The Auditor-General
Audit Report No.44 2008–09
Performance Audit

Security Risk Management

Australian National Audit Office

ISSN 1036–7632

ISBN 0 642 81078 8

Australian National
Audit Office

Canberra ACT
23 June 2009

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken a performance audit across agencies in accordance with the authority contained in the *Auditor-General Act 1997*. I present the report of this audit and the accompanying brochure to the Parliament. The report is titled *Security Risk Management.*

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

Ian McPhee
Auditor-General

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

AUDITING FOR AUSTRALIA

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

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

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

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

http://www.anao.gov.au

Audit Team
Grace Guilfoyle
Rowena Hayman
Caroline Smith
Bill Bonney
Dr Paul Nicoll

Contents

Tables

Figures

Abbreviations

AGD	Attorney-General's Department
AGS	Australian Government Solicitor
AIHW	Australian Institute of Health and Welfare
ANAO	Australian National Audit Office
ASA	Agency Security Adviser
AusAID	Australian Agency for International Development
CAC Act	*Commonwealth Authorities and Companies Act 1997*
Finance	Department of Finance and Deregulation
FMA Act	*Financial Management and Accountability Act 1997*
ICT	Information and Communications Technology
PSM	Australian Government Protective Security Manual (2005)
Treasury	Department of the Treasury

Glossary

Agency Security Adviser	The person responsible for the day-to-day performance of the protective security functions within an organisation
Protective security	A broad concept covering information, personnel, and physical security
Security awareness	Understanding and appreciating potential risks and threats to, and the costs of, the loss or compromise of information or assets, and accepting the responsibilities and obligations to address those issues
Security classified information	Official information that must be afforded a level of protection to safeguard it from compromise or unauthorised use because such misuse could cause harm, or have adverse consequences
Security clearance process	The process of assessing individuals' eligibility and suitability for access to security classified information through a comprehensive evaluation of their history, attitudes, values and behaviour
Security Executive	The Senior Executive Service officer (or equivalent) responsible for protective security functions in an organisation
Security risk	An event that could result in the compromise of official resources, including personnel, measured in terms of its likelihood and consequences

Summary and Recommendations

Summary

Background

1. All Australian Government organisations face a range of security risks. These include risks that may affect:

- their reputation and/or that of the Australian Government;
- their performance against their outputs or the achievement of the Government's outcomes;
- the safety of their staff, customers and other stakeholders; and
- the integrity of their information and physical resources.

2. The creation and maintenance of a sound protective security environment provides assurance to the Parliament, Government, and others that organisations are well placed to reduce their exposure to such risks.

3. The Attorney-General's Department (AGD) is responsible for the development and dissemination of the Protective Security Manual (PSM). The PSM is the principal source of policy, associated guidance material and the minimum requirements or standards relating to the security of Australian Government organisations' information, assets and people.

4. The PSM requires organisations to design their protective security arrangements on the basis of risk management principles. In particular, the PSM states that organisations should develop a systematic and coordinated program for managing security-related risks, including processes for the ongoing monitoring of risk treatment controls. The manual contains a range of guidance material on the key elements of an effective security risk management process.

5. The preface to the PSM indicates that the PSM applies to:

- all agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act);
- those organisations subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) that have received notice (under that Act) from their responsible Minister that the manual applies to them.

6. AGD obtained advice from the Australian Government Solicitor (AGS) in January 2008 regarding the applicability of the PSM. The AGS advised that

CAC Act organisations are legally obliged to comply with the PSM when they are subject to notification by their responsible Minister that the PSM applies to them as a general policy of the Australian Government. AGS further advised that FMA Act and CAC Act organisations must comply with the PSM if their employees are engaged under the provisions of the *Public Service Act 1999* (PSA), as those employees are obliged to implement government policies. The AGD advised that it disseminated the advice to Agency Security Advisers (ASA) and security executives through the Protective Security Policy (PSP) website in June 2008, and maintains a copy on the new GovDex PSP website.

7. The preface of the PSM has not been updated to reflect amendments to the CAC Act in 2008 that changed the way in which general policies of the Australian Government (including the PSM) are applied to CAC Act organisations. As a result of these amendments the Finance Minister may issue General Policy Orders (GPO) specifying the general policies of the Australian Government to be applied by CAC Act organisations, rather than each organisation needing to be directed to comply by its responsible Minister.

Previous audit coverage

8. The Australian National Audit Office (ANAO) has undertaken nine previous cross-agency protective security audits. The AGD, which is responsible for promulgating Australian Government protective security policy, has indicated its support for the conduct of these audits and acknowledged their contribution to improving the management and delivery of protective security practices in the Australian Government sector. The current audit continues the ANAO's series of cross-agency protective security audits.

9. Previous audits have addressed aspects of security risk management practices. Overall, the findings of these audits suggested that Australian Government organisations have not paid sufficient attention to the ongoing management of security risks.

Audit approach

Audit objective and criteria

10. The objective of this audit was to assess whether selected organisations had effective security risk management programs, including whether a selection of protective security risk treatment controls was working as designed.

11. In order to address the audit objective, the ANAO assessed whether each organisation had:

- established and implemented effective arrangements for managing security risks;
- established sufficient and appropriate monitoring arrangements for security risks; and
- implemented effective security risk mitigation measures or treatment controls.

Audit scope, coverage and methodology

12. The protective security risk management arrangements at three Australian Government organisations were assessed against these audit criteria. The three organisations were the:

- Australian Agency for International Development (AusAID);
- Australian Institute of Health and Welfare (AIHW); and the
- Department of the Treasury (Treasury).

13. The audit did not extend to security risk management arrangements relating to overseas based personnel or operations. In addition, it did not examine security risk practices or controls relating specifically to information and communications technology (ICT).

14. Given their respective roles in the development of the PSM and the application of general policies of the Australian Government, the ANAO also sought responses from AGD and the Department of Finance and Deregulation.

Audit conclusion

15. Having a sound protective security environment is an important element in the management of an organisation's human, information and physical resources. A key element of an effective protective security environment is the identification and management of security related risks.

16. The PSM is the principal source of policy, associated guidance material and the minimum requirements or standards relating to the protective security of Australian Government organisations' information, assets and people. The principles and standards contained in the PSM provide organisations with a sound basis to assist in the identification and assessment of their security risks.

17. There is a risk that some CAC Act organisations which employ staff under the PSA are not aware of the legal advice from the AGS regarding the applicability of the PSM. The legal advice indicated that such organisations are obliged to comply with the PSM even if they have not been directed under the CAC Act to do so. There is also a lack of visibility concerning which CAC Act organisations have received a direction (from their responsible Minister) to apply the PSM.

18. The ANAO examined Treasury and AusAID which, as organisations subject to the FMA Act, are both required to comply with the PSM. Both organisations receive, produce, use and hold security classified information, and therefore require strong protective security measures to protect such information and the people who use it.

19. Overall, the audit concluded that Treasury and AusAID had established and implemented effective arrangements for managing security risks. In particular both organisations had:

- policies outlining arrangements for the management of security risks;
- senior management involvement in security risk management issues;
- clear roles, responsibilities and appropriate training for staff with security responsibilities; and
- established sufficient and appropriate arrangements for monitoring their security environments.

20. Both organisations had processes in place for identifying and analysing their security risks, although there was scope to improve the documentation supporting the work undertaken. In addition, there was no written record of senior management's acceptance or otherwise of the security risks identified in either organisation. Both organisations would also benefit from better integrating the consideration of security risks in corporate risk management and business planning activities.

21. The AIHW is an Australian Government statutory authority that operates under the provisions of the *Australian Institute of Health and Welfare Act 1987*. The AIHW is defined as a body corporate subject to the CAC Act and it has not been directed to comply with the PSM. The AIHW's enabling legislation does contain specific provisions requiring it to protect the confidentiality of the information provided to it. Further, the AIHW's employees are engaged under the PSA.

22. In light of the legal advice from AGS, it is likely that the AIHW should comply with the PSM. However, this position has not been made clear to the AIHW. In any event, the guidance and requirements of the PSM provide a sound basis for assessing whether its security practices are effectively contributing to the management and protection of its resources.

23. The audit concluded that the AIHW had not established practices for identifying and managing security risks that were sufficient and appropriate when measured against the principles and guidance provided in the PSM. However, at the time of the audit, the AIHW had a number of initiatives in place to bring its security risk management practices into line with the better practice principles in the PSM. In particular, the AIHW had recognised the need to strengthen its security risk management arrangements and, amongst other things, had developed a draft security policy and commenced developing a security awareness program. Nevertheless, at the time of the audit:

- the AIHW's Audit and Finance Committee advised the Board on issues relating to risk management but the Committee's reports to the Board did not specifically address security risk management;
- security roles had been assigned but not fully documented;
- an assessment of security risks had not been completed;
- a security plan outlining the AIHW's approach to the management of its security risks had not been developed; and
- security issues were not systematically linked with the AIHW's corporate risk management and business planning activities.

24. Each of the three audited organisations had developed a range of controls designed to reduce their security risks. Overall, the controls we examined were operating effectively although there were some shortcomings. These shortcomings included insufficient documentation to support decisions made in the conduct of security clearances and limited evidence of monitoring the performance of security-related contractors. The results of the audit indicated there was scope to improve the monitoring of such controls to help ensure they are operating effectively.

25. The results of this audit suggest that issues identified in previous protective security audits continue to be challenging for organisations. These issues include the integration of security risk management activities with organisations' broader risk management activities, and the monitoring of security risk treatments or controls.

26. The ANAO made one recommendation aimed at clarifying which CAC Act organisations are required to comply with the PSM. The ANAO made three further recommendations designed to improve organisations' management of protective security risks. These recommendations focused on security risk management processes, better integrating security risks into organisational risk management and planning activities and monitoring of the controls implemented to reduce security risks.

Key Findings by Chapter

Managing security risks (Chapter 2)

27. The PSM is the principal source of policy, associated guidance material and the minimum requirements or standards relating to the protective security of Australian Government organisations' information, assets and people.

28. There is a risk that some CAC Act organisations which employ staff under the PSA are not aware of the legal advice from the AGS regarding the applicability of the PSM in January 2008. The legal advice indicated that such organisations are obliged to comply with the PSM even if they have not been directed under the CAC Act to do so. Given this advice, it is likely that the AIHW should comply with the PSM. However, this position has not been made clear to the AIHW.

29. AGD advised that it does not maintain a record of those CAC Act organisations directed by Ministers to comply with the PSM. As a result, there is also a lack of visibility as to which CAC Act organisations have (or have not) received a direction (from their responsible Minister) to apply the PSM. Given the amendments to the CAC Act in 2008, it is opportune that AGD work with the Department of Finance and Deregulation (Finance) to address the issues surrounding the applicability of the PSM to CAC Act organisations.

30. To assess whether organisations are effectively managing security risks, we considered whether they had well-designed security risk management policies, an appropriate level of senior management involvement, clear roles and responsibilities and appropriate training for staff with security responsibilities. In addition, we assessed whether they had a systematic and coordinated security risk management process to identify, assess, treat and control protective security risks.

31. Of the three organisations audited, only AusAID had a separate security risk management policy. That policy provided detailed instructions for

AusAID's employees in the practical implementation of the security measures supporting the policy. At the time of the audit, the AIHW had a draft security policy. The ANAO considered that the focus of the proposed policy should be expanded to reflect other elements of protective security risks faced by the AIHW.

32. Treasury had developed a corporate risk management policy which provided the framework for all risk management activities in the department. Treasury's policy states that line managers throughout the department, including certain specialist areas, such as security, are responsible for undertaking risk assessment and reporting, and for maintaining current risk management plans.

33. Treasury and AusAID had clear reporting lines to and from their respective senior executives in relation to security risk matters. In particular, Treasury had established a security committee to coordinate protective security activities. At the AIHW, security risk management issues were raised with the Executive Committee as part of other risk management issues. A more targeted level of involvement by the AIHW's senior management in security risk matters would assist in achieving a more integrated approach to security risk management.

34. In Treasury and AusAID security team roles and responsibilities were well-defined and key security staff were either sufficiently trained or had suitable experience to undertake their duties. At the time of audit security roles had been assigned but not fully documented at the AIHW and training of all staff with specific security roles had not been completed.

35. Also, at the time of the audit, the AIHW had not completed an assessment of its security risks, nor developed a security risk register and security plan. While Treasury and AusAID had developed sound security risk management processes, there was scope for improvement in both organisations. In particular, neither had:

- appropriate managerial acceptance, or otherwise, of identified security risks; and
- developed a comprehensive risk register that reflected the key steps in their risk management process. In particular, the registers did not identify treatment priorities nor assign responsibility for the implementation and monitoring of risk reduction measures.

36. Treasury had developed a security plan that generally reflected the guidance contained in the PSM. By contrast, the security plans at AusAID did not contain many of the key elements of a security plan as described in the PSM.

37. The ANAO considers, as reflected in the PSM, that having security risks reflected in corporate risk management policies assists in promoting a stronger security culture. Specifically, organisations will be better placed to identify and deal with security issues when the management of security risks is integrated, or aligned, with the organisation's broader risk management and planning processes.

38. In AusAID and the AIHW security issues were not systematically linked with corporate risk management and business planning activities. Treasury's risk management policy indicated that, as part of operational planning, groups/divisions must complete an assessment of risks relevant to their areas of operation. Our audit indicated, however, that security risks were generally not explicitly considered in the identification of risks in Treasury's group or divisional operational plans.

Monitoring and review (Chapter 3)

39. Organisations that monitor security risks and changes in their risk environment are better placed to detect events that may alter their risk management priorities. The ANAO noted that Treasury and AusAID monitored their security environments. On the other hand, the AIHW's monitoring of its general risk environment did not include a separate structured consideration of security risks.

Each of the audited organisations has implemented controls designed to reduce their security risks. Our examination of selected controls indicated that they generally operated as intended. However, the results also indicated that there was scope to improve ongoing monitoring of those controls used to reduce identified security risks at each of the audited organisations. In particular, the main issues identified were that:

- sufficient information was not available in all cases to fully support decisions made to grant or deny a security clearance (AusAID);
- the effective date of clearances was often backdated prior to the date of the delegate's approval of the clearance (AusAID); and

- there was no evidence of regular and formal monitoring taking place in relation to important security services contracts (AusAID and Treasury).

Summary of organisations' responses to the audit

40. The AGD, Finance and each of the audited organisations agreed with the recommendations in this report. The organisations' responses to each of the recommendations are shown in the body of the report. Organisations' general comments are shown at Appendix 2.

Recommendations

The first recommendation is directed at the Attorney-General's Department and the Department of Finance and Deregulation given their respective roles in the development of the PSM and the application of general policies of the Australian Government.

The remaining recommendations are based on findings from fieldwork at the selected organisations and are likely to be relevant to other Australian Government organisations. Therefore, all Australian Government organisations are encouraged to assess the benefits of implementing these recommendations in light of their own circumstances, including the extent to which each recommendation, or part thereof, is addressed by practices already in place.

Recommendation No.1

Para 2.20

The ANAO recommends that AGD, given its role in developing and promulgating protective security policy, work with Finance to clarify to which CAC Act organisations the PSM applies.

Recommendation No.2

Para. 2.70

The ANAO recommends that Australian Government organisations adopt a systematic and coordinated security risk management process, including documenting the identification, analysis, evaluation and treatment of security risks in a security risk register that is endorsed by the organisation's senior management.

Recommendation No.3

Para. 2.82

The ANAO recommends that organisations establish mechanisms to ensure that security risks are integrated, as appropriate, into broader corporate risk management and business planning activities.

Recommendation No.4

Para. 3.39

The ANAO recommends that organisations periodically assess whether controls designed to reduce security risks are operating effectively and remain appropriate.

Audit Findings and Conclusions

1. Introduction

This chapter provides background information about the audit, including an overview of protective security risk management requirements.

Introduction

1.1 Australian Government organisations face a range of security risks. These include risks that may affect their reputations, their ability to achieve their objectives, and the safety of their staff and other stakeholders. In order to reduce their exposure to such risks, organisations need to create and maintain a sound protective security environment. Protective security arrangements are usually a combination of physical, personnel, information, and information and communications technology (ICT) security measures.

The Protective Security Manual

1.2 Effective protective security arrangements are central to the protection of the Australian Government's official resources The Attorney-General's Department (AGD) is responsible for the development and dissemination of the Protective Security Manual (PSM).[1] The PSM is designed to assist Australian Government organisations in the design and implementation of their protective security arrangements. Specifically, the PSM is the principal source of policy, associated guidance material and the minimum requirements or standards relating to the security of Australian Government organisations' information, assets and people. The PSM was first published in January 1991 and has been revised and re-released twice, in October 2000 and August 2005.

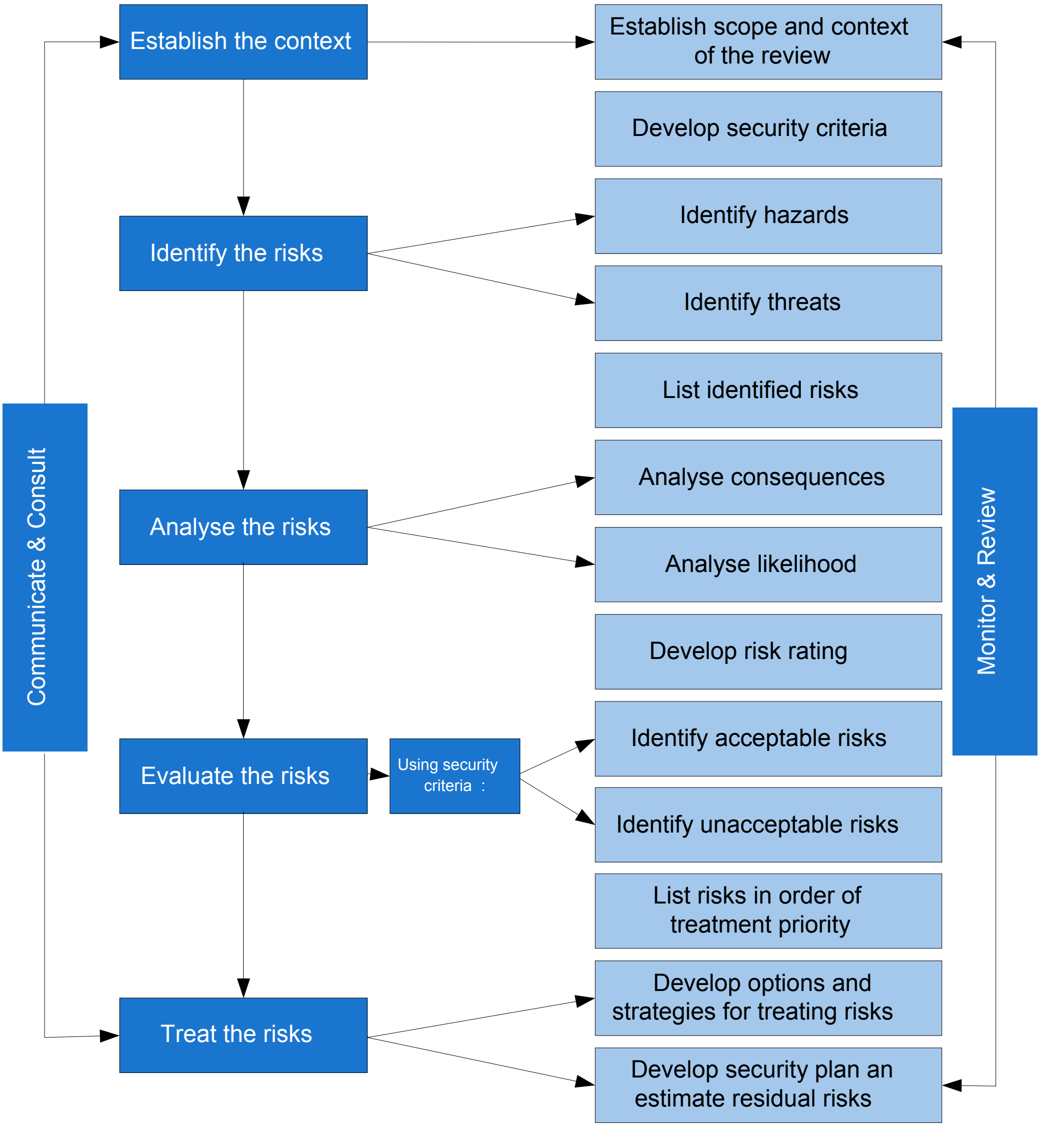
1.3 The PSM requires organisations to design their protective security arrangements on the basis of risk management principles. In particular, Part B of the PSM states that organisations should adopt a systematic and coordinated risk management program to identify, assess, evaluate and treat their protective security risks. In addition, Part B of the manual states that organisations should regularly monitor their security risks and the controls which have been implemented to manage those risks.

[1] Attorney-General's Department, *Protective Security Manual*, Canberra, August 2005. The Manual is issued to all Australian Government organisations. Further information regarding the Manual is available at:<http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005)> [Accessed on 9 April 2009].

1.4 Figure 1.1 illustrates key elements of the security risk management process as set out in Part B of the PSM.

Figure 1.1

Security Risk Management Process


Establish the context
Identify the risks
Analyse the risks
Evaluate the risks
Using security criteria :
Treat the risks
Communicate & Consult
Monitor & Review
Establish scope and context of the review
Develop security criteria
Identify hazards
Identify threats
List identified risks
Analyse consequences
Analyse likelihood
Develop risk rating
Identify acceptable risks
Identify unacceptable risks
List risks in order of treatment priority
Develop options and strategies for treating risks
Develop security plan an estimate residual risks

Source: ANAO based on the Australian Government Protective Security Manual (PSM) 2005. p. B7.

Previous audit coverage of protective security risk management

1.5 The Australian National Audit Office (ANAO) has undertaken nine previous cross-agency protective security audits.[2] The AGD, which is responsible for promulgating Australian Government protective security policy, has indicated its support for the conduct of these audits and acknowledged their contribution to improving the management and delivery of protective security practices in the Australian Government sector. The current audit continues the ANAO's series of cross-agency protective security audits.

1.6 Five of these previous audits have addressed aspects of security risk management practices. Overall, the findings of these audits suggested that Australian Government organisations have not paid sufficient attention to the ongoing management of security risks. In particular, while most organisations audited have assessed their security risks, these details were not always kept up-to-date. Additionally, although many organisations had developed plans to help manage their security risks, including setting-out arrangements for monitoring risk treatments or controls, these plans were not always properly implemented or adhered to.

1.7 As well as these issues, our audits have identified the following shortcomings in relation to security risk management activities:

- security risk assessments not well integrated with or linked to corporate risk management activity;
- processes for identifying new and emerging risks being informal and unstructured; and
- security risk assessments not covering all dimensions of protective security.

[2] Following a recommendation from the 1979 *Inquiry into Protective Security*, undertaken by Mr Justice Hope, the ANAO commenced a program of audits to evaluate protective security arrangements in Australian Government organisations. In the majority of cases, these audits were conducted and reported on an individual basis (that is, independently from each other). In 1995, the ANAO included protective security audits in its cross-agency general performance audit program. Appendix 1 lists the earlier protective security audits undertaken by the ANAO.

Current audit

Audit objective and criteria

1.8 The objective of this audit was to assess whether selected organisations had effective security risk management programs, including whether a selection of protective security risk treatment controls was working as designed.

1.9 In order to address the audit objective, the ANAO assessed whether each organisation had:

- established and implemented effective arrangements for managing security risks;
- established sufficient and appropriate monitoring arrangements for security risks; and
- implemented effective security risk mitigation measures or treatment controls.

Audit scope, coverage and methodology

1.10 The protective security risk management arrangements at three Australian Government organisations were assessed against the audit criteria listed in paragraph 1.9. The three organisations were the:

- Australian Agency for International Development (AusAID);
- Australian Institute of Health and Welfare (AIHW); and the
- Department of the Treasury (Treasury).

1.11 The audit did not extend to security risk management arrangements relating to overseas based personnel or operations. In addition, we did not examine security risk practices or controls relating specifically to ICT.

1.12 The ANAO held interviews with key staff at these organisations and reviewed relevant documentation, including security risk management policies and guidance material, security risk assessments, security plans, records of security incidents, security awareness and training programs, and management reports that outlined the monitoring and performance of protective security risk management activities. In addition, we tested the operation of selected security risk treatments and controls.

1.13 Given their respective roles in the development of the PSM and the application of general policies of the Australian Government, the ANAO also sought responses from AGD and the Department of Finance and Deregulation.

1.14 The audit was conducted in accordance with ANAO's Auditing Standards at a cost of $430 000.

Audit reporting and structure

1.15 This audit is part of a program of cross-agency performance audits that examines business processes which support the delivery of services provided by Australian Government organisations. These audits are conducted under the provisions of section 18 of the *Auditor-General Act 1997*, which provides for the examination of a particular aspect of the operations of the whole or part of the Australian Government sector. Accordingly, the findings discussed in this report are based on the fieldwork at the three audited organisations.

1.16 Three of the four audit recommendations are framed to have general application to all Australian Government organisations. The other recommendation is directed at the AGD and the Department of Finance and Deregulation.

1.17 As well as this introductory chapter, this report contains the following chapters:

- Managing security risks (Chapter 2); and
- Monitoring and review (Chapter 3).

1.18 Appendix 2 provides comments from AGD, the Department of Finance and Deregulation and each of the audited organisations on the draft audit report.

2. Managing security risks

This chapter addresses the applicability of the Protective Security Manual and the establishment and implementation of effective arrangements for managing security risks.

Introduction

> Risk management is the culture, process and structures that are directed towards realising potential opportunities whilst managing adverse effects. It involves establishing the context, identifying, analysing, evaluating, treating, communicating, monitoring and reviewing risk. Everyone managing official resources must adopt approaches that keep risks within acceptable bounds, and determine what resources are necessary to achieve this.[3]

2.1 All Australian Government organisations face a range of common security risks. These include risks that may affect:

- their reputation and/or that of the Australian Government or their respective Minister;
- their performance against their outputs or the achievement of the Government's outcomes;
- the safety of their staff, customers and other stakeholders; and
- the integrity of their information and physical resources.

2.2 The creation and maintenance of a sound protective security environment provides assurance to the Parliament, Government, and others, that organisations are well placed to reduce their exposure to such risks. A key element of an effective protective security environment is the identification and management of security related risks. All organisations should, as a minimum, identify their key security risks and develop appropriate protective security arrangements to manage those risks.

2.3 Ultimately, the responsibility for the development, implementation and maintenance of effective protective security functions lies with the Chief Executive of each government organisation. In practice in most organisations,

[3] *Protective Security Manual, 2005*, op.cit, p B5.

this responsibility is exercised by a Security Executive, supported by the Agency Security Adviser (ASA).

2.4 The PSM is the principal source of policy, associated guidance material and the minimum requirements or standards relating to the security of Australian Government organisations' information, assets and people. The principles and standards contained in the PSM provide organisations with a sound basis to assist in the identification and assessment of their security risks. AGD is responsible for developing and disseminating the PSM.

2.5 The Department of Finance and Deregulation has indicated that the PSM is a general policy of the Australian Government.[4] A general policy of the Australian Government is any policy made by the Government that is relevant and capable of being applied to all, or most, FMA and CAC Act organisations.

Applicability of the Protective Security Manual

2.6 The preface to the PSM indicates that the PSM applies to:

- all agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act);
- those organisations subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) that have received notice (under that Act) from their responsible Minister that the manual applies to them.

2.7 Treasury and AusAID are subject to the FMA Act and therefore it is clear they are both required to comply with the PSM.

2.8 The AIHW is an Australian Government statutory authority that operates under the provisions of the *Australian Institute of Health and Welfare Act 1987*. The AIHW is defined as a body corporate subject to the CAC Act and it has not been directed to comply with the PSM. The AIHW's enabling legislation does contain specific provisions[5] requiring it to protect the confidentiality of the information provided to it.

2.9 AGD obtained advice from the Australian Government Solicitor (AGS) in January 2008 regarding the applicability of the PSM. The AGS advised that

[4] Draft Finance Circular titled *Application of general policies of the Australian Government to bodies subject to the CAC Act – General Policy Orders*.

[5] *Australian Institute of Health and Welfare Act 1987*, section 29.

CAC Act organisations are legally obliged[6] to comply with the PSM when they are subject to notification by their responsible Minister, under (the former) sections 28 or 43 of the CAC Act, that the PSM applies to them as a general policy of the Australian Government. AGS further advised that FMA Act and CAC Act organisations must comply with the PSM if their employees are engaged under the provisions of the *Public Service Act 1999* (PSA), as those employees are obliged to implement government policies[7].

2.10 AGD advised that it disseminated the advice to ASAs and security executives through the Protective Security Policy (PSP) website in June 2008. The PSP site ceased being updated on 31 January 2009 and all content, including a copy of the legal advice, was transferred to the new GovDex PSP website[8].

2.11 AGD advised that it does not maintain a record of those CAC Act organisations directed by Ministers to comply with the PSM. However, through its advisory and monitoring activities, it has identified that approximately 30 CAC Act organisations have not received a Ministerial Direction to apply Australian Government general policies, including the PSM. In addition, AGD was unsure whether the responsible Ministers had directed a further 12 CAC Act organisations to adhere to the requirements PSM.

2.12 Of the approximately 30 CAC Act organisations AGD advised have not been directed to comply with the PSM, the ANAO notes there is a small number of organisations, including the AIHW, which employ staff under the provisions of the PSA Act. These organisations are described as statutory agencies for the purposes of the PSA Act.

2.13 There is a risk that some of these CAC Act organisations are not aware of the legal advice from the AGS that indicates that such organisations are obliged to comply with the PSM even if they have not been directed under the

[6] The legal opinion also provided advice in relation to the applicability of the PSM to other types of organisations mentioned in the preface to the PSM.

[7] By virtue of a combined reading of subsection 13 (11) which requires APS employees to uphold the APS Values and paragraph 10 (1) (f) which refers to the requirement to implement the Government's policies.

[8] govdex.gov.au is administered by the Australian Government Information Management Office (AGIMO) within the Department of Finance and Deregulation. GovDex provides a secure internet based space for government agencies to manage stakeholders and projects, deliver information in one central location and use a collaborative workspace for file and document sharing, meeting management and centralised information and contact management.

CAC Act to do so. There is also a lack of visibility as to which CAC Act organisations have received a direction (from their responsible Minister) to apply the PSM.

2.14 Given this advice it is likely that the AIHW should comply with the PSM. However, this position has not been made clear to the AIHW. In any event the guidance and requirements of the PSM provide a sound basis to assess whether its security practices are effectively contributing to the management and protection of its resources. In addition, applying the principles of the PSM will better enable the AIHW to meet the confidentiality requirements in its enabling legislation.

2.15 The preface to the PSM has not been updated to reflect amendments to the CAC Act (which commenced on 1 July 2008). These amendments changed the way in which general policies of the Australian Government (including the PSM) are applied to CAC Act organisations. In short, as a result of these amendments:

- the Finance Minister may issue General Policy Orders (GPO) specifying the general policies of the Australian Government to be applied by CAC Act organisations; and
- CAC Act organisations are required to comply with these GPOs (unless specifically exempted) - rather than each organisation needing to be directed to comply by their responsible Minister.

2.16 In January 2009, the Department of Finance and Deregulation released a draft Finance Circular to provide information on the effect of these amendments. This draft circular replaces Finance Circular 2005/04 - *Application of general policies of the Australian Government to bodies under the Commonwealth Authorities and Companies Act 1997*, which has been withdrawn.

2.17 The draft circular indicates that the Finance Minister will issue GPOs at the request of the relevant policy Minister. The draft circular also states that the relevant policy Minister is the Minister responsible for developing and administering the general policy. In addition, the policy Minister is responsible for ensuring consultation with other relevant Ministers to obtain their views on the proposed application of the general policy. In the case of the PSM, the relevant policy Minister is the Attorney-General.

2.18 The draft circular also states that any directions to follow the general policies of the Australian Government issued prior to the amendments (that is issued prior to 1 July 2008) remain in-force unless the Finance Minister determines otherwise. Finance has advised that, as at 30 April 2009, the Finance Minister has not issued any GPOs nor made any determinations relating to existing directions.

2.19 Given the amendments to the CAC Act in 2008 and the draft advice from Finance relating to the application of general policies of the Australian Government to CAC Act organisations, the ANAO considers it is opportune that AGD work with Finance to address the issue surrounding the applicability of the PSM to CAC Act organisations.

Recommendation No.1

2.20 The ANAO recommends that AGD, given its role in developing and promulgating protective security policy, work with Finance to clarify to which CAC Act organisations the PSM applies.

Organisations' responses to the recommendation

Attorney-General's Department

Agreed. Once AGD meets with Finance further advice may be sought from the Australian Government Solicitor, given the changes to the CAC Act.

AGD will , in collaboration with Finance, update advice on the applicability of the PSM to CAC Act bodies.

Department of Finance and Deregulation

Agreed.

2.21 It is also suggested that the preface to the PSM be amended to clearly identify to which organisations the PSM applies. Irrespective of whether Australian Government organisations are required to comply with the PSM, they all have a responsibility to ensure security risks are effectively managed in light of their particular circumstances. The security arrangements organisations require will vary depending on such considerations as the nature and extent of their operations and the specific physical, information and personnel security risks faced. The guidance and better practice principles contained in the PSM provide organisations with a sound framework for managing their security risks.

Security risk profiles of the audited organisations

2.22 Although the three audited organisations shared these common security risks, their individual risk profiles varied.

2.23 At 30 June 2008, Treasury had approximately 940 staff.[9] Treasury provides advice to the Australian Government on such issues as the macroeconomic environment, public and private sector expenditure, taxation and financial markets. Treasury works closely with other Australian Government organisations, professional organisations, industry groups as well as participating in multilateral, bilateral and regional engagements.

2.24 AusAID manages Australia's overseas aid program and provides advice and support to its Minister on development policy, and it plans and coordinates poverty reduction activities in partnership with developing countries. It had approximately 655 staff at 30 June 2008.[10]

2.25 Both Treasury and AusAID often receive, produce, use and hold national security and non-national security classified information in order to fulfil the roles for which they were established. Consequently, both organisations require protective security measures that reflect the more-significant risks and consequences arising from the loss or compromise of such information.

2.26 The AIHW is smaller, with a staff of approximately 250 at 30 June 2008.[11] The AIHW works with Australian Government, State and Territory health and community services departments, and with peak non-government organisations to collect and report health and welfare statistics. Typically, the AIHW neither uses nor requires access to national security information. In addition, any non-national information it uses is generally at a lower-level of security classification than the information holdings at Treasury and AusAID. As mentioned, the AIHW's enabling legislation contains specific provisions[12] requiring it to protect the confidentiality of the information provided to it.

2.27 In this part of the audit the ANAO examined the extent to which the audited organisations had established sound protective security risk management arrangements by assessing whether each organisation:

[9] *Treasury Annual Report 2007-2008*, p 144. This publication is available at <http://www.treasury.gov.au/documents/1430/PDF/04_Part_3_Management_and_Accountability.pdf> [accessed on 9 April 2009].

[10] *AusAID Annual Report 2007-2008*, p. 264. This publication is available at <http://www.ausaid.gov.au/anrep/rep08/pdf/anrep07_08section5.pdf> [accessed on 9 April 2009].

[11] *AIHW Annual Report 2007-2008*, p 118. This publication is available at <http://www.aihw.gov.au/publications/aus/ar07-08/ar07-08-c04.pdf> [accessed on 9 April 2009].

[12] *Australian Institute of Health and Welfare Act 1987*, section 29.

- had a security risk management policy in place;
- regularly communicated security risk management issues to senior management;
- clearly outlined the roles of staff with designated security responsibilities and ensured these staff are sufficiently trained;
- established a systematic and coordinated approach to identify, assess, treat and control their protective security risks;
- had developed a security plan; and
- had integrated security risk management into corporate risk management activities

2.28 The findings against each of these issues are outlined below.

Security risk management policy

> Good security risk management is based on a clear understanding of the aims, functions and goals of the agency. The most important tool for developing and gaining support for effectively managing security risk is a clear understanding of what is to be achieved as well as how and why, and who is to be responsible. The agency's senior management needs to have considered the outcomes an appropriate security environment will deliver. These should form the basis of the agency security policy.[13]

2.29 All organisations should have a security risk management policy that articulates their security objectives. A well-designed security risk management policy is a key source of information and instruction for staff in the performance of their respective roles and responsibilities. In particular, such a policy will assist organisations to establish consistent standards across their operations in order to minimise security risks.

2.30 The ANAO assessed if each of the audited organisations had established policies in relation to security risk management. Only AusAID had a separate security risk management policy in place. At the time of the audit, the AIHW had a draft security policy. Treasury did not have a specific security risk management policy. Rather it had developed a corporate risk management policy which provided the framework for all risk management activities in the department.

[13] *Protective Security Manual*, 2005, op.cit, p B2.

2.31 AusAID's security policy was current, had been endorsed by its Chief Executive and defined the organisation's objectives and rationale for managing security risk. It also provided detailed instructions for AusAID employees in the practical implementation of the security measures that supported the policy.

2.32 The AIHW's draft security policy largely focused on data access and information privacy issues. In particular, the draft policy proposes a framework based on the requirements of the Australian Government Information and Communications Technology Security Manual (ACSI 33).[14] ACSI 33 provides policies and guidance for Australian Government organisations on the protection of their ICT systems.

2.33 While this framework is consistent with the AIHW's need to maintain the confidentiality of the information it holds, the ANAO considers that the focus of the policy should be expanded to reflect other elements of protective security risks. For example, the policy could address the AIHW's management of physical and personnel security risks and associated issues.

2.34 Treasury's corporate risk management policy sets out the overarching risk management framework for the department and states that there are a number of existing areas of Treasury (such as security) that employ formal risk management strategies. The policy provides guidance on the analysis of risks and opportunities as well as setting out Treasury's definitions of likelihood and consequence ratings. It also states that line managers throughout the department, including certain specialist areas, such as security, are responsible for undertaking risk assessment and reporting, and maintaining current risk management plans.

Communication with senior management

2.35 The achievement of an integrated security risk management approach and culture requires strong direction, leadership and commitment from the head of the organisation as well as senior management. In order to support senior managers in this role, clear and effective communication is needed to ensure they are able to gain sufficient assurance in relation to security risk management issues, including security risk exposures affecting the entire organisation.

[14] ACSI 33 is available at <http://www.dsd.gov.au/library/infosec/ism.html> [Accessed on 16 April 2009].

2.36 The ANAO assessed the extent to which each of the audited organisations communicated security risk management issues to senior management.

2.37 Treasury and AusAID have established clear reporting lines to and from their Senior Executive in relation to security risk matters. In this regard, a key element of senior management's engagement at Treasury is its Security Committee. Establishment of a security committee, where it is cost effective, is an important means of promoting greater control and coordination of protective security activities.

2.38 The terms of reference of Treasury's Security Committee state that:

> The Security Committee of Treasury's role is to provide advice to the Executive in exercising their obligations for maintaining a secure environment. The Committee is to function as a forum of review of security issues and to advise the Executive Board on these issues and where possible considered recommendations. The Committee will seek to:
>
> - provide sound advice on matters of physical, personnel, information, communication and IT security; and
> - identify and address whole of Treasury security issues.

2.39 The Security Committee meets twice a year with ad-hoc meetings held in between should an urgent issue arise. Membership of the Committee comprises representation from across relevant areas of the Department, such as Information and Communications Technology (ICT) Security, Information Management and the Security Team.

2.40 In addition to the work of the Security Committee, following its monthly meeting, Treasury's Executive Board communicates details of important issues that it has discussed to staff. The ANAO noted examples of security-related matters being advised to staff, including information on enhanced security awareness training requirements and strengthened requirements regarding the wearing of identification passes.

2.41 AusAID senior management is provided with a weekly report on the status of important priorities and projects including on security issues. In addition, the security section provides a monthly report to the Executive highlighting key security issues. These reports are largely focused on overseas security matters and to a lesser extent on domestic security. AusAID's more significant risks relate to its overseas operations and that this is reflected in its management reporting. The ASA also reports at executive meetings on a monthly basis.

2.42 Security risk management issues are raised with the AIHW's Executive Committee as part of other risk management issues. In addition, although the AIHW's Audit and Finance Committee advised the Board on issues relating to risk management, the ANAO noted that the Committee's reports to the Board did not specifically address security risk management.

2.43 Given its size and lower risk profile, it reasonable that the AIHW's senior management is less actively involved in protective security risk management issues than the senior management of Treasury and AusAID. A more targeted level of involvement by the AIHW's senior management in security risk matters would assist in achieving a more integrated approach to security risk management. The AIHW has advised that the regular review of risks, including security risks, has now been introduced as a regular agenda item for meetings of its Board, Audit and Finance Committee and Executive Committee.

Clarity of security-related roles and responsibilities, and sufficiency of training

2.44 An important element in the management of security risks is ensuring that designated security roles and responsibilities are clear and that security staff are sufficiently trained to enable them to perform their roles effectively.

2.45 The ANAO assessed whether each of the audited organisations clearly documented the roles and responsibilities for key staff with designated security responsibilities, and that these staff were trained in security risk management. For the purpose of the audit key staff were the ASA, the assistant ASA (or equivalent) and the Security Executive.[15]

2.46 The ANAO examined the job descriptions of those staff with designated security responsibilities. Based on our analysis, the ANAO considers the security team roles and responsibilities are well-defined in Treasury and AusAID. In particular, at both organisations, staff roles are documented in their respective security plans. While the roles and responsibilities of key security staff are clearly outlined, the ANAO considers greater staff awareness

[15] The terms 'Agency Security Adviser' and 'Security Executive' are defined in the Glossary.

could be achieved if these roles and responsibilities were further promoted throughout each organisation.

2.47 At the time of audit, security roles had been assigned but not fully documented at the AIHW. With the exception of the Information and Communications Technology Security Adviser (ICTSA), none of the security related position profiles, including those for the Security Executive/ASA, mentioned their security management responsibilities.

2.48 Organisations will benefit when the ASA (or equivalent position) has security qualifications or receives training to assist them in their duties. The ANAO examined the qualifications and details of relevant training courses attended by the key security staff in each organisation. Overall, the ANAO considered that the key security staff in Treasury and AusAID were either sufficiently trained in, or had relevant experience to undertake their role.

2.49 At the AIHW, with the exception of the ICTSA, none of the staff with security responsibilities had received formal training in security risk management. These staff included the ASA. The AIHW advised that following completion of its review of security responsibilities, those staff with designated security responsibilities will be given relevant training

2.50 The ANAO was advised that none of the Security Executives at the audited organisations had received any specific training in relation to their role. The ANAO considers that each organisation should consider the training or awareness sessions that would be appropriate for this position given the organisation's security risks. The AGD offers a half day *Protective Security Seminar*[16] aimed at Security Executives. The seminar is designed to provide participants with an understanding of their roles and responsibilities in the creation and maintenance of an appropriate security environment.

Security risk management processes

2.51 The PSM states that organisations adopt a systematic and coordinated risk management program in order to efficiently and effectively identify,

[16] See, <http://www.ag.gov.au/www/agd.nsf/Page/Securitytraining_Courses_SeniorProtectiveSecuritySeminar> [accessed 16 April 2009].

assess, treat and control their protective security risks. A typical security risk management process has the following key steps:[17]

- communicate and consult;
- establish the context;
- identification and analysis of risks; and
- evaluation and treatment of risks.

2.52 As shown in Table 2.1 the PSM provides guidance for each of these steps.

Table 2.1

Guidance on the Security Risk Management Process

Step	Description based on PSM
Communicate and consult	Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process …The communications plan should address issues relating to the risk itself and the process to manage it… To maintain the engagement of stakeholders and enhance the chances of delivering a successful outcome, consultation needs to take place at every step of the process (PSM 2005 p. B6).
Establish the context	The purpose of conducting a security review is to help the agency's senior management make decisions about the level of risk it is prepared to accept and the resources required for treating risk. Therefore, each element of the agency must be considered in terms of how it contributes to the agency's goals, objectives, values, policies and strategies (PSM 2005 p. B8).
Identification and analysis of risk	Identify risks to the agency and its official resources by identifying the nature and source of the harm that could occur to its key functions and valuable resources. Potential harm is evaluated after considering exposure to threats and hazards. Each identified security risk should be analysed to determine how significant the potential risk is to the agency. The analysis usually results in each risk being given a risk rating (PSM 2005 p. B10-12).
Evaluation and treatment of risk	Once risks have been rated, agency management must decide which risks are unacceptable without new or additional treatments…A list of risks in order of treatment priority should be compiled for management approval. Management will be able to use this document to make decisions about treatments and the priority of treatments (PSM 2005 p. B14-16).

Source: Australian Government Protective Security Manual, 2005 section B pages B6 -16.

[17] Another key element of the security risk management process, monitoring and review, is addressed in Chapter 3.

2.53 Organisations benefit by documenting key elements of this process and using the results as the basis for establishing an organisational risk register and security plan.

2.54 The ANAO examined the security risk management processes at each of the audited organisations. At the time of the audit, the AIHW had recognised the need to strengthen its security risk management arrangements in line with the better practice principles in the PSM. The AIHW advised that work in relation to the security risk management process was in progress and was estimated to be completed around December 2009. Therefore the remainder of this chapter discusses the detailed findings and opportunities for improvement identified from the ANAO's examination of security risk management processes at Treasury and AusAID.

Communicate and consult

2.55 Treasury did not have a communications plan. Treasury's corporate risk management policy defined the importance of communication and consultation with stakeholders. It also stated that a communication plan will be developed to help ensure that risk management issues are addressed as part of its planning, evaluation, monitoring and reporting processes. At the time of the audit this plan was still to be developed.

2.56 AusAID established a draft internal communication plan that covered a six month period ending March 2008. This plan provided a framework for communicating security related policy and initiatives. The plan was designed to inform staff and contractors of their role in AusAID's international and domestic security measures and procedures and create a well informed and responsive attitude toward security awareness.

2.57 While the plan defined the importance of communication, it did not refer to communication with external stakeholders such as police or specialist security organisations or contractors, who could be expected to provide information that would assist in the identification and analysis of risks. In late 2008 AusAID advised the ANAO that it considered this document to be operational, although there was no evidence that the draft plan was endorsed by the organisation's senior management.

2.58 The ANAO considers that both organisations should finalise and endorse a communications strategy as effective consultation will better inform the risk identification and analysis process and help ensure that treatment priorities are consistent with management guidelines.

2.59 The risk reviews at both AusAID and Treasury indicated that the reviews had included consultation with a range of relevant staff. In addition AusAID's risk review included consultation with its security contractors. However, neither organisation was able to provide any record of consultation taking place.

Establish the context

2.60 The importance of establishing the context is set out in Treasury's corporate risk policy and security plan and in AusAID's *Security Policies and Procedures*. The ANAO considered that both Treasury and AusAID had soundly established the context for their respective security risk reviews.

Identification and analysis of risk

2.61 Treasury and AusAID have both outsourced the conduct of security risk reviews. In Treasury the review included a threat assessment, analysis of security risks and made 23 recommendations for improvement. In AusAID the review made 27 recommendations for improvement, and it also included the development of security plans for its two main Canberra premises.

2.62 The ANAO evaluated each organisation's progress in implementing selected recommendations from the respective security risk reviews.[18] Overall, while there was no evidence that the organisations had developed formal implementation plans, they had each taken steps to address the recommendations. There was also evidence that senior management at both organisations had approved the implementation of measures addressing some of the recommendations. However, there was no written record of endorsement of the respective reviews, including the acceptance or otherwise of the risks (and recommendations) identified.[19]

2.63 The risk assessments of Treasury and AusAID identified a number of security risks to their respective premises. In both organisations the identification and analysis of risk were based on :

- each organisation's main security threats (for example, terrorism, crime, loss of reputation);

[18] Progress in addressing recommendations associated with physical security and emergency response arrangements were not examined as they were outside the scope of this audit.

[19] A key element of the recommendations at both agencies related to enhancing the level of security awareness amongst staff. This issue is discussed in Chapter 3 of this report.

- consultation with staff; and
- physical security site inspections.

2.64 Overall, the ANAO considered that the identification and analysis of risk undertaken as part of these risks review was consistent with the principles outlined in the PSM. In particular, the likelihood of each risk occurring and the consequence of each risk were assessed and recorded. In addition, the controls already in place to reduce the likelihood and/or consequence of each risk were also identified. Finally, each risk factor was given an overall rating, for example, high, medium or low.

Evaluation and treatment of risks

2.65 The security risk reviews at both Treasury and AusAID identified a number of additional, or enhancements to, existing treatments to address residual risks.[20] However, neither organisation had identified the priorities for implementing these treatment options. The ANAO recognises that as the risk reviews were outsourced it would not be expected that this prioritisation would be part of the risk review; rather this is a management function. The ANAO considers it is important that senior management document their endorsement of the identified risks, and their decisions in relation to unacceptable risks. In addition the priorities given to the implementation of any new risk treatments should be documented.

Risk register

2.66 The PSM states that the most effective way of documenting the results of the security risk management process is to produce a Risk Register. In particular, documenting the identification, analysis, evaluation and treatment of security risk will better assist management to make informed decisions on protective security risk management. Neither Treasury and AusAID had comprehensive security risk registers.

2.67 Treasury developed a *Security Risk Management Register* and *Treasury Risk Treatment Register* to assist in managing the implementation of the recommendations contained in its protective security risk review. However, these registers did not address all of the elements of the recommendations contained in the report of the review. In addition, these risk registers did not

[20] Residual risk is the remaining level of risk after risk treatments already in place have been taken into account. The estimated level of residual risk can be used as a guide for determining additional risk treatment priorities.

contain the analysis of likelihood and consequence for each identified risk from the outsourced risk review, treatment priorities or assign responsibility for the implementation and monitoring of risk reduction measures.

2.68 AusAID advised that it had not developed a security risk register, but relied on the risk registers produced as part of the risk review. It was unable to provide evidence that management had reviewed or accepted these risk registers. Further, the ANAO noted that the registers produced as part of AusAID's security risk review did not identify treatment priorities or assign responsibility for the implementation and monitoring of risk reduction measures.

2.69 A comprehensive security risk register will better enable management to review, and as necessary, amend aspects of the risk assessment in light of new circumstances. Organisations should ensure that there is appropriate managerial acceptance of the identified risks, and of those risks that require treatment, as well as the type of treatment to be used. Information obtained from this process can then be used to assist in the development of an organisation's security plan.

Recommendation No.2

2.70 The ANAO recommends that Australian Government organisations adopt a systematic and coordinated security risk management process, including documenting the identification, analysis, evaluation and treatment of security risks in a security risk register that is endorsed by the organisation's senior management.

Organisations' responses to the recommendation

Attorney-General's Department

Agreed.

Australian Agency for International Development

Agreed. The report noted that AusAID had in place security risk registers that had been produced as part of a risk review conducted in 2007 but that it had not developed a comprehensive security risk register. AusAID has and will continue to strengthen its security risk management arrangements to ensure there is in place a systematic and coordinated security risk management process, including documenting identification, analysis, evaluation and treatment of security risk in a single comprehensive security risk register that is endorsed by AusAID's Security Executive.

We have already commenced a review of existing policy and procedures and are currently updating these. In 2009-10 AusAID will develop a whole-of-agency security risk register and agency security plan. The AusAID Security Plan, polices and procedures will be endorsed by the Security Executive.

Australian Institute of Health and Welfare

Agreed.

Department of the Treasury

Treasury agrees with this recommendation, and has a security risk register which incorporates many of the facets noted in the recommendation. Treasury will review its security risk management process as part of a wider corporate risk management approach to ensure compliance with this recommendation.

Security plans

2.71 The PSM advises that organisations should use the information derived and decisions made in the security risk management process to develop security risk management plans. A security risk management plan should define how security risk is identified and handled in the organisation. One of the minimum standards in the PSM is that:

> each agency must prepare a security plan to manage its security risks. The security plan should be updated or revised on a regular basis or when risks or circumstances change significantly.[21]

2.72 While the PSM does not mandate the matters to be included in a security plan it does provide guidance. The following Table (based on the guidance in the PSM) outlines the key issues that can be included in an organisation's security plan.

[21] *Protective Security Manual, 2005*, op.cit, p. B18.

Table 2.2

Guide to Preparing a Security Plan

What to include	Description
Introduction	A statement from the agency head (or equivalent) outlining the importance of the plan.
Statement of purpose	Explaining the relationship between agency security practices and the corporate plans and business objectives (in other words, what is valuable to the agency and how its protection will help to achieve desired outcomes).
Security environment	A summary of the threat assessment and the agency's current exposure as well as a general assessment of current protective security arrangement
Security values	A statement outlining the organisation philosophy in relation to security risk management
Objectives	Clear concise statements about what the security plan is designed to achieve. They should be related to the agency's corporate objectives The security plan should refer to all the agency's security publications such as the agency's security policy statement and any security instructions.
Security strategies and actions	The strategies to be introduced or maintained to achieve the desired corporate security outcomes. This section should describe the security treatments (actions) to be implemented and the implementation strategy. For instance, if a security awareness session for employees handling security classified information is one of the treatments, describe how this is to be achieved and who is responsible
Residual risks	Residual risks should be estimated, described and rated to guide priorities for monitoring risks and evaluating treatments.
Monitoring and evaluation	Outlines who is responsible for monitoring the security plan and when the plan should be evaluated to see if it objective is being achieved; or whether it should be updated or revised as a result of changing security risks or circumstances
Timetable	Information about significant steps in the implementation and monitoring of risk treatments.
Resources	This part should document the security budget and determine the cost of the recommendations or options.

Source: Based on PSM 2005 Part B Annexe G p. B28.

2.73 Treasury developed a security risk plan to help direct its security risk management activities. Treasury's security plan was consistent with ANAO's expectations of the type of information that organisations should include in a security plan and generally reflected the guidance suggested in the PSM. For example, Treasury's security plan outlined:

- principles of security;

- security environment and objectives;
- site security and threat assessments;
- security accountability and responsibility;
- details of operational risks collated from the security risk review;
- review and monitoring arrangements, including when the plan should be reviewed; and
- protective security risk reduction measures.

2.74 As mentioned, the development of security plans for AusAID's two major Canberra locations were included as part of its outsourced risk review. The ANAO notes that the scope of these plans was to provide a broad outline of the measures to address physical security risks at the relevant offices. The security plans provided information on:

- staff, visitor, contractor and guard awareness and responsibilities;
- access control;
- information marking, handling and storage;
- asset register and treatment of assets; and
- a recommended timetable for security audits.

2.75 These plans are likely to be useful to manage the physical security risks at these premises. However, the limited scope of AusAID's plans meant that they do not contain the key elements of an overarching security plan as described in the PSM (as per Table 2.2). In particular the plans did not contain:

- a statement from the head of the organisation;
- a statement of purpose;
- details of security values objectives and strategies;
- details of monitoring and evaluation (other than a recommended timetable for security related audits); and
- resources required.[22]

[22] The two security plans were appendices to the risk review undertaken by consultants. The full report on the risk review contained details of threat assessments, detailed information on the premises reviewed, risk analysis and assessment and risk registers.

2.76 In addition, as noted previously there was no evidence of AusAID management's endorsement of these plans.

Integrating security risk management into corporate risk management activities

2.77 In addition to security awareness training (which is discussed in Chapter 3), having key security risks reflected in corporate risk management policies assists in promoting a stronger security culture. Specifically, organisations will be better placed to identify and deal with security issues when the management of security risks is integrated, or aligned, with the organisation's overall risk management and planning processes. In the absence of a structured approach to achieve this, there is an increased likelihood that security risk management activities and practices:

- are not treated as an central part of the organisation's day-to-day business, but as support or peripheral functions;
- are not afforded sufficient attention or resources; and
- are inconsistent with the organisation's broader risk management priorities and strategies.[23]

2.78 As indicated in the PSM, better results are likely to be achieved when:

> Planning for the management of security risks should be part of an agency's culture. It should be integrated into the agency's philosophy, practices and strategic and organisational plans and not viewed or practised as a separate program. Corporate and business plans are key mechanisms an agency uses to establish its goals, objectives and strategies. When security considerations are included in the corporate planning process, the security plan is more likely to meet corporate needs.[24]

2.79 In AusAID and the AIHW security issues were not systematically linked with corporate risk management and business planning activities. Treasury's risk management policy, as discussed in paragraph 2.34, indicated that as part of operational planning, groups/divisions must complete an assessment of risks relevant to their areas of operation. Our audit indicated,

[23] Australian National Audit Office, ANAO Audit Report No.55 2003-04, *Management of Protective Security, pp. 23 and 27*, available from <http://www.anao.gov.au/uploads/documents/2003-04_Audit_Report_55.pdf> [accessed 2 April 2009].

[24] *Protective Security Manual*, op.cit, p. B2.

however, that security risks are generally not being explicitly considered in the identification of risks in group or divisional operational plans.

2.80 Our previous audit coverage has also identified that there is scope to improve the integration of security risk management activities with organisations' broader risk management activities.

2.81 As reflected in the PSM, organisations need to better integrate the consideration of security risks in corporate risk management policies and processes. In addition, security risks should also be considered in the development of line area business/operational plans. Mechanisms to achieve this could include having the ASA provide input to key steps in the planning processes and including references to security risks in risk management templates. This could be further supported by including security risks in risk management awareness seminars.

Recommendation No.3

2.82 The ANAO recommends that organisations establish mechanisms to ensure that security risks are integrated, as appropriate, into broader corporate risk management and business planning activities.

Organisations' responses to the recommendation

Attorney-General's Department

Agreed.

Australian Agency for International Development

Agreed. The Security Management Section already enjoys a good relationship with key sections within the agency including Corporate Planning and Reform Section and the Audit Section and will continue to work with these areas to better align security and corporate risks and to incorporate consideration of security risks in agency business planning activities. Through internal channels and the rollout of the Security Management Section's Communication Strategy, AusAID will enhance the agency's understanding of protective security and security risks.

Australian Institute of Health and Welfare

Agreed.

Department of the Treasury

Treasury agrees with this recommendation.

3. Monitoring and review

This chapter addresses whether organisations have sufficient and appropriate arrangements to monitor security risks. It also examines a selection of security risk reduction measures or treatment controls to assess if they are operating as intended.

Introduction

3.1 The effective management of security risks requires a systematic and coordinated program to monitor both identified risks and the related risk treatments and controls. Organisations that routinely monitor security risks, including any changes in their risk environment, are better placed to detect events that may alter their risk management priorities than organisations without regular monitoring arrangements.

3.2 Monitoring is important to help ensure that security plans are being properly implemented, remain relevant and continue to meet the organisation's needs. In particular, monitoring should assess whether security risk treatment controls are working as intended and remained focused on the areas of greatest risk or exposure.[25]

3.3 The PSM states that:

> The agency's external and internal context, as well as the sources of potential harm, must be monitored continuously to ensure that changes in the risk environment are detected. Substantial changes to the risk environment will require a partial or complete review to ensure the security plan is still relevant.[26]

Monitoring and review of the organisational risk environment

3.4 The ANAO assessed whether each of the audited organisations routinely monitored their security environments.

3.5 Treasury and AusAID had sound processes in place to enable the ongoing monitoring of their security environments. The AIHW's monitoring of its general risk environment did not include a separate structured

[25] Australian National Audit Office, op. cit. p.37.

[26] *Protective Security Manual*, op.cit, p B 18.

consideration of security risks. Rather, the AIHW advised the ANAO that changes impacting on the security environment are discussed by senior management only when required.

3.6 Treasury and AusAID demonstrated active monitoring of their security risk environment by:

- including a threat assessment as part of their risk reviews. This included obtaining advice on known threats and changes to their respective security environments from security specialists such as the Australian Federal Police and the Australian Security Intelligence Organisation.[27]
- regularly revising their security plans;
- regularly capturing and reporting details of security incidents or breaches (this is discussed later in Chapter 3); and
- establishing clear reporting lines to and from their senior executives, including having security as a standard agenda item at senior management meetings.

3.7 For organisations that rely on staff having a strong security focus as a mechanism to reduce security risk, including security related questions in staff surveys can be a useful way of monitoring potential changes to the security risk environment. The ANAO noted that Treasury included a series of questions relating to security awareness and responsibility in its 2007 Staff Survey. The results of the survey showed that 97 per cent of respondents indicated a high level of understanding of their security responsibilities and how they impact the handling of classified information. In addition, 89 per cent of respondents indicated that they considered the words and actions of Treasury's senior management adequately reflected the importance of security in Treasury.

3.8 The ANAO considers that including questions relating to security management in staff surveys is better practice, particularly for organisations which have significant security risks and consequences.

[27] The ANAO also observed that AusAID and Treasury regularly obtained advice about their overseas risks, but we did not review this advice as it was outside the scope of this audit.

Monitoring and review of key controls

3.9 Each of the audited organisations had developed a range of controls designed to reduce their security risks. The ANAO examined a number of selected controls to assess whether they were operating effectively and found that they were generally operating as intended. However, in each organisation there were shortcomings in the examined controls, including scope to improve the monitoring of such controls.

3.10 This result was consistent with the ANAO's previous protective security audits which identified that programs to monitor risk treatments and controls were not up-to-date. This finding suggests that organisations needed to increase their efforts in this area.

3.11 The ANAO focussed on controls that were similar across the three audited organisations under the broad themes of:

- displaying staff identification passes;
- security clearances/undertakings;
- security awareness training;
- breach reporting (Treasury and AusAID); and
- management of contracted security services (Treasury and AusAID).

3.12 The ANAO's findings are set out below.

Displaying staff identification passes

3.13 A key protective security control at each of the three audited organisations was that staff were required to display their personal identification pass at all times. All staff observed during the audit at Treasury and AusAID were found to be displaying their passes. The ANAO observed that not all staff at the AIHW displayed their passes. In order to gauge the level of compliance the ANAO tested a sample of 51 staff members at the AIHW and found that only 41 per cent displayed their pass at the time of our examination.

3.14 The difference in this result could be due to the fact that, unlike Treasury and AusAID, passes at the AIHW were not required to gain access to the buildings and/or specific floors. The AIHW advised that the physical security arrangements for entry to its premises were being reviewed to ascertain whether a swipe card system could be introduced. The ANAO notes where decisions are taken not to adopt such measures for cost effectiveness reasons, organisations can still increase staff use of identification passes in a low cost manner by:

- better promoting the wearing of passes;
- regularly monitoring whether passes are being displayed correctly – that is assessing if the control is working effectively; and as necessary
- strengthening sanctions for non-compliance.

Security clearances/undertakings

3.15 All of the audited organisations required employees and other persons, such as contractors, who required access to security classified information to be security cleared to appropriate levels.

3.16 The ANAO examined a sample of security clearances in each organisation to assess if the information contained on the clearance subjects' personal security files was sufficient to support the decision to grant or deny the security clearance. In this regard, the ANAO examined whether the personal security file included: details of the position assessment; copies of all relevant personal documentation (properly certified); interview and referee reports (where these were required); a record of the checks and enquiries undertaken; and a copy of the clearance decision.

3.17 The ANAO examined a sample of 30[28] security clearances in Treasury and found that all the files examined contained sufficient information to support the decision made. The ANAO also examined a sample of 30 security clearances at AusAID. Our examination found files did not always contain sufficient information to support the decision made. The main issues identified were that:

- around 24 per cent of requests for security clearance forms did not always clearly identify the reason for the security clearance, nor indicate whether the duties of the position required access to security classified information or resources;
- information documents and consent forms were incomplete in approximately 12 per cent of files examined;

[28] Of the sample, eight were in the process of reevaluation at the time of the audit and were not able to be tested.

- in around 12 per cent of files examined there was limited documentation to indicate whether an individual's background had been assessed. The most common missing forms were police checks, ASIO security assessments and workplace and personal referees; and
- three files transferred to AusAID from other Australian Government organisations did not contain evidence that AusAID had reviewed or assessed the work done by the other organisation before accepting the clearance.

3.18 In addition, in 15 of the 30 files examined at AusAID, the date of effect for the security clearance was backdated prior to the date of the delegate's approval of the clearance. In six cases, the difference was 60 days or more. The backdating of the granting of security clearances suggested that these clearance subjects may have had access to classified material before their clearance had been obtained.

3.19 The ANAO notes that AusAID has recently contracted out the provision of security vetting services to the Australian Security Vetting Service (ASVS). The ANAO's examination indicated that those files reviewed where the clearance had been undertaken by the ASVS were complete in all instances. However, the security clearances submitted by ASVS to AusAID for approval were endorsed by a staff member without the delegation to grant a security clearance on behalf of organisation. AusAID has advised that it will establish appropriate delegations for the approval of security clearances.

3.20 The AIHW also outsources its security clearances to the ASVS. ANAO's examination of the personal security files for its four cleared personnel found that all clearances had been appropriately conducted.

3.21 As previously mentioned, the AIHW's enabling legislation contains specific provisions requiring it to protect the confidentiality of the information provided to it. An important control in the protection of its data is that staff and contractors are required to sign a confidentiality undertaking upon commencement. Given the high reliance the AIHW places on this control, the ANAO tested whether confidentiality undertakings were signed for all staff. ANAO testing found signed confidentiality undertakings were in place for around 91 per cent of staff. However, approximately 12 per cent of the confidentiality undertakings on file contained errors such as:

- not signed by staff member;
- variances in dates between the staff member and witness signing; and

- forms signed well after date of commencement.

3.22 The AIHW advised that a recent internal review of confidentiality undertakings identified some recordkeeping issues and these could have contributed to this result. Given the importance of this control, the ANAO suggested the AIHW take additional measures to improve the level of compliance.

Security awareness training

3.23 A common security risk reduction measure is security awareness and training, particularly for those staff with access to security classified information. It is important that organisations ensure all staff are provided with sufficient instructions to:

- enable them to understand their own responsibilities in relation to security; and
- gain a general understanding of the particular security environment, including the security risks.

3.24 It is also important that organisations record attendance at such training in order to be able to monitor whether staff and contractors attended the required training. The PSM states:

> All levels of staff will need to be made aware of security risk. It is of paramount importance that information about security risk is readily available so that agency management and employees can take responsibility for managing security risks. This means that training, education and security awareness briefings should form a central part of any security plan'.[29]

3.25 The risk reviews in Treasury and AusAID and internal audit reviews undertaken at the AIHW each identified that the organisations needed to improve the level of security awareness among their staff. At the time of the audit, the AIHW was in the process of developing a security awareness training program, while Treasury and AusAID were both progressively strengthening their arrangements for heightening security awareness amongst staff.

3.26 Across the audited organisations security awareness training was designed to be delivered in a number of circumstances including:

[29] *Protective Security Manual*, op. cit, p B.27.

- when staff or contractors were issued a building pass;
- during new starters' induction sessions;
- remedially, that is in those instances where recurring breaches of security were identified (Treasury and AusAID); and
- upon issue and re-evaluation of a security clearance.

3.27 The ANAO examined existing and proposed training materials, and examined records of attendance at security briefings and other related training. Overall, the training materials addressed most of the key security issues relevant to each organisation. However, the ANAO observed:

- training records were not available or were not always maintained accurately – thereby reducing their reliability as evidence of the delivery of security awareness training;
- while training was encouraged or made compulsory for particular categories of staff, such as new staff, it was not targeted at existing staff or contractors; and
- none of the organisations was able to provide evidence of the security training being delivered upon the issue or re-evaluation of a security clearance. This may reflect a record keeping issue and suggests that organisations may need to improve their documentation of training attendance.

3.28 As the changes to the audited organisations' respective security awareness programs were only recently implemented (or were still in progress) at the time of the audit, it was too early to confirm that the enhanced training had been effective.

Breach reporting

3.29 Treasury and AusAID both had mechanisms in place to identify and report security breaches in relation to the access, handling and storage of classified material or resources. When a breach was identified, a breach notice was left in the relevant container, office or on the nearest desk and an explanation required for the staff member's manager.

3.30 Both organisations reported details of breach incidents to senior management on a regular basis. The arrangements supporting the issue and recording of breach notices at both organisations were sound, and the ANAO noted copies of breach notices were filed in employees' personal security files.

3.31 However, in AusAID a large number of breach notices issued were not 'closed out' by the return of the 'signed off' notice. At the time of the audit AusAID was unable to confirm who was responsible for the follow up of outstanding breach notices.

3.32 The ANAO's examination of the breach records for 2008 at Treasury and AusAID indicated that the recorded breaches largely related to information security issues, for example: security containers left unlocked; or security classified material not secured within the work area.[30] While these breaches represented a breakdown in security controls they were not, on their own, an indication that any information has been lost or that unauthorised use of that information had occurred. Both organisations had a series of sanctions for staff with recurring breaches, including a requirement to attend further security awareness training or the loss or lowering of their security clearances.

Management of contracted security services.

3.33 One of the major protective security measures Treasury and AusAID had established was the use of specialist guarding services. Guards were engaged to provide a range of security services including assisting with building access, security patrols and the issuing of security breaches for such things as unsecured classified material and open storage containers.

3.34 Across both organisations these contracts contained a range of standards that the contractors were required to meet. These included:

- compliance with the specific guarding instructions and standard operating procedures such as:
  - guarding positions being staffed at all times;
  - visitors registers being accurately maintained; and
  - timely breach and security incident reporting;
- compliance with all laws, codes of conduct and organisational policies; and
- personnel holding the required qualifications, clearance and approvals to provide the services.

[30] As previously mentioned, the ANAO's analysis of security breach records did not include security incidents relating to overseas activities.

3.35 Both organisations had a range of mechanisms available to them to monitor whether required standards were being met. These included:

- meetings;
- reviews of daily log book (which recorded visitors and guarding information);
- ad hoc inspections;
- quarterly checks;
- audits; and
- reviews of documentation and/or reports provided by the contractors.

3.36 Both organisations advised that regular meetings were held with the contractors to discuss performance and that other informal monitoring, such as the regular sighting of the log books, was undertaken. However, there was no evidence of the conduct of regular and formal monitoring taking place such as audits, inspections or quarterly checks.

3.37 The monitoring of contract performance is important to ensure that contractors are delivering the required services at a suitable standard of performance, as well as providing value for money. Treasury and AusAID will benefit from strengthening and formalising the monitoring of the performance of contractors performing security related services.

3.38 The results discussed in this chapter indicate that there was scope for the audited organisations to improve the monitoring of the controls used to reduce identified security risks. The strength of an organisation's protective security arrangements can be undermined if relevant controls are not operating effectively, or if they do not remain focused on the areas of greatest risk or exposure.

Recommendation No.4

3.39 The ANAO recommends that organisations periodically assess whether controls designed to reduce security risks are operating effectively and remain appropriate.

Organisations' responses to the recommendation

Attorney-General's Department

Agreed.

Australian Agency for International Development

Agreed. The Security Committee and Audit Committee are key mechanisms through which the review of effectiveness and appropriateness of security measures are conducted. A key component of the AusAID Security Plan will be a program of monitoring and review to ensure that strategies to control security risks are operating effectively and remain appropriate.

The report noted some room for improvement in the agency's security clearance processes. AusAID had already taken action to enhance its processes including:

- improved record keeping and documentation to support decisions to grant clearances;
- updating the Chief Executive Instructions to reflect security delegations;
- the introduction of checklists and delegate approval forms to accurately record the delegate's approval of a security clearance; and
- implementation of an audit of security service providers (vetting contractors). One review had already been conducted and the remaining two providers will be audited early in 2009–10.

Australian Institute of Health and Welfare

Agreed.

Department of the Treasury

Treasury agrees with this recommendation.

Ian McPhee
Auditor-General

Canberra ACT
23 June 2009

Appendices

Appendix 1: Protective Security Audits Undertaken by the ANAO

Since 1995, the ANAO has completed the following cross-agency protective security audits:

- ANAO Audit Report No.21 1996–97, *Protective Security;*
- ANAO Audit Report No.7 1999–2000, *Operation of the Classification System for Protecting Sensitive Information;*
- ANAO Audit Report No.22, 2001–02, *Personnel Security—Management of Security Clearances;*
- ANAO Audit Report No.23 2002–03, *Physical Security Arrangements in Commonwealth Agencies;*
- ANAO Audit Report No.55 2003–04, *Management of Protective Security;*
- ANAO Audit Report No.41 2004–05, *Administration of Security Incidents, including the Conduct of Security Investigations;*
- ANAO Audit Report No.23 2005–06, *IT Security Management;* and
- ANAO Audit Report No.43 2006–07, *Managing Security Issues in Procurement and Contracting.*
- ANAO Audit Report No.41 2007–08, *Management of Personnel Security-Follow-up Audit.*

Appendix 2: Comments from the Selected Organisations

This Appendix contains general comments received on the audit report that are not shown in the body of the report.

Each of the organisations involved in the audit were provided with the opportunity to comment on the proposed audit report in accordance with the provisions of section 19 of the *Auditor-General Act 1997*.

Organisations' responses to the recommendations have been included in the main body of the report under the subheading 'Organisations' responses' directly following the recommendation.

General responses are reproduced below.

Attorney-General's Department

AGD supports the overall findings and recommendations of the report.

With regard to Recommendation 1, AGD will work together with Finance to clarify the requirements for CAC Act agencies to comply with the PSM.

The other recommendations, when implemented, will assist the audited organisations to meet the Government's and the public's expectations that the functions performed by Government agencies and the official resources held by them will be given appropriate protection.

Australian Agency for International Development

AusAID welcomes the audit which recognises the agency has in place sound security risk management processes. As noted in the report, AusAID has established and implemented effective arrangements for managing security risks. This includes a current and endorsed security risk management policy and clear reporting lines to and from the Senior Executive in relation to security risk matters.

Australian Institute of Health and Welfare

The AIHW agrees with each of the four recommendations in the proposed report.

As stated in this report, the audit "did not examine security risk practices or controls relating specifically to information and communications technology (ICT)". As a small Government agency that holds and analyses large amounts of electronic data, the AIHW has a very strong focus on ICT security risks, with a full-time Information and Communications Technology Security Advisor. Other security roles are assigned to staff but form only a relatively small part of their roles and responsibilities. The detailed comments in this report on the AIHW's security practices should be read in light of the exclusion of ICT security risks from the scope of this audit.

The AIHW has not been directed to comply with the Protective Security Manual (PSM). The AIHW agrees that the AGD should discuss its legal advice with the Department of Finance and Deregulation (DoFD), and that AGD and DoFD should then provide jointly agreed written advice to the Chief Executives of the affected CAC Act agencies about the consequences of that legal advice.

Despite not having been directed to comply with the PSM, the AIHW uses the PSM to guide its security management. For many years the AIHW has completed a full response to the AGD's annual Australian Government Protective Security Survey even though the AGD has not required the AIHW to complete it.

This audit has been very useful to the AIHW. The AIHW has since made several improvements to its security risk management practices including the installation of swipe card controlled entry to all the AIHW buildings. This measure, backed up by a staff education program, has dramatically increased the number of staff displaying passes. The AIHW has agreed a timetable with its Audit and Finance Committee for making other security improvements arising from this audit by the end of 2009.

Department of Finance and Deregulation

Finance agrees with the recommendation.

Department of the Treasury

Treasury has reviewed the three applicable recommendations and broadly agrees with the ANAO's findings.

Series Titles

ANAO Audit Report No.1 2008–09
Employment and Management of Locally Engaged Staff
Department of Foreign Affairs and Trade

ANAO Audit Report No.2 2008–09
Tourism Australia

ANAO Audit Report No.3 2008–09
Establishment and Management of the Communications Fund
Department of Broadband, Communications and the Digital Economy
Department of Finance and Deregulation

ANAO Audit Report No.4 2008–09
The Business Partnership Agreement between the Department of Education, Employment and Workplace Relations (DEEWR) and Centrelink
Department of Education, Employment and Workplace Relations
Centrelink

ANAO Audit Report No.5 2008–09
The Senate Order for Departmental and Agency Contracts (Calendar Year 2007 Compliance)

ANAO Audit Report No.6 2008–09
Illegal, Unreported and Unregulated Fishing in the Southern Ocean
Australian Customs Service

ANAO Audit Report No.7 2008–09
Centrelink's Tip-off System
Centrelink

ANAO Audit Report No.8 2008–09
National Marine Unit
Australian Customs Service

ANAO Report No.9 2008–09
Defence Materiel Organisation–Major Projects Report 2007–08

ANAO Audit Report No.10 2008–09
Administration of the Textile, Clothing and Footwear Post–2005 (SIP) Scheme
Department of Innovation, Industry, Science and Research

ANAO Audit Report No.11 2008–09
Disability Employment Services
Department of Families, Housing, Community Services and Indigenous Affairs
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.12 2008–09
Active After-school Communities Program
Australian Sports Commission

ANAO Audit Report No.13 2008–09
Government Agencies' Management of their Websites
Australian Bureau of Statistics
Department of Agriculture, Fisheries and Forestry
Department of Foreign Affairs and Trade

ANAO Audit Report No.14 2008–09
Audits of Financial Statement of Australian Government Agencies for the Period Ending June 2008

ANAO Audit Report No.15 2008–09
The Australian Institute of Marine Science's Management of its Co-investment Research Program
Australian Institute of Marine Science

ANAO Audit Report No.16 2008–09
The Australian Taxation Office's Administration of Business Continuity Management
Australian Taxation Office

ANAO Audit Report No.17 2008–09
The Administration of Job Network Outcome Payments
Department of Education, Employment and Workplace Relations

ANAO Audit Report No.18 2008–09
The Administration of Grants under the Australian Political Parties for Democracy Program
Department of Finance and Deregulation

ANAO Audit Report No.19 2008–09
CMAX Communications Contract for the 2020 summit
Department of the Prime Minister and Cabinet

ANAO Audit Report No.20 2008–09
Approval of Funding for Public Works

ANAO Audit Report No.21 2008–09
The Approval of Small and Medium Sized Business System Projects
Department of Education, Employment and Workplace Relations
Department of Health and Ageing
Department of Veterans' Affairs

ANAO Audit Report No.22 2008–09
Centrelink's Complaints Handling System
Centrelink

ANAO Audit Report No.23 2008–09
Management of the Collins-class Operations Sustainment
Department of Defence

ANAO Audit Report No.24 2008–09
The Administration of Contracting Arrangements in relation to Government Advertising to November 2007
Department of the Prime Minister and Cabinet
Department of Finance and Deregulation
Department of Education, Employment and Workplace Relations
Department of Health and Ageing
Attorney-General's Department

ANAO Audit Report No.25 2008–09
Green Office Procurement and Sustainable Office Management

ANAO Audit Report No.26 2008–09
Rural and Remote Health Workforce Capacity – the contribution made by programs administered by the Department of Health and Ageing
Department of Health and Ageing

ANAO Audit Report No.27 2008–09
Management of the M113 Armoured Personnel Upgrade Project
Department of Defence

ANAO Audit Report No.28 2008–09
Quality and Integrity of the Department of Veterans' Affairs Income Support Records
Department of Veterans' Affairs

ANAO Audit Report No.29 2008–09
Delivery of Projects on the AusLink National Network
Department of Infrastructure, Transport, Regional Development and Local Government

ANAO Audit Report No.30 2008–09
Management of the Australian Government's Action Plan to Eradicate Trafficking in Persons
Attorney-General's Department
Department of Immigration and Citizenship
Australian Federal Police
Department of Families, Housing, Community Services and Indigenous Affairs

ANAO Audit Report No.31 2008–09
Army Reserve Forces
Department of Defence

ANAO Audit Report No.32 2008–09
Management of the Tendering Process for the Construction of the Joint Operation Headquarters
Department of Defence

ANAO Audit Report No.33 2008–09
Administration of the Petroleum Resource Rent Tax
Australian Taxation Office

ANAO Audit Report No.34 2008–09
The Australian Taxation Office's Management of Serious Non-Compliance

ANAO Audit Report No.35 2008–09
Management of the Movement Alert List
Department of Immigration and Citizenship

ANAO Audit Report No.36 2008–09
Settlement Grants Program
Department of Immigration and Citizenship

ANAO Audit Report No.37 2008–09
Online Availability of Government Entities' Documents Tabled in the Australian Parliament

ANAO Audit Report No.38 2008–09
Administration of the Buyback Component of the Securing our Fishing Future Structural Adjustment Package
Department of Agriculture, Fisheries and Forestry

ANAO Audit Report No.39 2008–09
Administration of the Securing our Fishing Future Structural Adjustment Package Assistance Programs
Department of Agriculture, Fisheries and Forestry

ANAO Audit Report No.40 2008–09
Planning and Allocating Aged Care Places and Capital Grants
Department of Health and Ageing

ANAO Audit Report No.41 2008–09
The Super Seasprite
Department of Defence

ANAO Audit Report No.42 2008–09
Interim Phase of the Audit of Financial Statements of General Government Sector Agencies for the Year ending 30 June 2009

ANAO Audit Report No.43 2008–09
Construction of the Christmas Island Immigration Detention Centre
Department of Finance and Deregulation

Current Better Practice Guides

The following Better Practice Guides are available on the Australian National Audit Office Website.

Business Continuity Management	June 2009
Building resilience in public sector entities	
Developing and Managing Internal Budgets	June 2008
Agency Management of Parliamentary Workflow	May 2008
Public Sector Internal Audit	
An Investment in Assurance and Business Improvement	Sep 2007
Fairness and Transparency in Purchasing Decisions	
Probity in Australian Government Procurement	Aug 2007
Administering Regulation	Mar 2007
Developing and Managing Contracts	
Getting the Right Outcome, Paying the Right Price	Feb 2007
Implementation of Programme and Policy Initiatives:	
Making implementation matter	Oct 2006
Legal Services Arrangements in Australian Government Agencies	Aug 2006
Preparation of Financial Statements by Public Sector Entities	Apr 2006
Administration of Fringe Benefits Tax	Feb 2006
User–Friendly Forms	
Key Principles and Practices to Effectively Design and Communicate Australian Government Forms	Jan 2006
Public Sector Audit Committees	Feb 2005
Fraud Control in Australian Government Agencies	Aug 2004
Security and Control Update for SAP R/3	June 2004
Better Practice in Annual Performance Reporting	Apr 2004
Management of Scientific Research and Development Projects in Commonwealth Agencies	Dec 2003
Public Sector Governance	July 2003
Goods and Services Tax (GST) Administration	May 2003

Building Capability—A framework for managing learning and development in the APS	Apr 2003
Administration of Grants	May 2002
Performance Information in Portfolio Budget Statements	May 2002
Some Better Practice Principles for Developing Policy Advice	Nov 2001
Rehabilitation: Managing Return to Work	June 2001
Building a Better Financial Management Framework	Nov 1999
Building Better Financial Management Support	Nov 1999
Commonwealth Agency Energy Management	June 1999
Security and Control for SAP R/3	Oct 1998
Controlling Performance and Outcomes	Dec 1997
Protective Security Principles (in Audit Report No.21 1997–98)	Dec 1997