Management System;
- implement consistent accountability controls for all Workplace Access Administrators and the Access Management Team so that special access privileges are used correctly; and
- ensure the legitimate use of *Firecall*, by monitoring and analysing all accesses using *Firecall*, and finalise its detailed security policy outlining the guidelines for controlling *Firecall* access.

ATO Response

Agree.

Pro-active IT controls—logging access of staff to ATO IT systems

4.54 Logging details of the access made by ATO staff to IT systems is an important mechanism to ensure the security of ATO taxpayer and other data.[104] Comprehensive logging of IT systems provides an audit trail to identify perpetrators of IT fraud as well as contributing to maintaining community confidence in the ATO and its staff. It also provides staff with the confidence that the ATO is in a position to defend them should they become a victim of an unjustified allegation of unauthorised accessing.[105]

4.55 As part of its RACF mechanism the ATO has implemented a comprehensive logging system that records all 'normal' accesses by staff to the ATO mainframe and WAN environment.[106] The responsibility for the maintenance and review of the IT logging system is the IT Security Section's Audit and Assurance area.

---

[104] IT system logging refers to the process of recording staff user details each time a system is accessed.

[105] ATO has advised that the audit trail system exonerates approximately 70 per cent or more of allegations reported to FP&C Section relating to unauthorised access.

[106] This logging system does not record the use of *Firecall*, which is logged under a separate system.

4.56 There are thousands of daily accesses to the various IT systems within the ATO mainframe environment and WAN. This makes continuous monitoring of all IT logs impractical.[107] However, the ANAO considers that there is scope for risk-assessed targeting of IT logs to detect potential fraud.

4.57 The ANAO noted that the ATO does not utilise a systematic approach to targeted analysis of access logs on a regular basis. Analysis is, however, undertaken by the IT security area when there is a specific purpose, such as an ATO internal audit or fraud investigation. As noted earlier, the most common type of fraud perpetrated in the ATO is unauthorised access to information. Consequently, the IT security area undertakes a considerable amount of work on behalf of the FP&C Section in collating IT logs of staff suspected of unlawfully accessing taxpayer information.

4.58 In 1995, the FP&C Section, in conjunction with the IT Security Section undertook a one-off project to identify unauthorised access to celebrity taxpayer records by ATO staff.[108] The project results showed that between 1 January 1994 and 12 February 1995, 128 ATO staff had accessed one or more of the selected high profile taxpayers records. Of the 128 tax officers, 86 had questionable explanations as to why they had accessed the selected tax records. The investigation resulted in:

- 15 ATO employee cases being referred to the DPP for further action;[109] and
- 71 cases were referred to Business Line Management for consideration of disciplinary action.

4.59 Using the same methodology, a supplementary project was completed by the FP&C Section in 1996–97, but with a different selection of high-profile taxpayers. Figure 11 illustrates information accesses between 1 July 1999 and 30 June 2000. This figure shows these projects' likely contribution to the reduction of unauthorised access to taxpayer data by ATO staff.

---

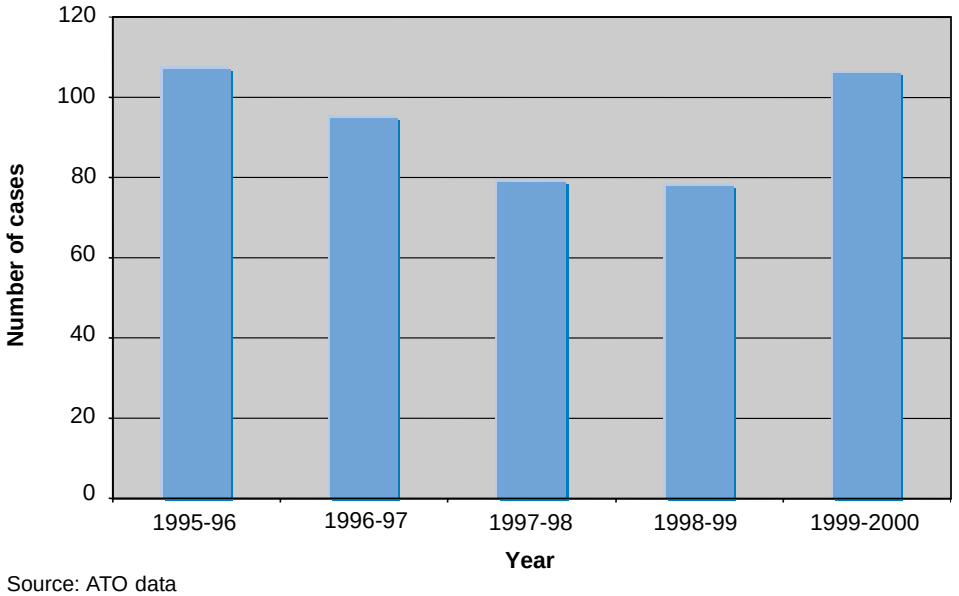
[107] The ANAO notes that certain taxpayer records are closely monitored by the IT Security Section. Any attempt by an ATO officer to access these records without a legitimate reason will alert IT security staff. These alerts are always acted upon.

[108] This project involved the IT Security Section selecting access logs for a range of high profile taxpayers, to determine the legitimacy of ATO staff accesses to these records.

[109] Of these staff, 10 employees were convicted with a penalty, three employees had charges proven without a penalty, and two employees received a caution from the DPP.

Figure 11

Number of unauthorised accesses to taxpayer data reported by ATO staff between 1 July 1995–30 June 2000.[110]



Source: ATO data

4.60 Following the initial project undertaken in 1994–95, the analysis of FP&C Section data showed a high level of unauthorised access to taxpayer data by ATO staff. However, as staff awareness of the special project grew, the number of unauthorised information accesses reported to the FP&C Section in 1996–97 decreased. The results of the 1996–97 follow-up project reinforce the deterrent impact of the earlier project, with results showing that 31 tax officers had unlawfully accessed the targeted high-profile taxpayer records. However, the ANAO notes the significant increase in the number of unauthorised information accesses for 1999–2000. We consider that this is due in part to unauthorised access projects (similar to those outlined above) not being undertaken for three years. We note that the unauthorised information access figures may be affected by the use of *Firecall* to gain unauthorised access to taxpayer information. The advantage of ATO resuming these unauthorised access information projects is that it could also detect whether *Firecall* was used to gain unauthorised access to taxpayer information.

[110] Note: These figures do not include the cases detected as a result of the one-off projects.

4.61 The ATO attributes the increase in reported cases in 1999–2000 to its fraud and ethics awareness program and raising the profile of the FP&C Section, and not to the lack of conducting these projects. However, the ANAO notes that soon after these projects were undertaken, the FP&C Section acknowledged, in its briefings to the ATO Executive, the value in a joint approach (by combining awareness raising with visible enforcement through unauthorised access investigations projects) to achieve a shift in the corporate culture.

4.62 The ANAO considers that the ATO should examine the potential benefits of further targeted analysis of ATO IT system logs in the future as it provides two benefits. Firstly, it is likely to prove an efficient mechanism to detect the numbers of staff who illegally access taxpayer information. Secondly, if well publicised, it can be used as a strong deterrent to ATO staff considering illegal access to taxpayer records.

4.63 The ATO acknowledges the benefits of pro-active fraud investigations and stated that it is proposing to undertake similar projects as a result of the ANAO's observations. The ATO advised that a process for the acquisition of an automated product that will enable pro-active and efficient review of security logs is underway. If approved and funded, the product will be available by the end of 2000.

Recommendation No.8

4.64 The ANAO recommends that to minimise exposure to fraudulent activity, the ATO IT Security Section and, where necessary the Fraud Prevention and Control Section, undertake regular targeted reviews of ATO IT system logs to detect and deter unauthorised access to taxpayer data.

ATO Response

Agree.

Conclusion

4.65 The ATO is reliant on the efficient and effective operation of its IT systems. Failure of ATO systems would seriously disrupt the delivery of ATO services including the collection of taxation revenue. Since 1994–95 the ANAO has assessed the effectiveness of many of the ATO's IT system controls. We found that there were significant risks associated with ensuring the security of the ATO IT systems. These risks relate primarily to the granting and monitoring of access to the ATO IT systems and the storage of taxpayer data on the ATO WAN.

4.66 During this audit, we found that not only do these risks remain, but the risk factors have increased due to the outsourcing of many IT system functions. This is because the ATO contractor staff have had limited exposure to ATO fraud prevention education and awareness material and programs compared to ATO employees. In addition, the ATO could not provide evidence that the IT Security Section had monitored outsourced contractors' activity to ensure compliance with taxpayer data security provisions of its IT outsourcing contracts. ATO statistics also show that a high number of fraud allegations relate to the unauthorised access of taxpayer information by ATO staff.

4.67 The ANAO considers that it is imperative that these risks associated with access to ATO systems be addressed to ensure the integrity of the ATO's IT systems and the confidentiality of taxpayer data. The ANAO considers that the ATO should assess the feasibility of increasing the number of pro-active fraud detection reviews, which includes regular analysis of access logs, as an effective means of ensuring security and detecting fraud.

5. Fraud Detection

This Chapter discusses ATO's internal fraud detection strategy. It examines ATO's use of computer-based detection techniques and pro-active projects in preventing and detecting fraud. We also examine the coordination between the ATO's Fraud Prevention and Control Section and Internal Audit in detecting fraud.

Introduction

5.1 Fraud detection is a key element of an agency's overall fraud control strategy. It provides staff and external stakeholders with tangible assurance that an agency's assets are protected, and perpetrators of fraudulent activity are identified and prosecuted. Fraud research shows that not only is the amount of fraud increasing, the means of perpetrating fraud is shifting towards electronic or computer assisted fraud. To be fully effective, an agency's fraud detection methodology must now constantly evolve to keep pace with new fraud types and new technologies used to perpetrate these frauds.

5.2 In addition to an evolving fraud detection methodology, there are a number of key elements that underpin effective fraud detection strategy. These include:

- the development of an effective fraud prevention program. Detection is invariably linked to prevention, as staff awareness and the robustness of quality assurance processes also contribute to the effective detection of fraudulent activity;
- the existence of effective internal controls to detect fraud;
- undertaking pro-active investigations. For example, initiating investigations based on risk profiles developed through the fraud risk assessment process; and
- cooperative implementation of agency fraud detection policy.

5.3 To determine the effectiveness of the ATO's fraud detection strategy, and the implementation of these key elements, the ANAO examined the following areas:

- ATO's pro-active detection activities; and
- the relationship between the ATO's Internal Audit and FP&C Sections.

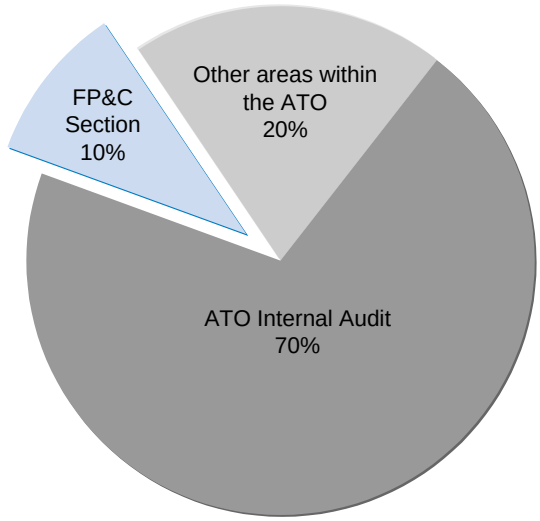
ATO pro-active fraud detection activities

5.4 The use of sophisticated computer software to analyse and collect large amounts of data in an IT environment offers a new and efficient tool to detect indicators of fraudulent IT activity. Through the use of computer-assisted audit techniques (CAATS) and sophisticated data-mining software, fraud investigators are able to analyse, compare and compile data over numerous large databases and build profiles of likely fraudulent activity within an organisation.

5.5 In late 1997, the ATO's Internal Assurance Branch (IAB) recognised the potential application of CAATS and data-mining software to its internal audit program and formed the ATO's IAB Analytical Support Section. This Section acts as a support facility, primarily for the ATO's IAB, however, it does provide specialist data-mining and extraction capability for FP&C Section as well as a number of other areas throughout the ATO. The following figure shows the workload referred to the Analytical Support Section by its principal clients.

Figure 12

Percentage of client use of the Analytical Support Section



Source: Analytical Support Section, ATO

5.6 In its 1997–98 accountability report the FP&C Section indicated that it was making some use of the Analytical Support Section's CAATS capability to identify suspected fraud against the ATO. However, the FP&C Section acknowledges that it has made only limited use of this capability and that it has devoted greater resources to other areas of its operations such as its prevention and education strategies and its important investigation function.

5.7 The FP&C Section uses the Analytical Support Section on a monthly basis to conduct the following detection queries on the ATO IT system using data mining technology:

- aircraft flight confirmation: the Analytical Support Section downloads a list of ATO staff carried by its service providers. This list is then matched against ATO records of reservations made by ATO staff to determine whether they actually boarded these flights;
- credit card checks: the Analytical Support Section downloads all ATO Corporate credit card records and cross-matches these to ATO records to determine whether ATO credit cards are being used for their intended purpose; and
- use of non-corporate/non-preferred carrier flights: the Analytical Support Section cross-matches applicable flight information to ATO records to determine whether staff are using the ATO's non-preferred travel service provider over their preferred service provider who provides the ATO with a greater corporate discount.

5.8 The use of CAATS and data-mining software for detecting the likelihood of fraud in the above areas has proven to be an efficient, effective and economical method of detecting fraud within the ATO. That is, once detection queries have been developed, very few resources are required to run these queries in subsequent months. This means that the FP&C Section is able to identify fraudulent activity in these areas in a timely, efficient and effective manner.

5.9 The ANAO considers that FP&C has not fully utilised the services of the Analytical Support Section.[111] The ANAO considers that there is potential for further use of the Analytical Support Section in detecting the likelihood of fraud. By making greater use of these services, the FP&C Section could detect indicators of fraudulent activity in a timely manner with little additional resource cost.

[111] This is illustrated in Figure 12.

5.10 The ATO stated that they must determine an optimal balance between conducting pro-active investigations,[112] and responding to fraud allegations made by staff and fraud prevention training.[113] The ATO also noted that major fraud investigations, that may require a number of investigators, draw resources away from pro-active investigations. The ANAO considers that there is benefit in conducting pro-active fraud detection even if ATO resources do not allow the investigation of all identified cases. As part of FP&C Section's risk-based approach, all cases identified in such projects would be considered for further investigation, after taking account of the Section's other work priorities.

Coordination between the Fraud Prevention and Control Section and ATO Internal Audit

5.11 The Commonwealth Fraud Control Policy outlines that internal audit is closely linked to fraud control and that many of the activities undertaken by internal audit may expose fraudulent activity. The Guide stipulates further, that all Commonwealth agencies should ensure that the linkage is maintained. Statistics contained in the *1999 KPMG Fraud Survey*, [114] emphasises the importance of link between internal audit and fraud control. Results showed that in the agencies surveyed, 48 per cent of frauds were detected by internal controls and that 23 per cent were detected by internal audit review. Similarly, the 1998 Ernst & Young fraud survey[115] found that normal internal controls and internal audit were the most effective ways of preventing and detecting fraud.

5.12 The ANAO notes also that the International Federation of Accountants (IFAC) are seeking to tighten the International Standard of Auditing (ISA) 240 on fraud and error. Although the existing standard provides guidance to auditors as to how to treat fraud and error when they detect it, the revised standard will require auditors, and more importantly, management of agencies, to take a more pro-active role in both fraud prevention and detection.

---

[112] These are investigations initiated as a result of using data generated from pro-active computer-based detection activities.

[113] In Chapter 3, the ANAO noted that better practice indicates that the establishment of a sound ethical and fraud prevention environment is a key component in fraud control in the ATO. We found that, at the time of the audit, it takes precedence over pro-active fraud detection projects. However the balance between pro-active and re-active fraud detection projects may change in the future depending on assessed risk priorities.

[114] KPMG: Forensic Accounting, *1999 Fraud Survey.*

[115] Ernst & Young *Fraud the Unmanaged Risk – An international survey of the effect of fraud on business.*

5.13 Under the current ATO structure, FP&C Section and Internal Audit are part of the ATO's IAB. IAB Executive (including Directors of Internal Audit and FP&C Section) meetings are held on a regular basis to ensure open lines of communication exist between the two Sections and that there is regular exchange of relevant information.

5.14 Discussions with staff from Internal Audit and the FP&C Section, identified some weaknesses in the relationship between the two areas, particularly with regard to exchange of information. The Sections advised that they are currently working on improving this relationship.

5.15 During the audit, the ANAO was advised that, since 1999, Internal Audit has involved FP&C Section in their annual planning conference. This provides FP&C Section with an opportunity to comment on the Strategic Internal Audit Plan. It also increases internal audit staff awareness to the possibilities of detecting fraud through internal reviews.

5.16 However, Internal Audit has had little direct input into the ATO fraud control planning process or the Fraud Control Plan. Internal Audit considers there would be value in ensuring that a link exists between the two plans. This is particularly important since the Strategic Internal Audit Plan is based on a control self-risk assessment process, which needs to take account of the controls identified in the Fraud Control Plan.

5.17 The ANAO acknowledges the recent initiatives of the Internal Audit and FP&C Sections to coordinate their activities on fraud related issues. However, scope remains to improve communication between the two sections. As noted in paragraph 5.11, better practice dictates that a strong link be maintained.

5.18 The ANAO considers that Internal Audit and FP&C Section could use IAB Executive meetings to discuss fraud control issues and to coordinate fraud control activities, such as training programs and investigations. This forum could also be used to discuss findings emerging from fraud investigations, which indicate a potential breakdown in internal controls. Internal audit could use this information in the future development of their audit program.

Recommendation No.9

5.19 The ANAO recommends that, to improve the efficiency and effectiveness of its internal fraud detection strategy, the:

- Fraud Prevention Control Section make further use of the Analytical Support Section to identify potential fraud-related cases and assess the further investigation of these cases against other work priorities; and
- ATO strengthen the coordination between the Internal Audit Section and the Fraud Prevention Control Section to improve the development of fraud risk mitigation strategies.

ATO Response

Agree.

Conclusion

5.20 Computer Assisted Audit Techniques and data-mining software are effective and cost effective tools when fully utilised to detect indicators of fraud. The FP&C Section tasks the ATO's Analytical Support Section, to use these tools to detect likely fraudulent activity. However, the ANAO found that there is greater scope for the FP&C Section to use the services of the Analytical Section to detect indicators of systemic and large scale internal fraud.

5.21 The ANAO considers that, in accordance with Government policy, there should be a strong and cooperative relationship between the FP&C Section and ATO Internal Audit. Procedures for the sharing and dissemination of information between these two groups are important in ensuring effective ATO fraud detection systems.

6. Fraud Investigation

This chapter examines ATO's arrangements in relation to internal fraud investigations. The ANAO comments on ATO's investigation guidelines and procedures, processes for reporting and recording alleged instances of fraud and the operation of the internal investigations area.

Introduction

6.1 The Government recognises that an effective fraud control strategy requires a balance between the aims of prevention and the necessity for dealing effectively with cases which arise.[116] A significant issue regarding the conduct of sound investigations is an agency's ability to investigate subject matter in a timely and effective manner, to ensure confidence in its internal mechanisms are maintained. This is linked invariably to factors such as: resourcing; existence of investigation policies and procedures; compliance with existing policies and procedures; use of management information systems to record and monitor the investigations; and staff knowledge and training.

6.2 The capability of an investigation area is also an indication of the level of support it receives from within the organisation in areas identified above.

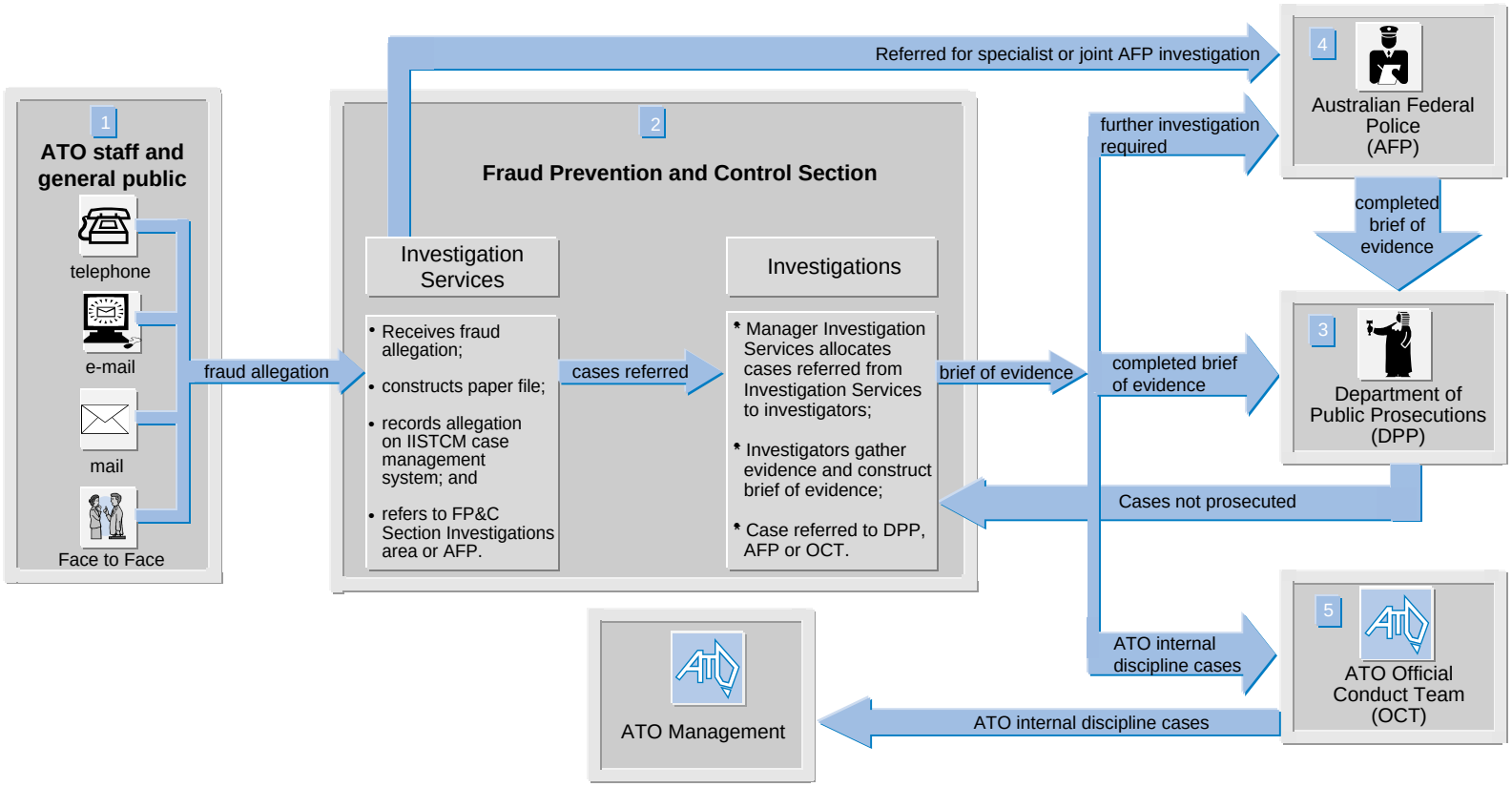
6.3 Prior to 1995, the Fraud Prevention and Control Section was concerned mainly with fraud investigations. However, in 1995 its role was expanded significantly with the introduction of fraud control planning, awareness and intelligence functions. The staffing levels in ATO's internal fraud investigations area have remained constant (between 12 to 15 staff) since 1995.

6.4 As mentioned in Chapter 2, the Investigations Unit is primarily staffed by ex-AFP staff who are experienced in criminal investigations. Figure 13 illustrates ATO's internal fraud investigation process.

---

[116] The Commonwealth Fraud Control Policy, para 53, p 9.

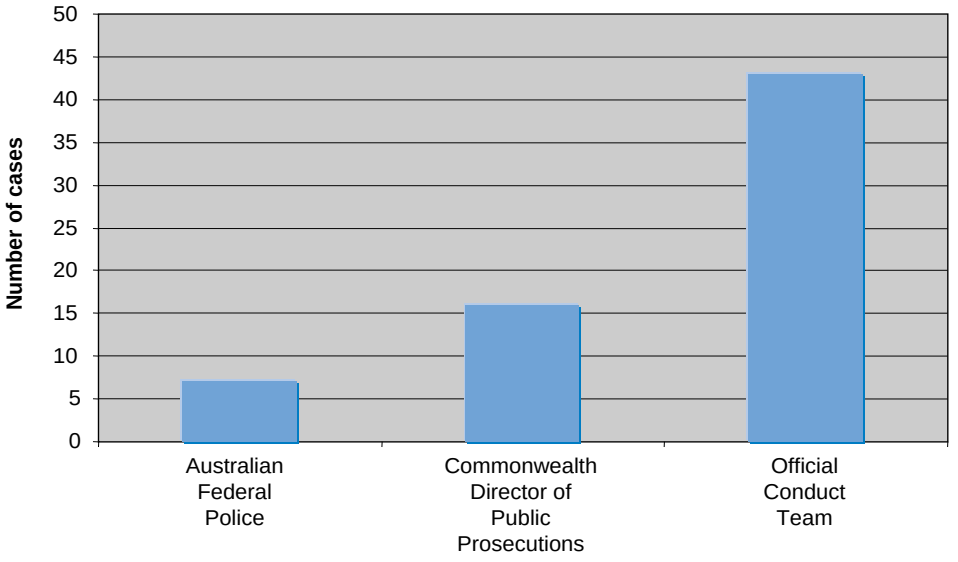
Figure 13
Fraud Prevention and Control Section's investigation process



6.5 If a complaint 1 were to be made regarding impropriety of an ATO staff member, it would be referred usually to the FP&C Section 2 who would then assess the complaint and, if necessary, investigate it. The outcome of an investigation could result in: no offence being proven; referral to the DPP 3 for prosecution; referral to the AFP 4 (if law enforcement powers or specialist investigation skills are required); or if it were a breach of the code of conduct not involving criminal behavior, referral to the OCT 5 who would consider the process under Public Service Act provisions relating to internal discipline. Complicated or sensitive cases would be referred directly to the AFP 4 for investigation. Figure 14 illustrates the number of internal fraud cases referred to the AFP, DPP and the OCT in 1999–2000.[117]

Figure 14

Number of cases referred to the Australian Federal Police, the Commonwealth Director of Public Prosecutions and the ATO Official Conduct Team for 1999–2000



Source: ATO Data

[117] Appendix 8 provides a more detailed breakdown of all Fraud Prevention and Control Section case results for 1999-2000.

Fraud investigations guidelines

6.6 The ATO has developed a statement of fraud investigation standards that outlines ATO's fraud investigations policy and procedures. This statement was reviewed and updated in February 1999. The *Statement of Investigation Standards* (the Investigation Guidelines) covers key aspects of the investigation process.[118] The Investigation Guidelines also cover issues relating to a breakdown of internal control, outlining the need for a review of each completed investigation to establish control and management issues that require program managers' attention.

6.7 The Investigation Guidelines contain appropriate links to several other documents such as the ATO Guidelines on *Reporting Matters for Internal Investigation*, *the Commonwealth Fraud Control Policy*, *the Prosecution Policy of the Commonwealth*, *the ATO Staff Protection and Reporting Policy* and the *Commonwealth Fraud Investigation Model Procedures*[119].

6.8 The Investigation Guidelines are also available on a CD-ROM initially produced by the ATO in 1998 and updated in June 2000. Each investigator has a copy of the CD, which can be accessed when undertaking field work. The ANAO regards this as better practice because it eliminates the need to transfer bulky documents and provides ready access to all reference material when travelling away from the office.

Reporting and recording allegations

6.9 The *Guidelines on Reporting Matters for Internal Investigation* (Reporting Guidelines) provides guidance on how to report matters to FP&C Section. These were first developed in 1990 and were recently reviewed and updated. The Guidelines are detailed and provide guidance on a number of fraud and misconduct related matters.[120] Several alternative means of contact are suggested in the Reporting Guidelines, such as by telephone, normal mail, *ATO Concern*[121] or anonymously on the ATO's Fraud Hotline number. The Reporting Guidelines also provide guidance in circumstances where the matter is reported to the staff's manager in the first instance.

---

[118] The Investigation Guidelines include ATO investigation principles; procedures for dealing with allegations of fraud; operational practices for investigations; steps for preparing investigation briefs of evidence and information on investigation management methodology and support.

[119] Best practice investigation procedures developed under the direction of the Attorney-General's Department by the Commonwealth Technical Standards Committee, in consultation with Commonwealth departments and agencies.

[120] For example: when should the suspicion of 'dishonest and unlawful conduct' be reported; who should the suspicions be reported to; how to report the matter; what to report; and operation of the ATO staff protection and reporting policy.

[121] A confidential service introduced by the Commissioner in 1998 to help ATO staff air their concerns or complaints relating to the organisation. *ATO Concern* is independent of Business and Services Line influence and reports to the Commissioner.

6.10 The ANAO considers the Reporting Guidelines are adequate and provide guidance to, and instigate a level of confidence in, staff who are trying to decide what they should do about the possible or suspected dishonest or unlawful behavior of another member of staff.

6.11 The Investigations Services Unit[122] consults with the Manager Investigations to determine case allocation priorities according to existing workload.[123] The current segregation of duties between FP&C Section's Investigation Services and Investigation Unit is considered to be better practice. The present arrangement minimises the scope for collusion. It also enables a preliminary screening of cases to be undertaken prior to being referred for investigations.

The Case Management System

6.12 In 1995 the FP&C Section initiated the development of a computer-based Case Management System to facilitate better administrative management of fraud investigations. The Case Management System (CMS) replaced aspects of the existing manual (paper-based) case system as well as providing an additional case-costing functionality. The CMS increases administrative efficiency and effectiveness in areas such as:

- timely entry and access to case investigation information;
- consistency of case investigation information, as FP&C Section investigators must enter information into the System in an established format; and
- analysis by FP&C management of case statistics, extraction of performance information and tracking the progress of investigations.

Development of the Case Management System

6.13 When the CMS was first developed in 1995 there were no computer packages that provided the case management functions required by the FP&C Section. As a result, FP&C Section developed the CMS using the *Microsoft Access* relational database package.[124] The ANAO considers that the use of this software was an innovative and cost effective method of modernising the manual case management system.

---

[122] The Investigation Services Unit is responsible for: being a focal point for receiving and registering reports of possible fraud or misconduct; creating and accounting for investigation files; determining whether a reasonable basis exists for the making of an allegation; and undertaking preliminary inquiries and case preparation.

[123] *Statement of Investigation Standards*, p. 13.

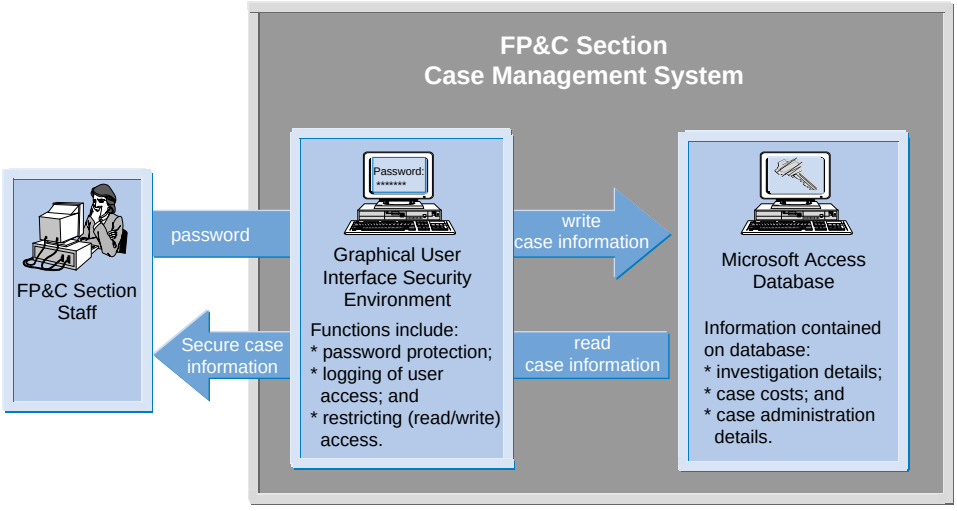
[124] The Access database is a series of linked tables. Data is entered through a series of forms accessed through an entry screen which is a form with a number of buttons. Data may be extracted from the database either through visual reference (ie. looking at raw data in tables) or through a series of custom-designed queries.

6.14 For security purposes, the CMS operates on a Local Area Network (LAN) that is not connected to other ATO networks. The physical separation of the CMS from other ATO computer systems provides assurance that case investigation information can only be accessed by FP&C Section staff and not by other ATO staff members.[125]

6.15 A 1998 review of the FP&C Section also examined the effectiveness and integrity of FP&C Section systems for the identification, recording and allocation of fraud investigation cases.[126] The review raised a number of issues relating to the integrity of CMS data.[127]

6.16 As a result of the 1998 review the FP&C Section implemented a new graphical user interface security environment[128] for the CMS as part of a $110 000 upgrade of the system. Figure 15 illustrates the configuration of the new CMS, including the security module.

Figure 15
Internal Investigations System Total Case Management system



---

125 The FP&C Section is located in a secure section of the ATO National Office. Entry to this secure area can be gained only with 'swipe card' access not available to non-FP&C Section staff. Therefore only FP&C Section staff can gain access to computer terminals connected to the FP&C Section LAN.

126 External consultants were engaged to review the operations of the FP&C Section on 27 July 1998. The review was completed and a draft report was provided to ATO by 7 August 1998.

127 The issues raised related to: difficulties in safeguarding the CMS from unintentional or deliberate misuse with all FP&C Section staff having access to all elements and transactions of the CMS; and the design and implementation of the CMS did not support sufficient restrictions and event logging. That is, modifications could be made to the CMS data with no audit trail.

128 The new security module was written using the Visual Basic programming language.

Case Management System security module

6.17 The new security environment addresses the issues relating to logging accesses and restricting user access (raised in the 1998 review) by providing:

- access to the case management data through a password control mechanism;[129]
- an environment in which users can examine and alter the data within certain restrictions.[130] Where a user accesses a record that is not assigned to him/her, the security environment logs that access[131]; and
- a facility to generate reports on case and performance information from the security environment.

6.18 The ANAO notes that if the CMS is accessed through the security environment, then the data contained on the system is secure.

Unauthorised access to Case Management System database

6.19 As noted previously, the CMS is located on a separate FP&C Section LAN to prevent unauthorised access. However all users of the LAN (that is, FP&C Section staff) have the ability to access all information contained on the LAN server.[132] This includes the Microsoft Access database file. Directly accessing this file from the server bypasses all security controls provided by the security environment. Therefore, information contained on the CMS may be altered, deleted or corrupted without an audit trail.

6.20 The ANAO acknowledges that it would be difficult for a user with limited experience to bypass CMS security. However, a persistent user, or a user with high level computing skills, could bypass CMS security in a relatively short period of time and without detection. The ANAO considers that security could be significantly enhanced through the encryption[133] of the CMS Microsoft Access Database file.

---

[129] Under the security module, passwords must be changed every month. The same password cannot be used for 10 months. This complies with the standards proffered by the Department of Defence's Defence Signals Directorate to ensure password security.

[130] For example, all FP&C Section investigation officers are able to read and write to the cases they manage. However, investigators are only able to view each others cases not alter the data.

[131] A log shows the date, time and action of a user accessing a file not assigned to that user. Log files do not show accesses by the users where a case is assigned to that user. The ANAO acknowledges that to log every instance where a user reads or alters one of their cases may become administratively unwieldy.

[132] Servers are computers that provide users with access to: commonly used databases; communications services; and remote software.

[133] Encryption is a technique for scrambling information to make it unintelligible during transmission or when not properly accessed. It provides security by preventing an accidental intruder, hacker, or computer criminal gaining access to information.

Recommendation No.10

6.21 The ANAO recommends that the ATO examine the cost/benefits of enhancing the security of its Fraud Prevention Case Management System with encryption to ensure information held on the system is secure and cannot be altered, deleted or corrupted by the Fraud Prevention and Control Section staff without an audit trail.

ATO Response

Agree.

Effectiveness of fraud investigations

6.22 To discuss the effectiveness of the ATO's fraud investigations process, the ANAO:

- reviewed the findings of the AFP Quality Assurance Review[134];
- examined the FP&C Section's internal quality assurance processes for investigations;
- established whether officers responsible for conducting investigations in the ATO were trained to meet prescribed requirements; and
- examined a sample[135] of finalised case files to assess compliance with the ATO operational procedures as outlined in the Statement of Investigation Standards.

6.23 The ANAO also sought feedback from ATO Business Lines and *ATO Concern* on the overall investigation process. The staff that we spoke to from Business Lines were unanimous in confirming the professionalism of the current investigations team. Staff acknowledged that there had been a marked improvement in the attitude and approach of the investigations team since 1995.

---

[134] In July 1999 the AFP undertook a Quality Assurance Review of the FP&C Section's investigation processes. The review was undertaken in accordance with the Commonwealth Fraud Control Policy using the better practice fraud investigations package issued by the Commonwealth Investigations Technical Standards Committee.

[135] The sample size was not selected as a statistical basis, but more to provide an indication whether processes were being followed. The ANAO initially reviewed 20 cases finalised in the last three years (18 were made available—one case file could not be found and one case file was identified as a second part of another case). Subsequently another 20 case files finalised in 1999-200 were examined to verify FP&C Section's assertions that file administration practices had significantly improved in the last financial year. The cases were selected at random from the Case Management System.

AFP Quality Assurance Review

6.24 This was the first Quality Assurance Review conducted by the AFP on ATO's internal investigation processes since the implementation of the revised Fraud Control Policy in 1994. The review was undertaken in 1999 and examined a finalised investigation case file and a range of material produced by the ATO relating to investigation procedures and fraud awareness issues. The review was finalised in January 2000 and identified a number of 'worthy'[136] practices.

6.25 The FP&C Section advised that the AFP, in providing feedback, had commended ATO's standards and considered them to be the Australian benchmark regarding fraud investigation and fraud awareness practice. The areas for improvement identified by the review largely related to file administrative practices.[137] The ANAO's review of a sample of finalised cases supported the AFP's views.

Internal quality assurance processes

6.26 The FP&C Section has introduced a number of quality assurance processes with a view to continuous improvement. These include:

- implementing a system of internal post-investigation reviews (peer reviews), which are to be conducted on 30 to 40 per cent of completed investigations;
- the Manager Investigations approving all cases recommended for closure; and
- FP&C Section management conducting annual better practice seminars for all staff.

6.27 The ANAO supports these initiatives introduced to ensure the effectiveness of the internal investigations process. Where files were subjected to peer review, the ANAO found that reports were prepared outlining the scope and outcome of the review. There was also evidence to show that matters raised as a result of the review were followed-up with the relevant investigator or proposed as a discussion point at the FP&C Section staff meeting.

---

[136] Practices identified as 'worthy' were the new Fraud Prevention Case Management System, Investigations reference CD-ROM, training and development program for the investigators and the ATO's fraud awareness program.

[137] Issues raised by the review related to maintaining a consistent format of the running sheets (a chronology of dates and events relating to actioning of case), assigning appropriate security classification to the documents on file and ensuring that exhibit registration procedures (maintaining all exhibits in a secure storage) are followed.

6.28 The ANAO noted that there was no systematic process to record the findings from the peer review. Although the Manager Investigations was maintaining a database to identify the case files that had undergone peer review, this had not been kept up-to-date. The ATO advised that this was due to a significant operational commitment involving the Manager, Investigations in 1999–2000.

6.29 The ANAO considers the peer review process to be valuable. Maintaining a systematic database of the peer reviews would provide ready information on the number of peer reviews undertaken at any given time, the broad findings arising from these reviews and the coverage of the individual investigators. It would also assist in undertaking a systematic analysis of lessons learned from these reviews, thus contributing to the continuous improvement process.

6.30 The ANAO also found some weaknesses in FP&C Section's file closure practices. A high proportion of the case files[138] examined by the ANAO (35 per cent) had not been closed appropriately. That is, there was no evidence of the file being approved for closure. The ANAO acknowledges that work pressures and priorities can cause delays in files being approved for closure. However, files should not be registered as closed on the CMS until the relevant officer has approved them. This procedure would provide assurance that correct work practices were being followed, and would maintain the integrity of the process.

Staff training

6.31 The ANAO found that the ATO had provided FP&C Section staff with access to a number of internal and external training programs. All investigators within the FP&C Section were enrolled in the Attorney-General's Department-endorsed Graduate Diploma in Fraud Control (Investigation) Program. The majority (75 per cent) of the FP&C Section investigations staff have also completed the AFP Management of Serious Crime (MOSC) program.

6.32 The ATO advised that the Section's senior investigators were drawn from fraud squads in various law enforcement agencies and had several years of detective experience. The Section's staff training strategy, has therefore been designed to ensure their ongoing professional development.

6.33 The ANAO considers that the Section has been pro-active in ensuring that its investigations staff fulfil the basic training requirements prescribed by the Attorney-General's Department. We also noted that it

---

[138] Of those finalised in 1999-2000.

has formulated a long-term training strategy to ensure the ongoing professional development of staff.

ANAO case file analysis

6.34 Overall, the ANAO found that investigations were undertaken in accordance with the documented procedures. The review of case files indicated that cases that were significant in terms of materiality or visibility were handled promptly by the Investigations Unit. Cases, which involved routine or minor instances of fraud, were handled by the Unit as part of a team approach, which involved identifying and investigating outstanding complaints by region to achieve economies of scale.

6.35 However, the ANAO found scope for improvement in administrative aspects of the FP&C Section's investigation function. Particularly in the quality of the information held in the CMS. These included:

- timeliness of investigations: analysis of FP&C Section's case management data for 1998–99 and 1999–2000 showed a significant decrease in the average time[139] taken to complete investigations despite a substantial increase in the number of cases received. We noted that much of the timeliness data contained in the CMS is incorrectly recorded or incomplete.[140] This significantly distorts these results. However, the FP&C Section does not use the CMS data to report on the timeliness of its investigations.[141] Due to the poor quality of the CMS data on this aspect, the ANAO could not undertake analysis to form a view on the time taken between various stages of the investigations process;
- weaknesses in the FP&C Section's file management practices.[142] We found over a third (35 per cent) of the cases examined were not closed in accordance with the Investigations Guidelines[143]. Appropriate file

---

[139] According to the FP&C Case Management System, in 1998-99 it took 527 days (average) for FP&C Section to complete a fraud case. In 1999-2000 this time was reduced to 163 days, despite a significant increase in the number of cases received (see Figure 2).

[140] The referral dates as noted on the paper file did not match the CMS referral date in 21 per cent of the cases examined. None of the file closure dates on the paper file matched the CMS file closed date for the cases examined.

[141] The total number of cases finalised each quarter divided by the total number of investigation staff involved in handling these cases, is the current basis of reporting.

[142] Since the exit interview (17 July 2000) we examined an additional 19 (requested 20, however one file could not be located) case files finalised in 1999-2000. The FP&C Section's requested that the ANAO examine 1999-2000 cases as file management practices had significantly improved during this period.

[143] Manager Investigations is required to approve the closure of all cases. This did not occur in over a third of the cases sampled by the ANAO.

closure practices are an important element of the accountability process. Adherence to these procedures provides some assurance on the integrity of the process; and

- recording of investigation costs: As part of the file maintenance process, investigators were also required to record the cost of the investigation (which includes salary and administration costs). From 1999–2000 indirect costs (overheads) have also been incorporated into the Case Management System. However, we found that while these costs were being recorded, they did not present an accurate reflection of the costs incurred (see Table 2).

Table 2

Analysis of FP&C Section's investigation costs[144]

FP&C Section Investigation Unit salary costs for 1999–2000 (as recorded in the FP&C section for 1999–2000)	$134 886 (a)	FP&C Section Investigation Unit investigations costs for 1999–2000[145] (as recorded in the FP&C section for 1999–2000)	$187 440 (a)
Total actual annual salary costs of investigators for 1999–2000	$1 111 656 (b)	Total budgeted investigation costs for 1999–2000	$1 700 000 (b)
FP&C Section Investigation Unit salary costs charged to investigations for 1999–2000 as a proportion of total actual salary costs for 1999–2000	12 per cent (a / b)	FP&C Section Investigation Unit investigation costs charged to investigations for 1999–2000 as a proportion of total budgeted investigation costs for 1999–2000.	11 per cent (a / b)

Source: Fraud Prevention and Control Section Case Management System and Fraud Prevention and Control Section budget papers.

6.36 The figures in Table 2 suggest that only 11–12 per cent of the investigations team's time is spent on conducting investigations or only 11–12 per cent of the cases are recorded on the CMS. The FP&C Section advised that these figures did not represent accurate investigation costs. Recording such costs provides ATO management with a complete picture on its fraud control arrangements and an accurate basis for undertaking internal benchmarking exercises. The Section advised also, that it would re-examine the costing methodology.

---

[144] Source: FP&C Section Case Management System.

[145] Includes administration and overheads.

6.37 The ANAO understands that the ATO is one of the few agencies which does record its investigation costs and we support this initiative. It is therefore important that the costing methodology appropriately reflects the actual cost of the investigations.

6.38 As mentioned in Chapter 1, the ATO's 1998 contestability exercise undertook comparisons between the ATO costs for a range of actual cases with the costs which would have resulted from a 'cheapest rate' commercial investigation. While the contestability results indicated that the ATO was more than contestable, the ANAO considers there are limitations about the results reported because of the costing methodology used.

Recommendation No.11

6.39 The ANAO recommends that the ATO strengthen the administrative controls associated with the Fraud Prevention Case Management System to ensure that the information contained in the system is accurate and timely.

ATO Response

Agree.

Prosecution and other remedies

6.40 As illustrated in Figure 13, an outcome of an internal investigations process could be a referral to the DPP, the AFP or the ATO's Official Conduct Team (OCT) for minor matters not involving criminal behaviour. The Commonwealth Fraud Control Policy outlines the circumstances under which the AFP is to be involved in investigations directed under the *Crimes Act 1914.*[146]

6.41 The ANAO examined whether the ATO had procedures established for:

- referral of cases to the DPP and the AFP; and
- imposing alternative remedies for minor fraud and other related matters.

[146] There are three exceptions to the AFP's involvement in investigations under the *Crimes Act 1914.* These are: agencies which prosecute fraud cases under their own legislation (includes ATO; agencies which can satisfy both the AFP and the DPP that they have the capacity and capability to investigate criminal cases; and matters involving multi-jurisdictional organised crime referred to the National Crime Authority.

Referral to DPP and AFP

6.42 The prosecution policy of the FP&C Section is the Prosecution Policy of the Commonwealth. The FP&C Section follows the referral guidelines detailed in the Commonwealth Prosecution Policy. The Statement of Investigation Standards also provides guidance on preparation of the briefs of evidence, disclosure requirements to the DPP and referrals to the AFP.

6.43 The FP&C Section is not required to clear cases referred to DPP through the ATO Executive. The current arrangements confer a semi-autonomous status on the FP&C Section. In the case files examined by the ANAO, three cases were referred to the DPP for prosecution. The ANAO found these cases were well-prepared, containing detailed briefs of evidence. This view was supported by the DPP, who considered the FP&C Section briefs of evidence to be of a high standard compared to other Commonwealth agencies.

Alternative remedies

6.44 Where an investigation identifies a case of misconduct or recommends staff disciplinary action, the Investigations Unit refers it to ATO's OCT.

6.45 The OCT was established in 1998 as part of the Human Resource function. Prior to this, the staff disciplinary process was handled through ATO personnel sections located in 26 Regional Offices. The team now has representation in five Regions (Canberra and National Office, NSW, Queensland, Vic/Tas and WA/SA).

6.46 Under the ATO's Managing Misconduct Policy, all managers must address all misconduct issues in their areas of responsibility. The role of the OCT is solely to support the integrity and proper application of the ATO's disciplinary process by ensuring:

- adherence to process and guidelines; and
- consistency of approach, especially when considering sanctions.

6.47 The ANAO found that the ATO has undertaken a number of initiatives to improve the relationship and liaison arrangements between the FP&C Section and OCT. These include:

- members of the FP&C Section are invited to attend formal OCT conferences;
- the establishment of an Official Conduct Investigations Unit within the FP&C Section (effective from 1 July 2000); and
- maintaining ongoing liaison between senior OCT members and management of FP&C.

6.48 The Official Conduct Investigations Unit established recently will be responsible for independently investigating alleged serious breaches of the Code of Conduct and will also provide investigative assistance to a 'Determining Officer' as required.

6.49 The ANAO was advised that due to the increasing fraud workload, the FP&C Section could not carry out their investigations to the extent preferred before matters were handed over to the OCT. This placed part of the investigative load on OCT and other relevant ATO officers. The establishment of a dedicated Official Conduct Investigations Unit will ensure that investigations are adequately completed before the case is handed over to the OCT. The initiative also improves the efficiency of the process in terms of the timely completion of investigations without compromising the quality and consistency aspects.

6.50 The ANAO's analysis of investigation cases also indicates that cases referred to the OCT comprise 73 per cent of the total cases referred outside the FP&C Section. Therefore, establishing the Misconduct Investigations Unit is seen as a positive initiative contributing to the effectiveness of the investigations process.

Conclusion

6.51 Internal fraud investigations form a significant aspect of the FP&C Section's activities. Being able to prepare detailed briefs of evidence and undertake internal investigations with limited AFP involvement signifies the confidence of the DPP and the AFP in the ATO's internal investigation capabilities. ATO has developed a set of Investigation Guidelines, which are appropriately linked to several other ATO and Commonwealth policy documents and procedures. Making the Investigation Guidelines available on CD-ROM, increases their accessibility. The AFP's quality assurance review commends ATO's investigation practices and this is supported by ANAO's review of a sample of finalised cases.

6.52 The FP&C Section has also taken initiatives to improve its relationship and liaison arrangements with the Official Conduct Team, which is responsible for ensuring the appropriate application of the ATO's disciplinary processes.

6.53 However, to ensure higher level of accountability and security of investigations information the FP&C Section should re-examine the following components of its operations:

- the security of its Fraud Case Management System; and
- investigations file management and administration practices, including the quality of information held in the Fraud Case Management System.

Canberra A.C.T.
29 November 2000

P. J. Barrett
Auditor-General

Appendices

Appendix 1

Relevant reports on fraud control arrangements

The ANAO's audit on the fraud control arrangements in the ATO is one of a series of performance audits into fraud control in the Commonwealth to be reported in the 2000–2001 financial year. To date, we have reported on:

- *Fraud Control Arrangements in the Department of Industry Science and Resources*, The Auditor-General Audit Report No.5 2000–2001; and
- *Fraud Control Arrangements in the Department of Health and Aged Care (DHAC)*, The Auditor-General Audit Report No.6 2000–20001.

The ANAO also conducted a *Survey of Fraud Control Arrangements in APS Agencies*, Audit Report No 47 1999–2000. The ANAO concluded that the majority of APS agencies responding to the survey had a framework in place that contained key elements for effectively preventing and dealing with fraud in line with Commonwealth Policy.

Previous audits conducted by the ANAO into fraud control have included:

- The Auditor-General Audit Report No.4 1999–2000 *Fraud Control Arrangements in Employment, Education and Youth Affairs;*
- The Auditor-General Audit Report No.52 1999–2000 *Control Structures as Part of the Audits of Financial Statements of Major Commonwealth Agencies for the Period Ended 30 June 2000;* and
- ANAO Audit Report No.6 1994–95 *Information Technology Security* Australian Taxation Office.

ATO Reviews

- Ernst and Young. *Draft review of the Australian Taxation Office's FP&C Section (report not finalised).*
- Freeman, P. *Internal Reporting: ATO Compliance with International Best Practice*, 30 August 1999; and
- Sherman, T*: Integrity of Private Binding Rulings and Advance Opinions.* Initiated by Commissioner of Taxation in May 2000.

Senate Inquiry into the ATO

On the 24 June 1998 the Senate referred to the Senate Economics and References Committee the matter of the operation of the Australian Taxation Office (ATO). The review was finalised in March 2000.

See Appendix 7 for the review's terms of reference.

Appendix 2

Functions of the ATO Integrity Advisory Committee

The functions of the Integrity Advisory Committee are to advise on:

- activities concerned with:
  - — upholding and fostering the APS Values;
  - — promoting compliance with the Code of Conduct, including ethical standards;
  - — preventing fraud, including the conduct of investigations and the protection of staff who report matters;
  - — managing the ethical challenges associated with contractor staff and outsourced business relationships; and
  - — emerging issues relevant to sustaining an integrity based ATO.
- the issues concerned with enhancing community confidence in the integrity of the ATO;
- innovations and emerging trends in public sector administration and accountability on issues relevant to the role of the Committee; and
- whether ATO endeavours on sustaining an integrity based organisation are realistic, achievable and accord with best practice standards.

Appendix 3

ATO fraud risk assessment methodology

The risk assessment methodology used was an adaptation of an overall fraud evaluation and control methodology designed by the consultants based on their experience with risk management and control evaluations in other Government organisations. The key elements were:

- an assessment of risks to ensure appropriate attention is directed to areas of greatest vulnerability;
- a detailed threat analysis of areas with significant exposures and risks identified in the 1997–99 assessment to confirm the nature and severity of the risk involved;
- an assessment of the adequacy of controls for the prevention and detection of fraud in the higher risk areas; and
- the development of a program for the ongoing control of fraud in the future (Fraud Control Plan).

In accordance with the requirements of the Commonwealth Fraud Control Policy, the risk assessment distinguishes between Inherent Risk (ie. before controls are applied) and Residual Risk (ie. remaining risk after controls have been applied) and provides a means of quantification of a risk.

Several workshops were held to make an assessment of the fraud risk for all of the ATO's functions and activities against an agreed set of criteria. The workshops involved a large number of staff of the ATO and information was gathered from staff experienced in a wide range of ATO activities. Workshops were held in the following offices:

- National Office (ACT);
- Hurstville, Parramatta, Penrith, Bankstown and Sydney CBD (NSW);
- Moonee Ponds, Box Hill and Casselden Place (VIC);
- Brisbane CBD (QLD);
- Waymouth (SA);
- Cannington (WA);
- Northbridge (WA); and
- Hobart (TAS).

The functions and activities were ranked by Inherent Risk. This is referred to as a 'green fields' measurement of the risk of fraud in the Commonwealth Fraud Control Policy. This involves the measurement of the risk of internal and external fraud in the absence of any internal control to prevent or detect the occurrence of the fraudulent activity. The functions and activities were also ranked by Residual Risk.

The primary purpose of the Fraud Risk Assessment was to identify those functions and activities within the ATO which have been assessed as having a higher risk of fraud. These functions and activities were then subject to a detailed review of fraud risks and controls.

The assessment of controls was based on the development of detailed analysis against the fraud/risk control model which was used to facilitate the control assessment process. It involved:

- analysis of actual procedures against desirable control or 'what can go wrong'. Actual procedures were established by a series of interviews and review of documentation and these were compared to the known standard control models;
- consideration of the adequacy of existing controls and design of improvements where necessary;
- collation of results of the analysis of all operations into one integrated control program; and
- integration within each program of all aspects of fraud control. That is, as the fraud control review was completed for each program, an overall picture was built up and common issues identified and addressed.

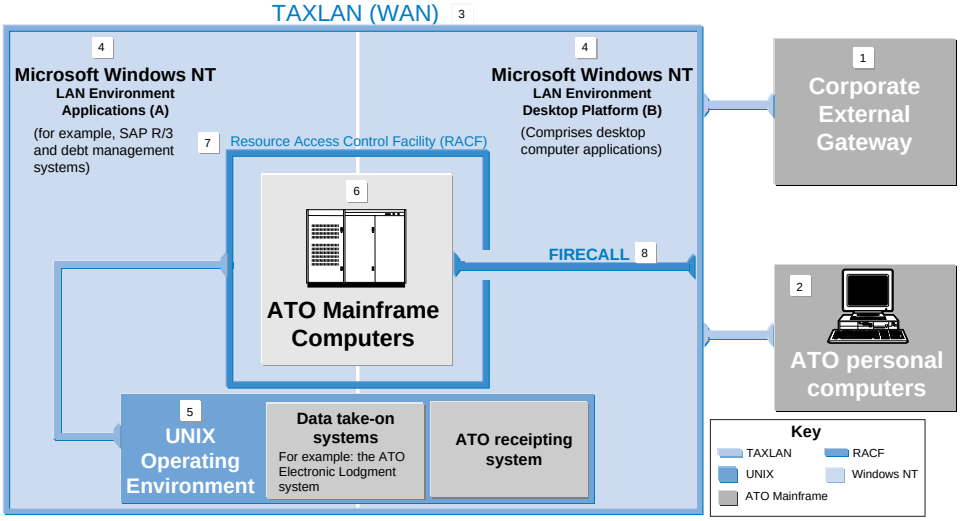
Appendix 4

Materials provided to ATO staff as part of the ATO's Fraud Awareness Program

- APS Code of Conduct;
- Fraud Prevention and Control Section details and information;
- *You and the ATO* brochure: outlines Public Service Values, Code of Conduct, and conflict of interest issues;
- ATO expected behaviours;
- ATO national policy on the proper use of ATO information technology facilities;
- ATO national policy on recruitment and selections;
- The fraud and misconduct staff protection and reporting policy;
- Guidelines for Public Servants seeking to take outside employment;
- ATO national policy for managing misconduct;
- Guidelines on internal investigations;
- Overview of the procurement guidelines;
- ATO Human Resources Service—Official Conduct Team;
- The role of the Fraud Prevention Team;
- Details on the Employee Assistance Program;
- Guidelines on Official Conduct of Commonwealth Public Servants;
- *ATO Concern* guidance document; and
- Computer mouse mat with fraud prevention information.

Appendix 5

ATO information technology environment



1. Corporate External Gateway: is the mechanism that takes a flow of messages (both internally and externally), determines their destination, makes any translations needed, and sends them out to their intended destination. For example a major function of the ATO External Gateway is the examination of electronic mail (for material deemed by the ATO to be inappropriate) entering and leaving the ATO computer system.

2. ATO Personal Computers: are the principal devices used by ATO staff to access the ATO computer system. ATO personal computers are networked through TAXLAN (see 3) and operate in a Microsoft Windows NT Operating Environment (4).

3. TAXLAN: is the ATO's Wide Area Network that connects principal components of the ATO's IT system together. The components include numerous other IT networks contained on Microsoft Windows NT, Unix and mainframe operating systems.

4. Windows NT operating environment: is the principal operating environment used by ATO staff to navigate to all other ATO IT networks (including networks contained on the Unix operating system and mainframe environment). It also contains Local Area Network applications such as the SAP R/3 human resources and financial management system and debt management systems. It is the operating environment for other desktop applications such as Microsoft Office.

5. Unix operating environment: is the operating environment housing a number of ATO applications including its Direct Data Entry

system, debt management system (COMPACT) and Electronic Lodgement system. Applications contained in this environment are linked directly to the ATO mainframe system.

6. ATO mainframe Computers: are the repositories for all taxpayer information and supporting computer programs. Access to ATO mainframe computers is protected by the RACF (see 7).

7. Resource Access Control Facility (RACF): provides access control to the ATO mainframe environment. Access control is structured to facilitate devolution of security administration. Devolution is based on users defining access rights by position.

8. *Firecall*: is a RACF facility to give nominated staff special access to the mainframe environment, not available to these users under their normal access rights**.** It allows users to bypass all regular RACF controls.

Appendix 6

ATO Secrecy Legislation and Information Technology Security Policy

ATO secrecy legislation

Extract from the *Taxation Administration Act 1953*

3C(1) ["officer"]

In this section, ''officer'' means a person:

(a) who is or has been appointed or employed by the Commonwealth; or

(b) to whom powers or functions have been delegated by the Commissioner, and who, by reason of the appointment or employment or in the course of the employment, or by reason of, or in the course of the exercise of powers or the performance of functions under, the delegation, as the case may be, may acquire or has acquired information with respect to the affairs of any other person disclosed or obtained under or for the purposes of this Act .

3C(1A) [Person performing services for Commonwealth]

For the purposes of this section, a person who, although not appointed or employed by the Commonwealth, performs services for the Commonwealth shall be taken to be employed by the Commonwealth.

3C(2) [Prohibition against disclosing information]

Subject to subsection (4), a person who is or has been an officer shall not, except for the purposes of this Act or otherwise than in the performance of the person's duties as an officer, directly or indirectly:

(a) make a record of any information with respect to the affairs of a second person; or

(b) divulge or communicate to a second person any information with respect to the affairs of a third person, being information disclosed or obtained under or for the purposes of this Act and acquired by the person by reason of the person's appointment or employment by the Commonwealth or in the course of such employment, or by reason of the delegation to the person of powers or functions by the Commissioner , or in the course of the exercise of such powers or the performance of such functions, as the case may be.

Penalty: $10,000 or imprisonment for 2 years, or both.

ATO security policy

Extract from the ATO document *The Proper Use of Australian Taxation Office Information Technology Facilities*

6 (1) Examples of Improper (Information Technology Facility) Use

In this context, improper use of IT facilities includes, but is not limited to, the following:

a. Violating any laws covering the use of computing facilities or networks.

b. Using IT facilities for purposes other than those for which they were intended.

c. Using IT facilities outside the scope of an employee's authority.

d. Using, or knowingly allowing another to use, any part of ATO IT facilities to devise or execute any artifice or scheme to defraud or obtain money, property, services or any other benefit by untrue representation.

e. Using any part of ATO IT facilities to conduct any business or other activity for commercial purposes or financial gain.

f. Introducing by any means unacceptable material onto ATO IT facilities.

g. Storing unacceptable material using ATO IT facilities.

h. Dispatching unacceptable material using ATO IT facilities.

i. Camouflaging, in any way, unacceptable material stored or maintained on ATO IT facilities.

j. Harassing or threatening other users or interfering with their legitimate access to IT facilities.

k. Degrading, disrupting or otherwise interfering with ATO IT facilities.

l. Attempting to test, bypass or defeat any security safeguard established to protect an ATO IT facility without specific authorisation from the Director, IT Security or their delegate.

m. Circumventing or attempting to circumvent assigned limits, procedures or privileges without specific authorisation from the Director, IT Security or their delegate.

n. Without authority, destroying, altering, dismantling, disfiguring, preventing rightful access to, or otherwise interfering with, the integrity of any part of ATO IT facilities.

o. Without authority, invading the privacy of any ATO employee.

p. Without authority, accessing, disclosing or removing third-party proprietary information.

q. Without authority, seeking or gaining access to any ATO IT facility, whether owned by the ATO or not.

r. Without authority, attempting to modify or remove any ATO IT facility or part of an ATO IT facility.

Appendix 7

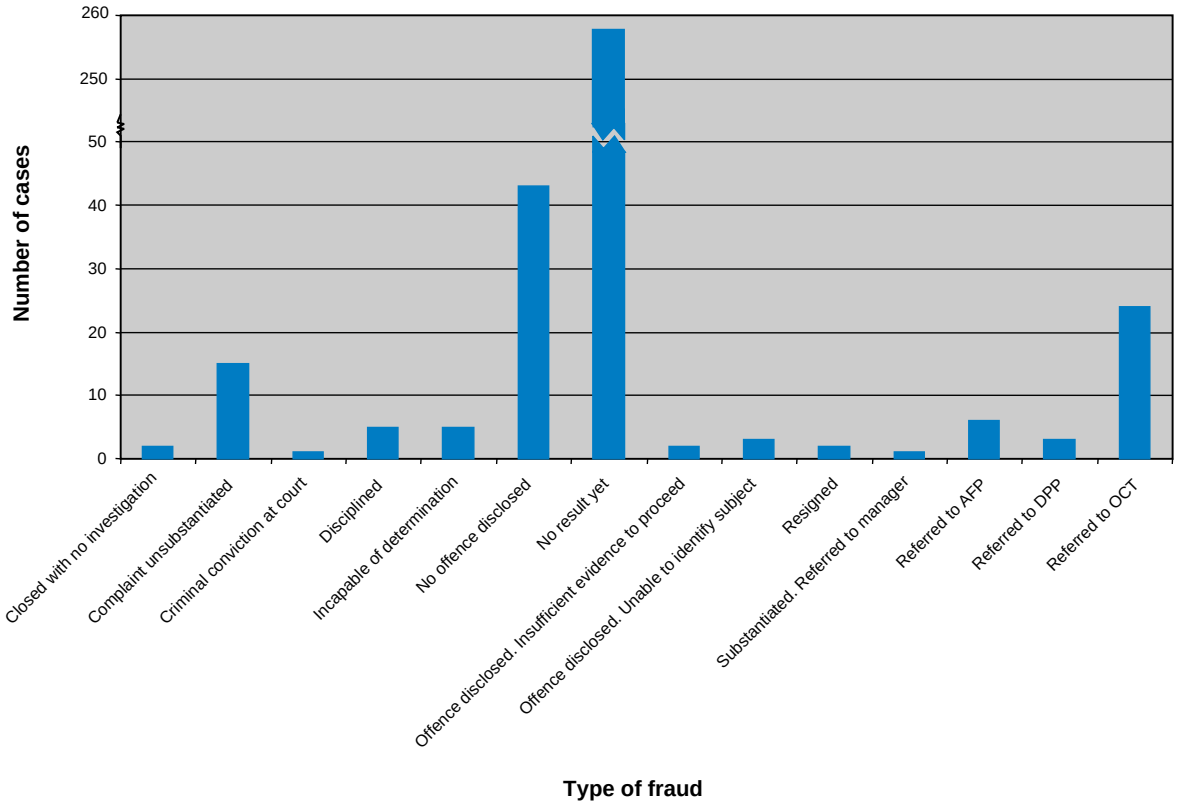
Senate Economics References Committee Inquiry into the Operation of the Australian Taxation Office, 6 August 1998

The terms of reference for the committee were:

- the equitable treatment of taxpayers;
- the performance of the Large Business and International Division, including, in particular, the High Wealth Individual Project;
- compliance by the ATO with the Client Settlement Guidelines; and
- allegations of infiltration of the ATO by organised crime.

Appendix 8

Results of Fraud Prevention and Control Section Cases for 1999–2000



Index

A

Access Management Team 27, 81, 82, 88
ATO Business and Service Lines 17, 37, 43, 50, 53, 58
Attorney-General Department 42, 59
audit approach 14
audit methodology 15, 17, 18, 31, 38, 40, 48-50, 53, 63, 64, 66, 89, 93, 102, 110, 111, 119
audit objective 14, 32, 35, 38, 47, 54, 62, 82
Australian Federal Police 16, 31, 40, 44, 67, 101

B

better practice 14, 15, 23, 33, 38, 42, 51, 59, 63, 66, 68, 69, 73, 82, 96, 97, 102, 103, 106, 107

C

Certificate of Compliance 20, 26, 70, 71, 73
Chief Executive Instruction (CEI) 43, 53
Commonwealth Director of Public Prosecutions (DPP) 14, 39, 40, 43, 44, 55, 89, 101, 111-113
Commonwealth Fraud Control Policy 13, 17, 18, 31-33, 42, 47, 48, 51, 58, 65, 67, 99, 103, 106, 125
Commonwealth Law Enforcement Board (CLEB) 13, 31, 42, 51

F

Financial Management and Accountability Act 1997 32, 33
Firecall 21, 27, 77, 81, 84-88, 90, 123
fraud awareness program 57, 63-66, 68, 107, 121
Fraud Control Liaison Officers 53, 71, 72
fraud control plan 15, 17-19, 25, 33, 42-44, 47-55, 57-60, 70-72, 97, 99, 119
fraud detection 16, 23, 27, 92-98
fraud investigation 14, 16, 22-24, 38, 44, 56, 62, 80, 89, 91, 96, 97, 99, 101-107, 109, 111, 113
fraud prevention 14-17, 19, 20, 22-24, 26-28, 31-33, 35, 36, 39, 40, 44, 45, 56, 57, 59, 61-65, 67-73, 9-93, 96, 98-101, 106, 107, 110, 111, 121, 128
Fraud Prevention and Control (FP&C) Section 16-20, 22-24, 35-37, 39, 40, 43-45, 52-58, 63-70, 72, 80, 88- 91, 93-98, 101-110, 112-114, 117
Fraud Prevention Case Management System 16, 28, 106, 107, 111
fraud risk assessment 15, 17, 18, 25, 42, 47-51, 53-55, 59, 93, 119, 120

H

Health of the System Assessment (HOTSA) 18, 48, 49, 51

I

Industry 132, 133
Information Technology (IT) 15
Integrity Advisory Committee (IAC) 43-45, 47, 53, 56, 57, 67, 118
Internal Assurance Branch (IAB) 35, 44, 55, 57, 59, 94, 97
internal audit 22, 27, 55, 57, 89, 93, 94, 96-98
Information Technology (IT) 15, 16, 20-22, 23, 27, 74-85, 87-89, 91, 92, 94, 95, 122, 125, 126
IT access 80-82

N

NSW Roads and Traffic Authority (RTA) 40, 68, 69

O

Official Conduct Team (OCT) 37, 101, 111-113

P

performance assessment framework 15, 18, 25, 42, 55, 56, 58-60
Pro-active IT controls 88

Q

quality assurance 61, 70, 72, 73, 93, 106, 107, 113

S

Statement of Investigations Standards 16

T

The Fraud Control Policy of the Commonwealth 13, 31, 32

U

unauthorised access 14, 20-22, 27, 36, 74, 78, 80, 82, 88-92, 105

W

Wide Area Network 16, 20, 21, 76, 122
Workplace Access Administrators 27, 81, 82, 88

Series Titles

Titles published during the financial year 2000–01

Audit Report No.15 Performance Audit
Agencies' Performance Monitoring of Commonwealth Government Business Enterprises

Audit Report No.14 Information Support Services Report
Benchmarking the Internal Audit Function

Audit Report No.13 Performance Audit
Certified Agreements in the Australian Public Service

Audit Report No.12 Performance Audit
Passenger Movement Charge - Follow-up Audit
Australian Customs Service

Audit Report No.11 Performance Audit
Knowledge System Equipment Acquisition Projects in Defence
Department of Defence

Audit Report No.10 Performance Audit
AQIS Cost-Recovery Systems
Australian Quarantine and Inspection Service

Audit Report No.9 Performance Audit
Implementation of Whole-of-Government Information Technology Infrastructure Consolidation and Outsourcing Initiative

Audit Report No.8 Performance Audit
Amphibious Transport Ship Project
Department of Defence

Audit Report No.7 Performance Audit
The Australian Taxation Office's Use of AUSTRAC Data
Australian Taxtion Office

Audit Report No.6 Performance Audit
Fraud Control Arrangements in the Department of Health & Aged Care
Department of Health & Aged Care

Audit Report No.5 Performance Audit
Fraud Control Arrangements in the Department of Industry, Science & Resources
Department of Industry, Science & Resources

Audit Report No.4 Activity Report
Audit Activity Report: January to June 2000—Summary of Outcomes

Audit Report No.3 Performance Audit
Environmental Management of Commonwealth Land—Follow-up audit
Department of Defence

Audit Report No.2 Performance Audit
Drug Evaluation by the Therapeutic Goods Administration—Follow-up audit
Department of Health and Aged Care
Therapeutic Goods Administration

Audit Report No.1 Performance Audit
Commonwealth Assistance to the Agrifood Industry

Better Practice Guides

AMODEL Illustrative Financial Statements 2000	Apr 2000
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.47 1998–99)	Jun 1999
Commonwealth Agency Energy Management	Jun 1999
Corporate Governance in Commonwealth Authorities and Companies–Principles and Better Practices	Jun 1999
Managing Parliamentary Workflow	Jun 1999
Cash Management	Mar 1999
Management of Occupational Stress in Commonwealth Agencies	Dec 1998
Security and Control for SAP R/3	Oct 1998
Selecting Suppliers: Managing the Risk	Oct 1998
New Directions in Internal Audit	Jul 1998
Life-cycle Costing (in Audit Report No.43 1997–98)	May 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	Jul 1997
Core Public Sector Corporate Governance (includes Applying Principles and Practice of Corporate Governance in Budget Funded Agencies)	Jun 1997
Administration of Grants	May 1997
Management of Corporate Sponsorship	Apr 1997
Return to Work: Workers Compensation Case Management	Dec 1996
Telephone Call Centres	Dec 1996
Telephone Call Centres Handbook	Dec 1996
Paying Accounts	Nov 1996
Performance Information Principles	Nov 1996
Asset Management	Jun 1996
Asset Management Handbook	Jun 1996
Managing APS Staff Reductions	Jun 1996