2

Audit Report No. 16, 2000-2001

Australian Taxation Office Internal Fraud Control Arrangements

Australian Taxation Office

Introduction

Background

2.1 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.

2.2 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.* Fraud is defined in this policy as:

> …inducing a course of acting or deceit involving acts or omissions or the making of false statement orally or in writing with the object of obtaining money or other benefit from, or evading liability to, the Commonwealth.[1]

[1] ANAO, Audit Report No. 16, *Australian Taxation Office Internal Fraud Control Arrangements*, 2000–2001, Commonwealth of Australia, p. 31.

2.3 In 1994, the Government formed the Commonwealth Law Enforcement Board (CLEB) 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[2] 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.[3]

2.4 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
- maintain high levels of service to the community consistent with the good Government of the Commonwealth.

2.5 The Attorney-General's Department is continuing the development of these objectives in three main areas, namely:

- 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.[4]

2.6 A review by the Attorney-General's Department of the Commonwealth Fraud Control Policy led to the release of *The Fraud Control Policy of the Commonwealth, Consultation Draft No. 1* in June 1999 and, in April 2001, the release of *Commonwealth Fraud Control Policy and Guidelines, Consultation Draft No. 2.*

2.7 The Government has outlined in this policy that responsibility for its implementation and for administration of fraud control rests with each Commonwealth agency and, more particularly, the Chief Executives of those agencies.[5]

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

[3] ANAO, Audit Report No. 16, 2000-2001, p. 31.

[4] ANAO, Audit Report No. 16, 2000-2001, p. 32.

[5] Attorney-General's Department, *Commonwealth Fraud Control Policy and Guidelines, Consultation Draft No. 2*, April 2001, pp.1-2.

ANAO objective and findings

2.8 In Audit Report No. 16, 2000–2001, *Australian Taxation Office Internal Fraud Control Arrangements,* the objective of the audit was to assess the administration of internal fraud control arrangements in the Australian Taxation Office (ATO) and to identify areas with potential for improvement.[6]

2.9 The audit focused on the ATO's internal fraud prevention and control arrangements. In particular, the audit looked at the activities of the Fraud Prevention and Control (FP&C) Section, corporate governance processes (including risk management) and ATO Business Line involvement in preventing and detecting internal fraud.[7]

2.10 The ANAO found that:

- the ATO had 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 had established a comprehensive fraud control policy framework;
- the level of alleged fraud in the ATO had steadily increased over the last few years;
- the security of IT systems should be an ongoing concern to ATO management; and
- the security of its Fraud Prevention Case Management System could be enhanced.[8]

2.11 The ANAO made 11 recommendations to improve the administration of internal fraud control arrangements in the ATO. The ATO agreed to all of the recommendations.

2.12 The ATO advised the Joint Committee of Public Accounts and Audit (JCPAA) that it expected to have the majority of the ANAO's recommendations implemented by the end of the calendar year.[9]

[6] ANAO, Audit Report No. 16, 2000-2001, p. 38.

[7] ANAO, Audit Report No. 16, 2000-2001, p. 39.

[8] ANAO, Audit Report No. 16, 2000-2001, pp. 15-16.

[9] A Preston, *Transcript*, 2 May 2001, p. 3.

Issues discussed at the public hearing

2.13 In the course of the public hearing, the JCPAA took evidence on the following:

- the definition of ’fraud’;
- fraud control framework;
- private binding rulings;
- fraud prevention, and
- IT security.

Definition of ‘fraud’

2.14 The audit report noted that the level of alleged fraud reported in the ATO has steadily increased over the last few years.

2.15 The dollar value of reported internal fraud is not readily available. Prior to 1998-99, the Fraud Prevention and Control (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 monetary amount of the fraud.[10]

2.16 Unauthorised access to taxpayer data remains the most common type of fraud perpetrated in the ATO.

2.17 The Committee asked the ATO how many of the 373 alleged cases of fraud reported in 1999-2000 were accessing a taxation file with the intent of blackmail or sale of information, or placing a contract with a supplier in return for money.[11]

2.18 An ATO spokesperson told the Committee:

> I am not aware of any cases in the last couple of years that fall into the categories that you have just mentioned....About 60 per cent of our cases [of fraud]

[10] ANAO, Audit Report No. 16, 2000-2001, p. 36.

[11] *Transcript*, 2 May 2001, p. 4.

> centre on unauthorised use of our computer systems to access taxpayer information.
>
> Our experience is that it is browsing and curiosity and acting in breach of the secrecy provisions in the various tax laws. We have no evidence of officers selling [information]. We have undertaken a number of investigations of staff who have been suspected of leaking information to the media for whatever purposes. But none of those enquiries have ever been able to substantiate to the required standard of proof that a particular individual committed the offence.[12]

2.19 The Committee raised the issue of the definition of 'fraud' with the ATO, asking whether it thought that the definition currently in place across the Commonwealth was a reasonable reflection of the common idea of fraudulent activity.[13]

2.20 The ATO responded that there had been a considerable degree of variation in the definition and it was now a service-wide issue to get a standardised definition:

> [The ATO puts] a very high focus on going beyond the purely quantitative direct harm [of fraud] to the Commonwealth in terms of revenues or expenditures and go to issues like inappropriate use of information, the influence value of gifts, and perception surrounding conflicts of interest. They are all intangibles, but they are of fundamental importance to an integrity based organisation.[14]

2.21 The Committee made the point that it attempted to promote widely greater accountability in the public sector, greater transparency, and reduction of fraud and criminality in dealings within the public sector and between the public and private sectors. It had some concern that other countries in the region may interpret the published fraud figures as representing what the Committee might term major fraud.[15]

[12] R Mulligan, *Transcript*, 2 May 2001, p. 4.

[13] *Transcript*, 2 May 2001, pp. 4-5.

[14] Preston, *Transcript*, 2 May 2001, p. 5.

[15] *Transcript*, 2 May 2001, p. 5.

2.22 The ATO indicated that it would not regard the published figures as an indicator of major fraud, but as an indicator of concern to the ATO:

> …I do not think I would interpret it as the source of concern in terms of our international credibility.[16]

2.23 The Committee asked whether there was a risk of encouraging fraud by talking about it so much, and whether there might be a need to change the language so that the highest ethical standards were encouraged in employees and contractors.[17]

2.24 The ATO was sympathetic to the Committee's view and noted that it was trying to transform the culture into a general focus on integrity in the broader context, within which the specific incidence of fraud was dealt with.[18]

Committee comments

2.25 While the Committee agrees with the ATO that unauthorised access to taxpayer data is serious, it is of some concern to the Committee that the current definition of fraud against the Commonwealth does not provide for subcategories which would clarify the nature of the reported fraud.

Recommendation 1

2.26 **The Committee recommends that the ANAO, in its preparation of a better practice guide on fraud control, develop subcategories of fraud for the purposes of fraud reporting, and discuss this issue with the Joint Committee of Public Accounts and Audit prior to finalisation of the better practice guide.**

Fraud control framework

2.27 The audit report stated that the ATO has established a comprehensive fraud control policy framework. The report noted that the ATO has also recognised the importance of an ethical and

[16] Preston, *Transcript*, 2 May 2001, pp. 5-6.

[17] *Transcript*, 2 May 2001, p. 6.

[18] *Transcript*, 2 May 2001, p. 6.

well controlled environment in maintaining community confidence in the taxation system and, particularly, in its revenue collection responsibilities.

2.28 At the hearing, the ATO drew attention to its fraud control plan and its development of fraud and ethics training programs. The ATO explained that the training programs had been well received in terms of improving both staff understanding and the level of staff reporting of suspected fraud:

> …the ATO's internal fraud control arrangements have not stood still since the [audit] report was tabled last November. The fraud and ethics training has continued in the current financial year. To 20 April, 3850 staff have attended the first program and 2094 the second. Work has commenced on developing the third in this series of fraud and ethics training programs.
>
> Our recently established Integrity Advisory Committee has been meeting quarterly to consider issues bearing on sustaining and reinforcing an integrity based ATO. A major focus has been the establishment of an integrity adviser position for the ATO. The integrity adviser would advise ATO officers and the ATO more generally on ethics and integrity issues that can arise in interactions with taxpayers, service providers to the ATO, and in normal administration. …we expect to fill the position shortly. [19]

2.29 The Committee noted the steadily increasing number of incidents of alleged fraud.[20] The level of alleged fraud reported in the ATO has steadily increased from 255 cases in 1994–95 to 373 cases in 1999–2000.

2.30 The ATO considers that the increased incidence is due to a significant improvement in staff awareness of fraud and ethics, increased staff confidence that a reported matter will receive attention and that the interests and well being of staff who report wrongdoing by other staff will be protected.[21]

[19] Preston, *Transcript*, 2 May 2001, p. 3.

[20] *Transcript*, 2 May 2001, p. 4.

[21] ANAO, Audit Report No. 16, 2000-2001, p. 36.

Committee comments

2.31 The audit report identified in the ATO areas of better practice in fraud control planning, and staff education and training. The Committee considers that the ATO is moving positively in these areas.

Private binding rulings

2.32 The Committee asked about the level of fraud control assurance in relation to private binding rulings.[22]

2.33 In response, the ATO stated that the processes for issuing both public and private rulings were treated exactly the same as other processes operating inside the ATO:

> They fall clearly within the ambit of the fraud control plan for the whole ATO. They were reviewed as part of that process when the latest fraud control plan was developed.[23]

2.34 The ATO noted that the Sherman report and various ATO initiatives will require the fraud control arrangements to be reviewed again:

> The Tax Office is now going through a very protracted process of reviewing the entire private ruling process. It is looking at it end to end, rather than simply as a series of functions located in each of the tax lines, and bringing together very active management reformulated IT systems to support it and overall management of the function in our Office of the Chief Tax Counsel. …We are also creating a publicly accessible database as a result of the Sherman recommendation.[24]

2.35 In a submission to the Committee, the ATO advised that major improvements had been made by the ATO in the way it provided private binding rulings. The improvements included:

[22] *Transcript*, 2 May 2001, p. 11.

[23] R Mulligan, *Transcript*, 2 May 2001, p. 11.

[24] Mulligan, *Transcript*, 2 May 2001, p. 12.

- new guidelines on the types of written binding advice which may be issued by the ATO and the officers who may approve such advice;
- a process to publish edited versions of the written binding advice given (with identifying features removed);
- an integrated case management system;
- the introduction of a registration number which can be used to track the progress of all requests for private binding rulings; and
- an improved process for assuring the capability of staff preparing or approving written binding advice.[25]

Committee comment

2.36 The Committee notes the measures implemented by the ATO in relation to the provision of private binding rulings. It also notes the recently released ANAO audit report on private rulings which found significant deficiencies associated with the private rulings system.[26]

Fraud prevention

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

2.38 The ATO's Financial Services Section 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.[27]

2.39 The ATO's Financial Services Section utilises a 'Certificate of Compliance' process to provide assurance that new financial

[25] ATO, Submission no. 4, pp. 1-2.

[26] ANAO, Audit Report No. 3, 2001-2002, *The Australian Taxation Office's Administration of Taxation Rulings*, Commonwealth of Australia, 17 July 2001.

[27] ANAO, Audit Report No. 16, 2000-2001, p. 70.

systems have controls in place to prevent and detect fraudulent activity.[28]

2.40 The ANAO report noted that the Certificate of Compliance process was limited to financial systems. The ANAO considered that fraudulent activity could occur in both financial and non-financial systems and recommended that the ATO extend its 'Certificate of Compliance' process to non-financial systems.[29]

2.41 The Committee asked the ATO about ATO systems which had not been issued with certificates of compliance.[30]

2.42 In response, the ATO stated that it had been progressively examining all its financial systems and giving them certificates of compliance to ensure that the risks were being identified and appropriately managed.[31]

2.43 The Committee asked whether all systems would be subjected to certificate of compliance tests and what the time frame for the process would be.[32]

2.44 In its submission, the ATO replied that:

- certificates of compliance had been issued for all financial systems;
- when some of the financial systems were eventually decommissioned, they would become legacy[33] systems and fresh risk evaluations would need to be undertaken; and
- the ATO was yet to settle timeframes for issuing certificates for non-financial systems.[34]

Committee comment

2.45 The Committee agrees with the ANAO that there should be a certificate of compliance process for non-financial systems and expects the ATO's agreement to the ANAO's recommendation no. 5 to result in appropriate and timely implementation of such a process.

[28] ANAO, Audit Report No. 16, 2000-2001, p. 70.

[29] ANAO, Audit Report No. 16, 2000-2001, p. 71.

[30] *Transcript*, 2 May 2001, p. 10.

[31] Mulligan, *Transcript*, 2 May 2001, pp. 10-11.

[32] *Transcript*, 2 May 2001, p. 11.

[33] Systems no longer required because of tax reform or legislative change.

[34] ATO, Submission no. 5, pp. 3-4.

IT security

2.46 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, protection of the information contained in these IT systems has become increasingly difficult.[35]

2.47 The ATO is reliant on its IT systems for recording information and for supporting its revenue collection systems. The ATO network can be broadly categorised into two main areas: the mainframe environment and the Wide Area Network (WAN) environment.

2.48 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.

2.49 The WAN environment comprises a number of linked local area network (LANs) 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.[36]

Outsourcing risks

2.50 The ANAO has noted in previous audits since 1994-95 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.[37]

2.51 During the current 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. The ANAO considers that this is due to ATO contractor staff having limited exposure to

[35] ANAO, Audit Report No. 16, 2000-2001, p. 74.

[36] ANAO, Audit Report No. 16, 2000-2001, p. 76.

[37] ANAO, Audit Report No. 16, 2000-2001, p. 20.

ATO fraud prevention, education and awareness material and programs in comparison to ATO employees.

2.52 In addition, the ATO could not provide evidence to the ANAO that the IT Security Section had monitored outsourced contractors' activity to ensure compliance with taxpayer data security provisions of its IT outsourcing contracts.[38]

2.53 The Committee asked the ATO where taxpayer data resided within Electronic Data Systems (EDS), the outsourced service provider.[39]

2.54 The ATO replied that the data sat in the EDS Burwood centre in Sydney on a mainframe, access to which was specifically for ATO use:

> We access it, and our ATO systems use the data from that particular location in the country. The contract as it stands does not allow that data to leave Australia.[40]

2.55 The Committee inquired whether EDS staff performing work associated with taxpayer data worked exclusively on the ATO contract, or worked on a number of contracts.[41]

2.56 In response, the ATO stated that while the majority would work specifically to the ATO, there would be a range of people brought in to address particular issues who may move on to other work.[42]

2.57 The Committee sought advice from the ATO on the measures it was implementing to address the ATO's concerns that the integrity of the data and the risk of misuse had been increased as a result of the outsourcing of the IT function.[43]

2.58 The ATO replied that it had looked again at all its vetting processes and procedures for contractors and agreed that it needed to implement more monitoring elements. It also agreed that it needed to provide evidence of monitoring.[44]

[38] ANAO, Audit Report No. 16, 2000-2001, p. 20.

[39] *Transcript*, 2 May 2001, p. 6.

[40] J Growder, *Transcript*, 2 May 2001, p. 7.

[41] *Transcript*, 2 May 2001, p. 7.

[42] Growder, *Transcript*, 2 May 2001, p. 7.

[43] *Transcript*, 2 May 2001, p. 7.

[44] Growder, *Transcript*, 2 May 2001, pp.7- 8.

2.59 In response to a request by the Committee for comment on whether the risk had been alleviated by the measures being taken by the ATO, the ANAO stated:

> In this particular area, our report said that it was important that the ATO contractor staff have the same sort of exposure to the education and awareness material as the ATO runs for its own staff, so that they equally are aware of the importance and are conscious of security matters. We felt a little more had to be done there. Similarly, in the monitoring of contractor performance, we said that the ATO should focus on that as much as they focus on their own staff … We felt that the tax office needed to do a little more to recognise that the risks had changed and that there may be a need to be conscious, when they run these programs or do this monitoring for their own staff, that the contractors are included within that umbrella.[45]

2.60 The ANAO stressed that while some initial comfort might be taken from the fact that a substantial proportion of EDS staff were ex-ATO staff, it was not advisable to rely totally on that fact:

> The regime you put in place on the appointment of the outsourcer should obviously take account of the different risk profile.[46]

Committee comments

2.61 The Committee considers that when work is contracted out by an agency, the contractors' staff should be put through the same security checks as the agency's own staff and should have the same level of fraud awareness.

2.62 The Committee considers that the ATO must actively manage the risks of change, and should now have a higher awareness of what those risks are. As operations are streamlined and fewer staff are applied to a range of tasks, there is a need to understand what is happening to the risk and whether there is a need to compensate in any way.

[45] I McPhee, *Transcript*, 2 May 2001, p. 9.

[46] McPhee, *Transcript*, 2 May 2001, p. 9.

Firecall

2.63 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.[47]

2.64 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.[48]

2.65 The ATO advised the ANAO that it was in the process of introducing systems changes and revising its policies to restrict the use of *Firecall*.[49]

2.66 The ANAO's audit report gave details of ATO *Firecall* usage to August 2000. The Committee asked whether there had been any peaks is the use of *Firecall* since June 1999.[50]

2.67 The ATO reported that in recent discussions with the ATO, it had been suggested that there had been a peak at the beginning of 2001, and the ATO was investigating that issue.[51]

2.68 The Committee asked the ATO whether, on an ongoing basis, it planned to sample *Firecall* usage or review each use of *Firecall*.[52]

2.69 In reply, the ATO stated:

> We want to get to 100 per cent. We do have the data for 100 per cent. We are logging all accesses to Firecall, but we want to get to the point where we can look at each one of those to be totally satisfied in that regard.[53]

[47] ANAO, Audit Report No. 16, 2000-2001, p. 21.

[48] ANAO, Audit Report No. 16, 2000-2001, p. 21.

[49] ANAO, Audit Report No. 16, 2000-2001, p. 21.

[50] *Transcript*, 2 May 2001, p. 12.

[51] Growder, *Transcript*, 2 May 2001, p. 12.

[52] *Transcript*, 2 May 2001, p. 13.

[53] Growder, *Transcript*, 2 May 2001, p. 13.

2.70 The ATO confirmed that when *Firecall* access was used to keep the system running , it was generally EDS usage. There were particular instances when ATO staff used *Firecall*:

> Essentially, what we are talking about in the instances of ATO staff using Firecall are instances where production application systems have failed, aborted or broken down for whatever reason, mostly due to corrupt data, and Firecall is used with appropriate authorisation to remove the corrupt data and re-establish the production processing.[54]

Committee comments

2.71 The ANAO report noted that *Firecall* alter and update usage between December 1999 and January 2000 was 24 911. The ATO stated that this 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.* The ATO has acknowledged that inappropriate use of the *Firecall* facility has also been a contributing factor.[55] The ATO advised the Committee that expected use of *Firecall* would normally be in the range of 200 to 300 per month.[56]

2.72 The Committee understands that *Firecall* is a facility that provides a mechanism to bypass all security controls and provides a user with unrestricted access to everything on the mainframe computer.

2.73 While there are appropriate controls on *Firecall*, and uses are logged and have the capability to be monitored, the Committee considers that the reasons for the high levels of usage need to be addressed. It is not possible for high levels of usage to be actively monitored.

2.74 The Committee notes that the ATO is in the process of introducing systems' changes and revising its policies to restrict the use of *Firecall*.

[54] W Collins, *Transcript*, 2 May 2001, p. 14.

[55] ANAO, Audit Report No. 16, 2000-2001, pp. 86–87.

[56] M Hirschfeld, *Transcript*, 2 May 2001, p. 13.

2.75 The ATO should ensure that if staff or contractors currently using *Firecall* for certain purposes are provided with an alternative mode of access, the alternative access has adequate controls and is able to be properly monitored.